

Bijlage 1 – Artikelen Woo

Artikel 1.1

Eenieder heeft recht op toegang tot publieke informatie zonder daartoe een belang te hoeven stellen, behoudens bij deze wet gestelde beperkingen.

Artikel 2.1

In deze wet en de daarop berustende bepalingen wordt verstaan onder:

document: een door een orgaan, persoon of college als bedoeld in artikel 2.2, eerste lid, opgemaakt of ontvangen schriftelijk stuk of ander geheel van vastgelegde gegevens dat naar zijn aard verband houdt met de publieke taak van dat orgaan, die persoon of dat college;

milieu-informatie: hetgeen daaronder wordt verstaan in artikel 19.1a van de Wet milieubeheer;

Onze Minister: Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties;

publieke informatie: informatie neergelegd in documenten die berusten bij een orgaan, persoon of college als bedoeld in artikel 2.2, eerste lid.

Artikel 2.4. Zorgplicht en openbaarmaking

1. Een bestuursorgaan draagt er zorg voor dat de documenten die het ontvangt, vervaardigt of anderszins onder zich heeft, zich in goede, geordende en toegankelijke staat bevinden.
2. Een bestuursorgaan draagt er zoveel mogelijk zorg voor dat de informatie die het overeenkomstig deze wet verstrekt, actueel, nauwkeurig en vergelijkbaar is.
3. Indien een bestuursorgaan overeenkomstig deze wet informatie openbaar maakt, geschiedt dat op zodanige wijze dat de belanghebbende en belangstellende burger zoveel mogelijk wordt bereikt en op de volgende algemeen toegankelijke wijze:
 - a. in een voor hergebruik beschikbare vorm die voldoet aan de voorwaarden van de Wet hergebruik van overheidsinformatie;
 - b. of, indien verstrekking in een machinaal leesbaar open formaat redelijkerwijs niet geveerd kan worden, in andere elektronisch doorzoekbare vorm;
 - c. of, indien elektronische verschaffing redelijkerwijs niet geveerd kan worden, door verstrekking van een kopie van de letterlijke inhoud ervan in andere vorm te verstrekken;
 - d. of, indien verstrekking van een kopie of de letterlijke inhoud redelijkerwijs niet geveerd kan worden, door een uittreksel of een samenvatting van de inhoud te geven, inlichtingen daaruit te verschaffen of door terinzagelegging.

Artikel 2.5

Bij de toepassing van deze wet wordt uitgegaan van het algemeen belang van openbaarheid van publieke informatie voor de democratische samenleving.

Artikel 4.1

1. Eenieder kan een verzoek om publieke informatie richten tot een bestuursorgaan of een onder verantwoordelijkheid van een bestuursorgaan werkzame instelling, dienst of bedrijf. In het laatste geval beslist het verantwoordelijke bestuursorgaan op het verzoek.
2. Een verzoek kan mondeling of schriftelijk worden ingediend en kan elektronisch worden verzonden op de door het bestuursorgaan aangegeven wijze.
3. De verzoeker behoeft bij zijn verzoek geen belang te stellen.
4. De verzoeker vermeldt bij zijn verzoek de aangelegenheid of het daarop betrekking hebbende document, waarover hij informatie wenst te ontvangen.
5. Indien een verzoek te algemeen geformuleerd is, verzoekt het bestuursorgaan binnen twee weken na ontvangst van het verzoek de verzoeker om het verzoek te preciseren en is het de verzoeker daarbij behulpzaam.
6. Het bestuursorgaan kan besluiten een verzoek niet te behandelen, indien de verzoeker niet meewerkt aan een verzoek tot precisering als bedoeld het vijfde lid. In afwijking van artikel 4:5, vierde lid, van de Algemene wet bestuursrecht wordt het besluit om het verzoek niet te behandelen aan de verzoeker bekendgemaakt binnen twee weken nadat het verzoek is gepreciseerd of nadat de daarvoor gestelde termijn ongebruikt is verstreken.
7. Een verzoek om informatie wordt ingewilligd met inachtneming van het bepaalde in hoofdstuk 5.

Artikel 4.4

1. Het bestuursorgaan beslist op het verzoek om informatie zo spoedig mogelijk, doch uiterlijk binnen vier weken gerekend vanaf de dag na die waarop het verzoek is ontvangen.
2. Het bestuursorgaan kan de beslissing voor ten hoogste twee weken verdagen, indien de omvang of de gecompliceerdheid van de informatie een verlenging rechtvaardigt. Van de verdaging wordt voor de afloop van de eerste termijn schriftelijk gemotiveerd mededeling gedaan aan de verzoeker.
3. Onverminderd artikel 4:15 van de Algemene wet bestuursrecht wordt de termijn voor het geven van een beschikking opgeschort gerekend vanaf de dag na die waarop het bestuursorgaan de verzoeker mededeelt dat toepassing is gegeven aan artikel 4:8 van de Algemene wet bestuursrecht, tot en met de dag waarop door de belanghebbende of belanghebbenden een zienswijze naar voren is gebracht of de daarvoor gestelde termijn ongebruikt is verstreken.
4. Indien de opschorting, bedoeld in het derde lid, eindigt, doet het bestuursorgaan daarvan zo spoedig mogelijk mededeling aan de verzoeker, onder vermelding van de termijn binnen welke de beschikking alsnog moet worden gegeven.
5. Indien het bestuursorgaan heeft besloten informatie te verstrekken, wordt de informatie verstrekt tegelijk met de bekendmaking van het besluit, tenzij naar verwachting een belanghebbende bezwaar daartegen heeft, in welk geval de informatie wordt verstrekt twee

weken nadat de beslissing is bekendgemaakt. Indien wordt verzocht om een voorlopige voorziening als bedoeld in artikel 8:81 van de Algemene wet bestuursrecht, wordt de openbaarmaking opgeschort totdat de voorzieningenrechter uitspraak heeft gedaan of het verzoek is ingetrokken.

6. Indien het bestuursorgaan heeft besloten informatie te verstrekken die rechtstreeks betrekking heeft op een derde of die van een derde afkomstig is, deelt het bestuursorgaan dit besluit gelijktijdig mede aan deze derde.

Artikel 4.5

1. Het bestuursorgaan verstrekt de informatie in de door verzoeker verzochte vorm of, indien dit redelijkerwijs niet gevegd kan worden, met inachtneming van het bepaalde in artikel 2.4, derde lid.

2. Indien de informatie reeds in een voor de verzoeker gemakkelijk toegankelijke vorm voor het publiek beschikbaar is, wijst het bestuursorgaan de verzoeker daarop.

Artikel 5.1

1. Het openbaar maken van informatie ingevolge deze wet blijft achterwege voor zover dit:

- a. de eenheid van de Kroon in gevaar zou kunnen brengen;
- b. de veiligheid van de Staat zou kunnen schaden;
- c. bedrijfs- en fabricagegegevens betreft die door natuurlijke personen of rechtspersonen vertrouwelijk aan de overheid zijn meegedeeld;
- d. persoonsgegevens betreft als bedoeld in paragraaf 3.1 onderscheidenlijk paragraaf 3.2 van de Uitvoeringswet Algemene verordening gegevensbescherming, tenzij de betrokkene uitdrukkelijk toestemming heeft gegeven voor de openbaarmaking van deze persoonsgegevens of deze persoonsgegevens kennelijk door de betrokkene openbaar zijn gemaakt;
- e. nummers betreft die dienen ter identificatie van personen die bij wet of algemene maatregel van bestuur zijn voorgeschreven als bedoeld in artikel 46 van de Uitvoeringswet Algemene verordening gegevensbescherming, tenzij de verstrekking kennelijk geen inbreuk op de levenssfeer maakt.

2. Het openbaar maken van informatie blijft eveneens achterwege voor zover het belang daarvan niet opweegt tegen de volgende belangen:

- a. de betrekkingen van Nederland met andere landen en staten en met internationale organisaties;
- b. de economische of financiële belangen van de Staat, andere publiekrechtelijke lichamen of bestuursorganen, in geval van milieu-informatie slechts voor zover de informatie betrekking heeft op handelingen met een vertrouwelijk karakter;
- c. de opsporing en vervolging van strafbare feiten;
- d. de inspectie, controle en toezicht door bestuursorganen;

- e. de eerbiediging van de persoonlijke levenssfeer;
 - f. de bescherming van andere dan in het eerste lid, onderdeel c, genoemde concurrentiegevoelige bedrijfs- en fabricagegegevens;
 - g. de bescherming van het milieu waarop deze informatie betrekking heeft;
 - h. de beveiliging van personen en bedrijven en het voorkomen van sabotage;
 - i. het goed functioneren van de Staat, andere publiekrechtelijke lichamen of bestuursorganen.
3. Indien een verzoek tot openbaarmaking op een van de in het tweede lid genoemde gronden wordt afgewezen, bevat het besluit hiervoor een uitdrukkelijke motivering.
4. Openbaarmaking kan tijdelijk achterwege blijven, indien het belang van de geadresseerde van de informatie om als eerste kennis te nemen van de informatie dit kennelijk vereist. Het bestuursorgaan doet mededeling aan de verzoeker van de termijn waarbinnen de openbaarmaking alsnog zal geschieden.
5. In uitzonderlijke gevallen kan openbaarmaking van andere informatie dan milieuinformatie voorts achterwege blijven indien openbaarmaking onevenredige benadeling toebrengt aan een ander belang dan genoemd in het eerste of tweede lid en het algemeen belang van openbaarheid niet tegen deze benadeling opweegt. Het bestuursorgaan baseert een beslissing tot achterwege laten van de openbaarmaking van enige informatie op deze grond ten aanzien van dezelfde informatie niet tevens op een van de in het eerste of tweede lid genoemde gronden.
6. Het openbaar maken van informatie blijft in afwijking van het eerste lid, onderdeel c, in geval van milieu-informatie eveneens achterwege voor zover daardoor het in het eerste lid, onderdeel c, genoemde belang ernstig geschaad wordt en het algemeen belang van openbaarheid van informatie niet opweegt tegen deze schade.
7. Het eerste en tweede lid zijn niet van toepassing op milieu-informatie die betrekking heeft op emissies in het milieu.

Artikel 5.2. Persoonlijke beleidsopvattingen

1. In geval van een verzoek om informatie uit documenten, opgesteld ten behoeve van intern beraad, wordt geen informatie verstrekt over daarin opgenomen persoonlijke beleidsopvattingen. Onder persoonlijke beleidsopvattingen worden verstaan ambtelijke adviezen, visies, standpunten en overwegingen ten behoeve van intern beraad, niet zijnde feiten, prognoses, beleidsalternatieven, de gevolgen van een bepaald beleidsalternatief of andere onderdelen met een overwegend objectief karakter.
2. Het bestuursorgaan kan over persoonlijke beleidsopvattingen met het oog op een goede en democratische bestuursvoering informatie verstrekken in niet tot personen herleidbare vorm. Indien degene die deze opvattingen heeft geuit of zich erachter heeft gesteld, daarmee heeft ingestemd, kan de informatie in tot personen herleidbare vorm worden verstrekt.
3. Onverminderd het eerste en tweede lid wordt uit documenten opgesteld ten behoeve van formele bestuurlijke besluitvorming door een minister, een commissaris van de Koning, Gedeputeerde Staten, een gedeputeerde, het college van burgemeester en wethouders, een burgemeester, een wethouder, het dagelijks bestuur van een waterschap of een lid van dat bestuur, informatie verstrekt over persoonlijke beleidsopvattingen in niet tot personen herleidbare vorm, tenzij het kunnen voeren van intern beraad onevenredig wordt geschaad.

4. In afwijking van het eerste lid wordt bij milieu-informatie het belang van de bescherming van de persoonlijke beleidsopvattingen afgewogen tegen het belang van openbaarmaking. Informatie over persoonlijke beleidsopvattingen kan worden verstrekt in niet tot personen herleidbare vorm. Indien degene die deze opvattingen heeft geuit of zich erachter heeft gesteld, daarmee heeft ingestemd, kan de informatie in tot personen herleidbare vorm worden verstrekt.

BIJLAGE II

Inventaris

Nr		Type document	Datum	Besluit	Grondslag
Beleidsdocumenten en instrumenten implementatie AVG					
1		Privacybeleidskader NVAO	Maart 2021	openbaar	
1A		Concept 01/02	Juli 2020	Gedeeltelijk openbaar	5.2, 2 ^e lid/5.1 2 ^e lid sub e
1B		Concepten 03	November 2020	openbaar	
1C		Concept 04	Februari/maart 2021	openbaar	
2		Privacybeleidskader NVAO	Februari 2025	openbaar	
2A		Concept Privacybeleidskader (herzien)	November 2024	openbaar	
3		Privacyverklaring NVAO (extern)	September 2021	openbaar	
4		Privacyverklaring NVAO (extern)	Februari 2025	Is reeds openbaar	
5		Privacyverklaring Medewerkers	September 2021	openbaar	
6		Privacyverklaring NVAO (intern)	Februari 2025	openbaar	
7		DPIA Proces NVAO	Juli 2021	openbaar	
8		Memo Quickscan DPIA	Februari 2021	openbaar	

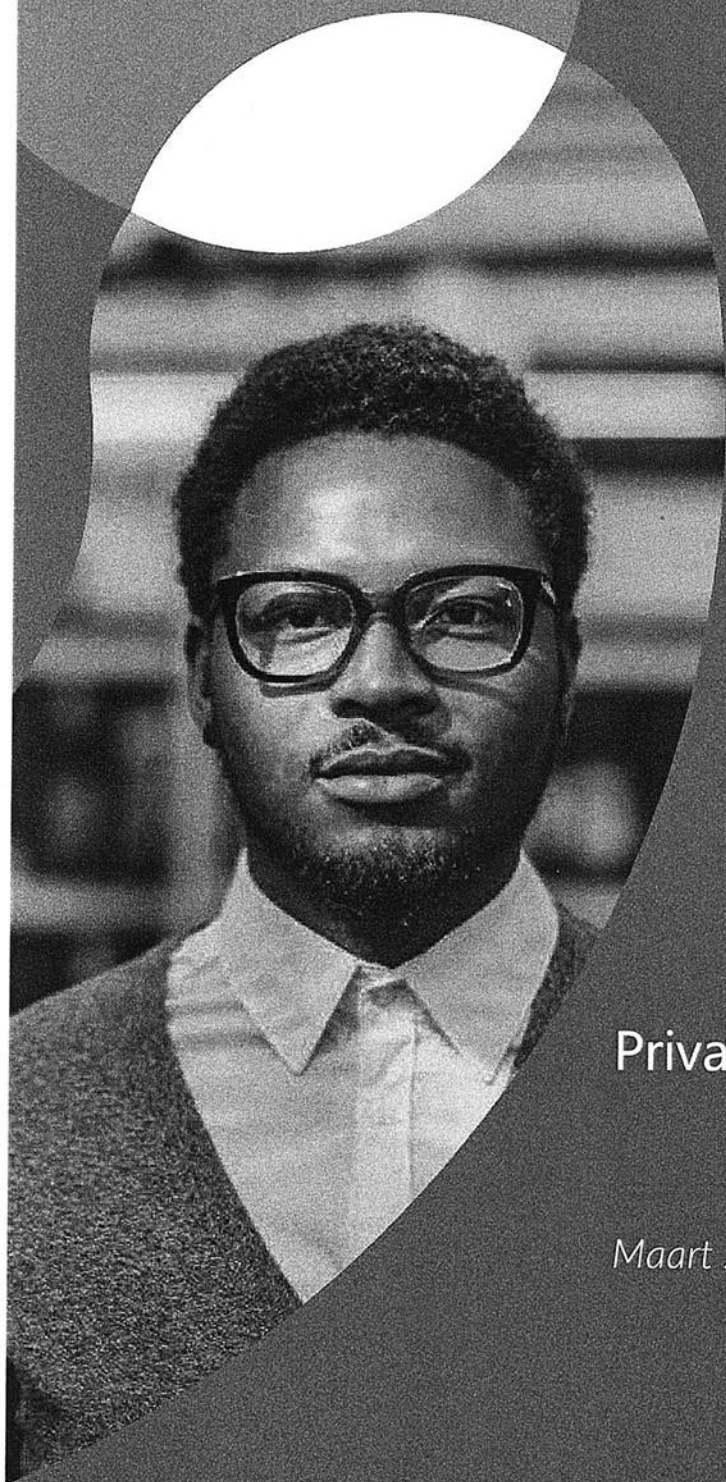
9	Protocol datalekken NVAO	November 2019	openbaar	
10	Protocol datalekken NVAO	Februari 2025	openbaar	
11	Protocol Rechten Betrokkenen NVAO	Juni 2021	openbaar	
12	Protocol Rechten Betrokkenen NVAO	Februari 2025	openbaar	
13	Handleiding Privacy by Design (model Rijksoverheid)	September 2023	Reeds openbaar	
14	Handleiding Bewaren van e-mail Rijksoverheid	Februari 2020	Reeds openbaar	
15	Register van verwerkingen	Februari 2025	openbaar	
16	Uitvoeringsregels NVAO	April 2024	Reeds openbaar	
17	Uitvoeringsregels NVAO (herzien)	September 2024	Reeds openbaar	
18	Model VWO NVAO	Februari 2025	openbaar	
19	Toestemmingsverklaring AVG accreditatie	2022	openbaar	
20	Personeelsreglement	2025	Gedeeltelijk openbaar, onderdeel Privacy openbaar, overige onderdelen buiten reikwijdte verzoek	

21	Handreiking veilige omgang persoonsgegevens	2021	Openbaar	
22	Toestemmingsverklaring Beeldmateriaal	2022	Openbaar	
Besluiten bestuur vaststellen documenten implementatie AVG				
23	Verslag DB	Februari 2021	Gedeeltelijk openbaar, onderdeel Privacy openbaar, overige onderdelen buiten reikwijdte verzoek	5.1, 2e lid, sub e
24	Verslag AB	Maart 2021	Gedeeltelijk openbaar, onderdeel Privacy openbaar, overige onderdelen buiten reikwijdte verzoek	5.1, 2e lid, sub e
25	Verslag DB	Augustus 2021	Gedeeltelijk openbaar, onderdeel Privacy openbaar, overige onderdelen buiten reikwijdte verzoek	5.1, 2e lid, sub e

E-mailberichten mbt beleidsdocumenten implementatie AVG					
26	Aanbieden stukken Directie	November 2020	Gedeeltelijk openbaar	5.1, 2e lid, sub e	
27	Aanbieden stukken DB met nota	Februari 2021	Gedeeltelijk openbaar	5.1, 2e lid, sub e	
28	Aanbieden stukken AB met nota	Maart 2021	Gedeeltelijk openbaar	5.1, 2e lid, sub e	
29	Aanbieden stukken Directie NL	Februari 2025	Gedeeltelijk openbaar	5.1, 2e lid, sub e	
Kennisdeling					
30	Bijeenkomst 2022	Januari 2022	openbaar		
31	Bijeenkomst 2023	Juni 2023	openbaar		
32	Bijeenkomst 2024 (Kwartet)	April 2024	openbaar		
33	Bijeenkomst 2025	Maart 2025	openbaar		
Jaarplanningen					
34	Jaarplanning 2024-		Openbaar		
DPIA					
35	Primair proces	2022	Openbaar		
Mededelingen Intranet en Selectielijst					

36	Publicatie intranet voor medewerkers	2021	Openbaar	
37	Selectielijst NVAO	2012	Is reeds openbaar	

Bijlage 3

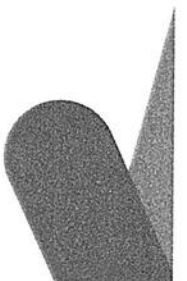


Privacy Beleidskader

Maart 2021

Privacy Beleidskader

Maart 2021



Inleiding

De Nederlands-Vlaamse Accreditatieorganisatie (NVAO) is een kwaliteitszorgorganisatie die op deskundige en onafhankelijke wijze de kwaliteit van het hoger onderwijs in Nederland en Vlaanderen borgt en die de kwaliteitscultuur binnen de instellingen voor hoger onderwijs in Nederland en Vlaanderen bevordert. Zij accrediteert bestaande en nieuwe opleidingen en beoordeelt de kwaliteitszorg van instellingen in het hoger onderwijs. Daarmee is de NVAO bewaker van de kwaliteit van het hoger onderwijs. De besluiten van de NVAO leiden tot erkenning van diploma's en titels en waar van toepassing tot bekostiging van opleidingen. De NVAO baseert haar beoordeling op advies van erkende deskundigen.

De NVAO werd in 2003 opgericht bij Verdrag tussen Nederland en Vlaanderen. De taken van de NVAO zijn in wetgeving vastgelegd. De NVAO wil ertoe bijdragen dat de kwaliteit van het hoger onderwijs in Vlaanderen en Nederland erkend wordt als internationaal aan de maat, maatschappelijk relevant en het vertrouwen geniet van studenten, werkgevers en de samenleving. Binnen de opdracht die in het accreditatieverdrag tussen Nederland en Vlaanderen aan de NVAO is toegekend, wil zij de kwaliteit van het hoger onderwijs borgen, verbeteringen stimuleren en een kwaliteitscultuur bevorderen.

Om dit werk goed te kunnen doen is verwerking van persoonsgegevens van medewerkers en de contactpersonen van ketenpartners en burgers noodzakelijk. De privacy van contactpersonen en relaties is erg belangrijk voor de NVAO en we hechten dan ook veel belang aan een correcte verwerking en gebruik van persoonsgegevens. De bescherming van persoonsgegevens is immers een grondrecht. De NVAO is verantwoordelijk voor de aantoonbare zorgvuldige omgang met persoonsgegevens.

De NVAO is een zelfstandig bestuursorgaan en opgericht naar Nederlands publiekrecht met de zetel in Den Haag. De NVAO valt onder verantwoordelijkheid van het Comité van Ministers. De NVAO heeft een nauwe samenwerking met de CDHO en CMMBO, die gebruik maken van de afdeling Ondersteuning en hostingsovereenkomsten hebben met de NVAO.

Dit privacy beleidskader richt zich tot iedereen die werkzaamheden verricht voor de NVAO en medewerkers van de CDHO en CMMBO. In het privacy beleidskader wordt uitgelegd hoe de NVAO aantoonbaar zorgvuldig omgaat met persoonsgegevens, wat daarbij de uitgangspunten zijn en wat de rol van de medewerker is bij de bescherming van persoonsgegevens¹.

¹ Voor een beknopte uitleg van begrippen (als persoonsgegevens en verwerking) zie bijlage 1.

Inhoud

- 1. Privacy beleidskader
 - 1.1 Doel
 - 1.2 Scope NVAO /CDHO/CMMBO
 - 1.3 Doelgroepen
 - 1.4 Wet- en regelgeving verwerking van persoonsgegevens
- 2. NVAO uitgangspunten voor omgang met persoonsgegevens
 - 2.1 Grondslag en doel
 - 2.2 Doelbinding
 - 2.3 Accuraat en actueel
 - 2.4 Bewaarbeperking
 - 2.5 Open en transparant
 - 2.6 Veilig en vertrouwelijk
 - 2.7 Verantwoordingsplicht
 - 2.8 Respect
- 3. Privacy governance
 - 3.1 Inleiding
 - 3.2 Privacy verantwoordelijkheden rollen en taken
 - 3.3 Privacy overlegstructuren
 - 3.4 Sturing, regie en toezicht
 - 3.5 Privacy trainingen en bewustwording
- 4. Slot
 - 4.1 Beheer
 - 4.2 Vaststellen
 - 4.3 Wijzigingen en evaluatie
- Bijlage 1 Begrippen
- Bijlage 2 Instrumenten (documenten, websites etc.)
- Bijlage 3 RASCI model

1 Privacy Beleidskader

Op het werk van het Nederlands Vlaamse Accreditatieorganisatie (NVAO) is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Daarnaast heeft de NVAO te maken met bijzondere wetgeving, waarin een grondslag voor verwerking van gegevens kan liggen. Denk hierbij bijvoorbeeld aan de gegevens die de NVAO nodig heeft van panelleden om hun deskundigheid voor deelname aan een panel te kunnen beoordelen. Voor de Afdeling Vlaanderen is dit geregeld in de Codex Hoger Onderwijs, voor de Afdeling Nederland is dit vastgelegd in de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW).

Het NVAO Privacy beleidskader geeft aan waar de NVAO op het vlak van gegevensbescherming voor staat en wat de uitgangspunten voor de omgang met persoonsgegevens zijn. Met dit kader wil de NVAO ervoor zorgen dat de privacybescherming in lijn is met de wettelijke vereisten en die aansluit of geïntegreerd wordt bij de bestaande processen en systemen van de NVAO. Bij alle uitgangspunten wordt steeds verwezen naar praktische ondersteunende instrumenten (checklists, stappenplan, procedures) van de NVAO dan wel (voor zover niet aanwezig) van OCW.

De uitleg van een aantal belangrijke begrippen uit de AVG is opgenomen in Bijlage 1: Begrippen.

1.1 Doel

Doel van dit beleidskader is een omgeving te creëren waarin elke medewerker van de NVAO:

- zijn of haar verantwoordelijkheid en rechten kent als het gaat om privacy en het verwerken van persoonsgegevens,
- in staat is om het juiste beleid en de juiste procedures te volgen,
- contact kan opnemen met de juiste personen wanneer er vragen zijn.

1.2 Scope

Het privacy beleidskader is bestemd voor de NVAO in zijn geheel. Alle handelingen binnen de NVAO met betrekking tot persoonsgegevens van burgers, bestuursleden, medewerkers, contactpersonen, zoals medewerkers kwaliteitszorg, panelleden en secretarissen, vallen allen binnen het bereik van dit beleidskader.

CMMBO en CDHO

Deze organisaties hebben zelfstandige taken en verantwoordelijkheden. Er is een nauwe samenwerkingsrelatie tussen de NVAO en de CMMBO/CDHO. Niet alleen zitten de organisaties fysiek in het pand bij de NVAO, de ondersteuning van CDHO en CMMBO is in dienst van de NVAO. Bovendien maken de drie organisaties gezamenlijk gebruik van de afdeling Ondersteuning van de NVAO (waaronder ICT, financiën en personeelszaken). Het privacybeleid van de NVAO omvat hiermee tevens de medewerkers werkzaam voor het secretariaat van CDHO en CMMBO. Het privacybeleid van de NVAO omvat niet de werkzaamheden van commissieleden CDHO en CMMBO, deze vallen onder verantwoordelijkheid van het Ministerie van Onderwijs, Cultuur en Wetenschap. Voor verwerkingen van de Commissie CDHO/CMMBO waar de NVAO verwerker is, wordt een verwerkingsovereenkomst gesloten.

1.3 Doelgroepen

Dit beleidskader is van toepassing op alle bestuurders, medewerkers, tijdelijke werknemers en op alle andere personen die namens de NVAO werken.

Het beleidskader is van toepassing op personen werkzaam in een ondersteunende functie, managementfunctie, juridische functie, staffunctie, beleidsfunctie, of in een andere discipline.

De aard van de werkzaamheden bepaalt het type privacyvraagstukken en afwegingen die voor de betreffende persoon relevant zijn.

1.4 Wet- en regelgeving verwerking van persoonsgegevens

1.4.1 Europese en Nederlandse wet- en regelgeving op het gebied van privacy

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Vanaf dat moment geldt dezelfde privacywetgeving in de hele Europese Unie ².

De AVG is rechtstreeks van toepassing. Daar waar de AVG ruimte laat voor nationale keuzes bij de uitvoering van de AVG, zijn deze ingevuld in de Uitvoeringswet AVG (UAVG) ³.

Naast genoemde wetgeving zijn er aanvullende documenten vanuit het Europees Comité⁴ voor gegevensbescherming waarmee (o.a.) verduidelijking wordt gegeven voor de toepassing van de AVG.

Daarnaast vormt ook de uitleg van de AVG (veelal vastgelegd in beleidsregels) door de Autoriteit Persoonsgegevens (AP) een belangrijke bron voor de naleving van de AVG. De AP gaat ervan uit dat verwerkingsverantwoordelijken als de NVAO de beleidsregels toepassen en adviezen opvolgen, dan wel gemotiveerd afwijken (comply or explain).

Links naar genoemde wetgeving en belangrijke documenten verband houdend met dit beleidskader zijn te vinden in Bijlage 2: Instrumenten.

1.4.2 Specifieke context NVAO

De AVG laat zich voor de NVAO het beste plaatsen vanuit het perspectief van de hoofdprocessen van de NVAO:

- Het primaire proces
- Het personeelsproces
- Het betalingsproces

Het primaire proces

De NVAO is een kwaliteitszorgorganisatie die primair op deskundige en onafhankelijke wijze de kwaliteit van het hoger onderwijs in Nederland en Vlaanderen borgt en die de kwaliteitscultuur binnen de hogeronderwijsinstellingen in Nederland en Vlaanderen bevordert. Zij accrediteert bestaande en nieuwe opleidingen en beoordeelt de kwaliteitszorg van instellingen in het hoger onderwijs.

In Nederland zijn deze taken van de NVAO gebaseerd op de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW, hoofdstuk 5): het accrediteren van bestaande opleidingen, het toetsen van nieuwe opleidingen in het hoger onderwijs en het adviseren van de Minister in specifieke aangelegenheden zoals opgenomen in de WHW. Het is niet uitgesloten dat in de toekomst ook andere wet- en regelgeving als basis dient voor taken van de NVAO.

In Vlaanderen zijn deze taken gebaseerd op de Codex Hoger Onderwijs van oktober 2013. Deze wetgeving dient als uitgangspunt voor alle beoordelingsprocedures in het hoger onderwijs in Vlaanderen.

² Een e-privacy verordening (EPV), waarin zaken als cookieregels en het spamverbod nader worden geregeld, is in ontwikkeling.

³ Verder heeft de rijksoverheid een Handreiking naleving AVG geformuleerd. De NVAO overweegt nog hoe deze handreiking in te zetten.

⁴ European Data Protection Supervisor (EDPS), <https://edps.europa.eu/>

Het personeelsproces

Onder het personeelsproces worden alle verwerkingen geschaard die betrekking hebben op de persoonsgegevens van het eigen personeel van de NVAO.

Het betalingsproces

Onder het betalingsproces behoren alle verwerkingen die gerelateerd zijn aan het overmaken van geld aan leveranciers, commissieleden, personeel en eventuele andere partijen.

N.B. Verwerkingen van persoonsgegevens kunnen in digitale dan wel in papieren vorm plaatsvinden. De Handreiking veilige omgang met persoonsgegevens werkt dit verder uit.

2 NVAO uitgangspunten voor omgang met persoonsgegevens

In hoofdstuk 2 staan de uitgangspunten voor onze omgang met persoonsgegevens en wordt vervolgens toegelicht wat dat betekent voor een medewerker en welke documenten of websites beschikbaar zijn om die uitgangspunten in het dagelijks werk toe te passen. Ieder instrument (document of site) dat onderstreept is, is te vinden in bijlage 2 op alfabetische volgorde.

Er zijn een achttal uitgangspunten opgesteld, waar medewerkers van de NVAO te allen tijde aan dienen te voldoen. Deze uitgangspunten reflecteren de visie van de NVAO ten opzichte van de verwerking van persoonsgegevens ⁵. De uitgangspunten voor gegevensbescherming zijn van toepassing op *alle* verwerkingsactiviteiten met betrekking tot persoonsgegevens binnen de NVAO.

Dit betekent dat alle verwerkingen van persoonsgegevens moeten voldoen aan de volgende acht eisen:

- De NVAO verwerkt alleen persoonsgegevens als voor de verwerking een rechtmatige grondslag aanwezig is en een duidelijk omschreven en gerechtvaardigd doel.
- De NVAO beperkt de verwerking tot die categorieën persoonsgegevens die nodig zijn voor het beschreven doel.
- De NVAO verwerkt persoonsgegevens die accuraat en actueel zijn.
- De NVAO bewaart gegevens niet langer dan noodzakelijk voor het beschreven doel.
- De NVAO is, als dat mogelijk is, open en transparant over de verwerking van persoonsgegevens aan de betrokkene, de samenleving en ketenpartners.
- De NVAO zorgt dat persoonsgegevens die aan ons zijn toevertrouwd, veilig en vertrouwelijk worden verwerkt.
- De NVAO legt verantwoording af over de zorgvuldige verwerking van persoonsgegevens.
- De NVAO respecteert de rechten van de betrokkenen.

Hieronder volgt een nadere instructie per uitgangspunt.

⁵ Het OECD is de organisatie voor economische samenwerking en ontwikkeling. De OECD heeft in 1980 principes opgesteld en in 2013 zijn deze voor het laatst herzien.

2.1 Grondslag en doel

De NVAO verwerkt alleen persoonsgegevens als voor de verwerking een rechtmatige grondslag aanwezig is en een duidelijk omschreven en gerechtvaardigd doel.

Instructies:

- Persoonsgegevens mogen alleen verwerkt worden als een van de rechtmatige grondslagen uit artikel 6 van de AVG aanwezig is. Te denken valt bijvoorbeeld aan: verwerking van persoonsgegevens ter uitvoering van een overeenkomst.
- Persoonsgegevens mogen eveneens alleen verwerkt worden indien de NVAO in het kader van zijn taken verwerkingen verricht, die "noodzakelijk voor de uitvoering van een wettelijke plicht" zijn en "noodzakelijk voor het uitoefenen van een publiekrechtelijke taak of uitoefenen van openbaar gezag". De rechtsgrondslag van een dergelijke taak moet in de WHW of in de Codex Hoger Onderwijs zijn verankerd.
- De grondslag "noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerker of van de verwerkingsverantwoordelijke of van een derde" kan niet worden gebruikt als er sprake is van verwerkingen door overheidsinstanties in het kader van de uitoefening van hun taken. Dit kan wel in beeld komen bij een verwerking in het kader van de bedrijfsvoering (denk bijvoorbeeld aan cameratoezicht rond het gebouw).
- De ongelijke machtsverhouding tussen betrokkene en de overheid staat over het algemeen in de weg aan de eis dat betrokkene de toestemming vrijelijk moet verlenen.
- Een (aanpassing van) verwerking moet steeds worden opgenomen in het Register van verwerkingen. Dit register geeft een beschrijving van verwerkingsactiviteiten. De verantwoordelijke (de NVAO) moet dit op verzoek aan de AP kunnen laten zien. Neem bij een dergelijk verzoek van de AP contact op met de privacy officer die dit in afstemming met de bestuurder verzorgt. Het Register van verwerkingen bevat zelf geen persoonsgegevens.
- Het doel van elke verwerking is concreet en vastgelegd in het Register van verwerkingen. Als een bestand voor meer doelen wordt gebruikt dan wordt dat vermeld in de doelomschrijving. Doelen die duidelijk zijn omschreven maken het voor betrokkene inzichtelijk wat met de gegevens wordt gedaan. Bij verdere verwerking van persoonsgegevens voor een ander doel dan waarvoor de gegevens oorspronkelijk zijn verzameld, wordt altijd beoordeeld of dit nieuwe doel verenigbaar is met het oorspronkelijke doel.
- De NVAO is verplicht een Data Protection Impact Assessment, DPIA (ook wel genoemd Gegevensbeschermingseffect-beoordeling, GEB), uit te voeren bij de ontwikkeling van beleid en regelgeving waaruit verwerkingen van persoonsgegevens voortvloeien. De AP heeft een lijst van verwerkingen opgesteld waarvoor de DPIA verplicht is ⁶. De DPIA is bedoeld om de effecten van de beoogde gegevensverwerking(en) voor betrokkenen te inventariseren en te beoordelen. Op basis van de DPIA kunnen maatregelen worden genomen om de risico's aan te pakken. Gebruik hiervoor het Rijksmodel GEB (PIA) of het model dat in Privacy Nexus is opgenomen. In Privacy Nexus wordt ook het DPIA-register (bij)gehouden.

⁶ <https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667>

- Vragen over het proces, de opzet en uitvoering van de DPIA kun je stellen aan de privacy officer en de Functionaris Gegevensbescherming. Raadpleeg eventueel het document DPIA Proces NVAO of de Memo Quick Scan DPIA om te beoordelen of een DPIA nodig is.

2.2 Doelbinding

De NVAO beperkt de verwerking tot die categorieën persoonsgegevens die nodig zijn voor het beschreven doel.

Instructies:

- Alleen de voor het vooraf en precies omschreven doel noodzakelijke gegevens mogen worden verzameld. Gegevens mogen vervolgens niet verder worden verwerkt als dit onverenigbaar is met dat doel. Persoonsgegevens die niet meer nodig zijn (moeten) worden verwijderd of waar mogelijk geanonimiseerd ⁷. Bij de ontwikkeling van nieuwe (of wijziging van bestaande) producten en diensten wordt met gegevensbescherming rekening gehouden.
- Verwerk niet meer gegevens dan die aantoonbaar noodzakelijk zijn voor het doel van de verwerking (*dataminimalisatie*). Bedenk waarom je gegevens voor die specifieke verwerking nodig hebt en of je daadwerkelijk alle gegevens nodig hebt.
- Nieuwe systemen worden geconfigureerd op een zodanige wijze dat alleen de voor het specifieke verwerkingsdoel noodzakelijke gegevens worden verwerkt. Privacy moet dus bij het ontwerp van een (nieuw) automatiseringssysteem als uitgangspunt worden genomen. (*privacy by design*).
- Ga bij het ontwikkelen van beleid, processen (en systemen) altijd uit van de meest privacybeschermende instellingen (*privacy by default*).
- Raadpleeg bij het ontwikkelen en uitwerken van beleid, processen en systemen de Handleiding Privacy by Design & by Default om meer zicht te krijgen op privacyvriendelijk ontwerp waarin de bescherming van persoonsgegevens is ingebouwd ⁸.

2.3 Accuraat en actueel

De NVAO verwerkt persoonsgegevens die accuraat en actueel zijn. Dit betekent onder meer dat er sprake is van zorgvuldig beheer van gegevens (*betrouwbaarheid en integriteit*) en dat het voor betrokkenen mogelijk is om verzoeken met betrekking tot rectificatie van onjuiste persoonsgegevens in te dienen (*rechten van betrokkenen*).

⁷ De AVG is niet van toepassing op anonieme gegevens omdat deze gegevens niet terug te voeren zijn op een geïdentificeerde of identificeerbare natuurlijke persoon. Anonimisering is versleuteling die onomkeerbaar is, het niet meer mogelijk om deze later weer met personen in verband te brengen. Bij pseudonimisering kunnen anonieme gegevens met de juiste sleutel inzichtelijk gemaakt worden, waardoor herleiding naar natuurlijke personen weer mogelijk is. De AVG is wel van toepassing op gepseudonimiseerde gegevens.

⁸ https://www.cip-overheid.nl/media/1136/20170507-handleiding-privacy-by-design-v3_0.pdf

Instructies:

- Zorg dat de juistheid en actualiteit van de persoonsgegevens zoveel mogelijk gewaarborgd is door periodieke controles en/of controle op bestaande gegevens of input, bijvoorbeeld wanneer panelleden opnieuw zitting nemen in een panel.
- Zorg dat het mogelijk is om gegevens aan te passen daar waar zij onjuist, onvolledig of verouderd zijn.
- Raadpleeg desgewenst Protocol Rechten Betrokkenen.

2.4 Bewaarbeperking

De NVAO bewaart gegevens niet langer dan noodzakelijk voor het beschreven doel of zolang als bepaald door een specifieke wet.

Instructies:

- De NVAO heeft maximale bewaartermijnen bepaald en geïmplementeerd voor alle persoonsgegevens waarover de organisatie mag beschikken. Nadat een bewaartermijn is verstreken, moeten de persoonsgegevens verwijderd worden of geanonimiseerd⁹.
- Persoonsgegevens kunnen meerdere doelen dienen. Houd hiermee rekening bij het opstellen van de bewaartermijnen.
- Bewaar persoonsgegevens niet langer dan noodzakelijk voor de doelen van de verwerking.
- Stel bewaartermijnen vast conform de Memo Bewaartermijn Persoonsgegevens in de AVG.
- Wis gegevens wanneer deze niet langer noodzakelijk zijn voor het verwerkingsdoel.
- Raadpleeg desgewenst de Handreiking Bewaren van e-mail Rijksoverheid en de Selectielijst van de NVAO.

2.5 Open en transparant

De NVAO is, als dat mogelijk is, open en transparant over de verwerking van persoonsgegevens aan de betrokkene, de samenleving en ketenpartners. Een betrokkene dient te weten wat er met zijn persoonsgegevens gebeurt. De informatie over de verwerking en de omgang met de gegevens en over de rechten van betrokkene dient eenvoudig toegankelijk en begrijpelijk te worden aangeboden. Dit gebeurt in een interne en een (of meerdere) externe privacyverklaring(en) en een cookieverklaring.

Instructies:

- De NVAO verstrekt de vereiste informatie over onze verwerkingsactiviteiten voor o.a. studenten en overige burgers via de Privacyverklaring NVAO en de Cookieverklaring op www.nvao.net.
- De NVAO verstrekt vereiste informatie voor bestuursleden en medewerkers (incl. de medewerkers van CDHO en CMMBO) via de Privacyverklaring medewerkers op intranet of Sharepoint.

⁹ Zie voetnoot 7

- Zowel de Privacyverklaring NVAO (extern), de Cookieverklaring en de Privacyverklaring medewerkers (intern) worden periodiek door het privacy office op actualiteit gecontroleerd.
- Raadpleeg ook desgewenst de Handreiking Veilige omgang met persoonsgegevens of de Personeelsregeling.

2.6 Veilig en vertrouwelijk

De NVAO zorgt dat persoonsgegevens die aan ons zijn toevertrouwd, veilig en vertrouwelijk worden verwerkt.

Instructies:

- De NVAO is verplicht (op basis van wet- en regelgeving) om passende technische en organisatorische maatregelen te treffen om persoonsgegevens een passend beschermingsniveau te bieden tegen ongeautoriseerde verwerkingen. De NVAO heeft hiertoe een Handreiking Veilige omgang Persoonsgegevens opgesteld.
- De NVAO verstrekt alleen toegang tot persoonsgegevens aan die mensen die toegang tot de gegevens nodig hebben en die toestemming hebben om gegevens verder te verwerken.
- Datalekken moeten zoveel mogelijk worden voorkomen. Een datalek is een inbreuk op de beveiliging van de persoonsgegevens die leidt tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking of toegang tot gegevens.
- Een datalek dat een risico voor de rechten van betrokkene inhoudt moet binnen 72 uur aan de Autoriteit Persoonsgegevens (AP) worden gemeld en soms ook aan betrokkene. Hiervoor is het Protocol datalekken NVAO opgesteld. Raadpleeg bij een (vermeend) datalek de privacy officer.
- Via de e-mail worden veel bestanden uitgewisseld en dus ook vaak persoonsgegevens. Het is belangrijk om een passend beschermingsniveau toe te passen bij het versturen van dergelijke gegevens. Bij het versturen van bestanden met persoonsgegevens is het passend om deze gegevens versleuteld te versturen naar de ontvanger. Op die manier wordt het risico verkleind dat er per ongeluk bestanden naar de verkeerde ontvanger worden gestuurd. Als het nodig is om gegevens versleuteld te versturen naar de ontvanger, verstuur deze bijvoorbeeld door middel van een versleutelde omgeving.
- De NVAO en in het bijzonder het privacy office houdt een register bij van datalekken en beveiligingsincidenten.
- Raadpleeg eventueel het Autorisatiebeleid en het Beveiligingsbeleid.

2.7 Verantwoordingsplicht

De NVAO legt verantwoording af over de zorgvuldige verwerking van persoonsgegevens.

Instructies:

- De NVAO neemt passende maatregelen om de bescherming van persoonsgegevens te waarborgen. Aan de hand van documentatie kan de NVAO aantonen dat de privacyregels worden nageleefd. Evaluatie, monitoring en logging van de maatregelen

maakt ook onderdeel uit van de verantwoording. Deze verantwoordingsplicht (*accountability*) staat centraal in het nieuwe wettelijk privacykader.

- Het privacy office van de NVAO beheert een Register van verwerkingen. In dat register staat informatie over de gegevens die worden verwerkt. De persoonsgegevens zelf staan niet in het register, wel welke categorieën persoonsgegevens er worden verwerkt.
- Wijzigingen in verwerkingen moeten door medewerkers en/of leden van het managementteam aan de privacy officer worden doorgegeven.
- De managers van de afdelingen Nederland en Vlaanderen hebben een zelfstandige verantwoordelijkheid om bij nieuwe verwerkingen (activiteiten/andere ICT systemen) de privacy officer en de FG op de hoogte te stellen.
- De NVAO vergewist zich ervan dat derde partijen behoorlijk en zorgvuldig met persoonsgegevens omgaan. Dit hoeft niet noodzakelijkerwijs te gaan over partijen waarmee een verwerkersovereenkomst mee afgesloten dient te worden. Denk hierbij aan de Arbodienst die een eigen verwerkingsverantwoordelijkheid heeft. Waar nodig wordt een verwerkingsovereenkomst gesloten; deze wordt opgenomen in het Register Verwerkingsovereenkomsten (in de tool Nexus).
- Raadpleeg Juridische Zaken bij vragen. Een Format verwerkersovereenkomst en Checklist verwerkersovereenkomst (model Privacy Company) zijn beschikbaar.

2.8 Respect

De NVAO respecteert de rechten van de betrokkenen.

Instructies:

- De NVAO richt systemen, processen en de interne organisatie zodanig in dat op de juiste manier gehoor wordt gegeven aan verzoeken van betrokkenen omtrent persoonsgegevens.
- De NVAO hanteert een Protocol Rechten Betrokkenen, waarin de (belangrijkste) rechten van betrokkenen zijn/worden geformuleerd, zoals inzage, rectificatie, wissen, overdracht en beperking van verwerking. Ook wordt in dit protocol vermeld hoe een bepaald verzoek wordt behandeld en waar een betrokkene rekening mee kan houden. Dit protocol heeft interne werking en is bedoeld om handvaten te bieden voor het Privacy Office. Voor betrokkenen kan verwezen worden naar de diverse privacyverklaringen.
- De NVAO kan gebruik maken van een model voor de beantwoording van inzageverzoeken of van andere modellen om aan verzoeken te voldoen.
- In de diverse privacyverklaringen worden o.a. de rechten van betrokkenen ten aanzien van hun persoonsgegevens omschreven. In de diverse privacyverklaringen wordt omschreven voor wie de betreffende privacyverklaring geldt.
- Alle betrokkenen (intern en extern) kunnen bij de Autoriteit Persoonsgegevens (AP) een klacht indienen over de manier waarop de NVAO met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.

3 Privacy governance

3.1 Inleiding

Doel van dit hoofdstuk over de privacy governance is inzicht te geven in de verantwoordelijkheden op het gebied van de privacybescherming binnen de NVAO. De governancestructuur helpt de NVAO om zorgvuldig met persoonsgegevens om te gaan en verantwoording af te kunnen leggen over genomen beslissingen. Een robuuste beheersorganisatie is van belang voor de implementatie en handhaving van de principes en doelstellingen uit het privacybeleid.

Omgevingsveld

De NVAO is een zelfstandig bestuursorgaan en valt onder de politieke verantwoordelijkheid van het *Comité van Ministers*. Hoewel de NVAO een zelfstandig bestuursorgaan is, blijft het Comité van Ministers politiek verantwoordelijk voor compliance met wet- en regelgeving en dus ook de AVG.

De *Autoriteit Persoonsgegevens* (AP) is de toezichthoudende autoriteit met betrekking tot het voldoen aan de vereisten van de AVG. Wanneer betrokkenen klachten hebben over hoe de NVAO omgaat met persoonsgegevens, kunnen zij terecht bij de AP.

De *Nationale Ombudsman* kan eventueel ook nog een bemiddelende rol spelen tussen de NVAO en personen waarvan de NVAO gegevens verwerkt.

3.2 Privacy verantwoordelijkheden rollen en taken

Privacy gaat de gehele NVAO aan en ziet ook op de gehele organisatie. Met elkaar werken we aan de naleving van het privacybeleid en draagt de NVAO als bestuursorgaan hiervoor verantwoordelijkheid.

Welke organen en personen dragen bij aan het privacybeleid of spelen een rol?

1. AB Algemeen Bestuur
2. DB Dagelijks Bestuur
3. DN Directeur Nederland
4. DV Directeur Vlaanderen
5. FG Functionaris voor gegevensbescherming
6. PO Privacy office
7. CISO/IM Chief Information Security Officer of Informatiemanager
8. AHN Afdelingshoofd Nederland
9. HR Hoofd HR
10. HF Hoofd Financiën
11. RB Relatiebeheer
12. Com Communicatie
13. OR Ondernemingsraad
14. Mw medewerker

N.B. 3, 4, 8 en 10 vormen samen het Management Team, ofwel MT

In het RASCI model (zie Bijlage 3) is uitgewerkt wie verantwoordelijk is voor welk onderdeel van de AVG. Meer in het algemeen staat hieronder beschreven bij wie, welke rollen en taken binnen de NVAO bij de uitvoering van de AVG zijn belegd.

De lijn: AB, DB, MT

Overeenkomstig de mandaatstructuur binnen de NVAO zijn het bestuur, de directeuren, het afdelingshoofd NL, en de hoofden HR en Financiën verder verantwoordelijk voor de strategische visie, de risicobeheersing en voor het borgen van de aantoonbare naleving van de wet- en regelgeving op het terrein van privacybescherming. Het MT is een overlegorgaan van de Directeur Nederland, Directeur Vlaanderen, Afdelingshoofd Nederland en Hoofd Financiën, waarbij ook het Hoofd HR aansluit. Beslissingen over de dagelijkse gang van zaken binnen de NVAO worden in het MT besproken. Vaak volgt hieruit een formele beslissing. Deze beslissing is dan (mandaattechnisch) toe te rekenen aan de Directeur Nederland.

De (niet met toezicht belaste) specialisten: PO, Chief Information Security Officer (CISO/IM) en HR

Naast een privacy officer heeft de NVAO een CISO (en/of Informatiemanager). De privacy officer en de CISO/IM adviseren, ondersteunen en controleren de directie, het bestuur en de medewerkers bij privacy aspecten. Ook bepaalde beleidstaken en het organiseren van interne risicoanalyses behoren tot hun takenpakket. Primair is de privacy officer het aanspreekpunt voor de uitleg van de AVG binnen de NVAO en bij de implementatie en uitvoering van de AVG.

Daarnaast heeft HR een rol als het gaat om de zorgvuldige omgang met persoonsgegevens. HR is het eerste aanspreekpunt bij personeelsgerelateerde vragen van medewerkers over de AVG.

Taakomschrijvingen meer specifiek van de FG, het PO en de CISO/IM:

Functionaris Gegevensbescherming (FG) ¹⁰

De NVAO heeft

een interne FG aangesteld overeenkomstig artikel 37 e.v. van de AVG. De FG rapporteert aan de voorzitter van het bestuur. In de AVG is de rol van de FG als volgt beschreven:

- informeren en adviseren van het lijnmanagement over hun verplichtingen uit hoofde wet- en regelgeving in het kader van privacy;
- toezien op de naleving van de relevante wetgeving, het privacybeleid en de inrichting van de interne privacy organisatie;
- advies leveren bij een DPIA, zowel de inhoudelijke beoordeling als de naleving van de voorgenomen beheermaatregelen;
- samenwerken met de AP, de centrale toezichthouder, in het geval van onderzoek;
- aanspreekpunt voor betrokkenen (burgers en medewerkers) voor alle aangelegenheden bij de verwerking van hun persoonsgegevens.

Jaarlijks kan de FG een werkplan privacy office opstellen in het kader van zijn toezichthoudende werkzaamheden.

Privacy office (PO)

De NVAO heeft een privacy officer die de volgende taken verricht:

- beheert het privacybeleid en kan op verzoek van de directie, het bestuur of uit eigen beweging een voorstel tot aanpassing van het beleid doen;
- zorgt voor de dagelijkse afhandeling van privacy aangelegenheden voor de NVAO;
- beheert het register van verwerkingsactiviteiten;

¹⁰ <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/functionaris-gegevensbescherming-fg>

- stelt de jaarplanning op;
- fungeert als vraagbaak voor het management ten aanzien van het verzamelen, registreren en leveren van persoonsgegevens. Hij raadpleegt indien nodig de Functionaris Gegevensbescherming of externe adviseurs over complexere verwerkingen en relaties met verwerkers.
- adviseert het management bij de analyse van mogelijke risico's die samenhangen met de verwerking van persoonsgegevens.

De NVAO heeft een privacy office¹¹ dat de volgende taken verricht: ondersteunt de NVAO in het naleven van de eisen uit dit privacybeleid en de privacywetgeving.

Chief Information Security Officer (CISO) en/of Informatiemanager (IM)

Het onderwerp privacy en gegevensbescherming heeft een multidisciplinair karakter. Het vraagt om een zorgvuldige afstemming met de experts van juridische zaken, ICT, beveiliging, communicatie, de privacy en de FG.

De CISO/IM heeft onder meer als taak:

- Opstellen informatievoorziening strategie en beleid en vertalen naar de techniek;
- Opstellen en actualiseren informatiebeveiligingsbeleid en de daaruit voortvloeiende plannen;
- Inrichten van de informatiebeveiligingsorganisatie en het coördineren en afhandelen van beveiligingsincidenten;
- Ophalen en vertalen van externe ontwikkelingen (wetgeving, technologie, bedrijfsvoering) naar consequenties en aanpassingen voor de informatievoorziening;
- Monitoren van relevante risico's voor de organisatie;
- Monitoren en borgen van de eisen en architectuur voor informatiebeveiliging en het consequent toepassen van Security-by-Design en Privacy-by-Design.

De CISO/IM ondersteunt de afdelingen Nederland en Ondersteuning en is in eerste instantie verantwoordelijk voor de informationele privacy. De CISO/IM ondersteunt en adviseert de NVAO bij privacyvraagstukken. De CISO/IM helpt onder meer door het geven van (zo mogelijk) advies op maat, het opbouwen van de noodzakelijke kennis over privacy wet- en regelgeving, het toepassen hiervan en het (mede-)ontwikkelen van producten zoals informatiebeleid en privacy convenanten.

Wat is de rol van de OR¹² bij privacyvraagstukken?

De ondernemingsraad vertegenwoordigt het personeel van de NVAO en beschermt hun belangen. De ondernemingsraad heeft daarvoor verschillende rechten en bevoegdheden, zoals het recht op informatie, het adviesrecht, het instemmingsrecht en het initiatiefrecht. Met name het adviesrecht, instemmingsrecht en het initiatiefrecht spelen een rol bij de uitvoering van de AVG. Artikel 27 WOR

Het kan zijn dat er nieuwe technische maatregelen worden getroffen om te voldoen aan de AVG. Denk bijvoorbeeld aan technische maatregelen om persoonsgegevens te beveiligen of om ervoor te zorgen dat alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor het verwerkingsdoel.

Op grond van de Wet op de Ondernemingsraden (WOR) dient een besluit tot het invoeren of wijzigen van een technologische voorziening ter advies aan de ondernemingsraad te worden voorgelegd. Dus als de NVAO wil over gaan tot de aanschaf van nieuwe ICT ter beveiliging van de persoonsgegevens, dan heeft de OR adviesrecht.

¹¹ Juridische Zaken fungeert als Privacy Office op het moment van inwerkingtreding van dit beleid; eventuele wijziging wordt gecommuniceerd.

¹² <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-uitkering/ondernemingsraad>

Een besluit tot vaststelling, wijziging of intrekking van een regeling over het verwerken van, alsmede de bescherming van de bij de NVAO werkzame personen is instemmingsplichtig. Het moet dus gaan om een regeling die tot doel heeft persoonsgegevens te verzamelen, bewaren, gebruiken, verstrekken of beveiligen. Dit geldt onder meer voor de vaststelling van dit privacybeleid en voor het melden van een datalek waarbij persoonsgegevens zijn betrokken.
>F

De ondernemingsraad kan tenslotte gebruikmaken van haar initiatiefrecht om voorstellen te doen voor (een aanpassing van) het privacybeleid.

3.3 Privacy overlegstructuren

Privacy moet als vast onderdeel opgenomen zijn op de agenda's van de reguliere overleggen tussen JZ/Directie alsook tussen JZ/Directie en HRM, Directie/Financiën, Dir/com, Dir/ICT en Dir/ICT-stuurgroep. Er is tenslotte ook nog een vast maandelijks overleg tussen het privacy office en de Functionaris Gegevensbescherming.

De NVAO doet daarnaast mee aan overleggen van KleinLef organisaties op het gebied van privacy om de kennis omtrent privacy te delen en elkaar te helpen om beleid omtrent privacy te ontwikkelen.

3.4 Sturing, regie en toezicht

Periodiek voert de NVAO met behulp van de tool in Privacy-Nexus self-assessments uit, waaruit blijkt wat de stand van zaken is met betrekking tot privacy.

De FG ziet toe op de naleving van de relevante wetgeving, het privacybeleid en de inrichting van de interne privacy organisatie.

Interne toezichtsorganen: FG en OR

Tenslotte kent de NVAO een Functionaris Gegevensbescherming (FG) en de Ondernemingsraad (OR). Zij zijn vanwege hun specifieke rollen en wettelijke taken bij aspecten van de privacy van de NVAO betrokken.

Externe toezichthouders, zoals de Autoriteit Persoonsgegevens (AP) en al dan niet ingehuurde auditors kunnen de inregeling en uitvoering van de AVG controleren. Het is de eigen verantwoordelijkheid van de NVAO om intern toezicht te houden op de waarborging van privacybescherming, los van eventuele externe audits en evaluaties.

3.5 Privacy trainingen en bewustwording

Alle medewerkers krijgen bij hun aanstelling een korte introductie AVG van de PO/FG. De tekst van de eed/belofte is in de Personeelsregeling opgenomen; hierin ligt de geheimhouding t.a.v. AVG besloten.

Daarnaast vinden reguliere bewustwordingsacties plaats, door minimaal één keer per jaar aandacht voor een privacy onderwerp vanuit het privacy office en minimaal één bureaubijeenkomst per jaar over een AVG onderwerp. Daarnaast worden medewerkers ook geïnformeerd over de AVG en privacy, doordat dit onderwerp een integraal onderdeel uitmaakt van de besprekingen van het Dagelijks Bestuur. De verslagen hiervan zijn voor medewerkers te raadplegen.

4 Slot

Met dit privacybeleid brengt de NVAO in kaart welke maatregelen er zijn genomen om de persoonsgegevens van medewerkers en externen, waaronder o.a. panelleden, secretarissen en studenten, te beschermen. Daarnaast geeft het beleid inzicht in de wijze waarop de verantwoordelijkheden op grond van de AVG zijn belegd bij de NVAO. Ook is per uitgangspunt vastgelegd welke instructies er zijn en welke documenten geraadpleegd kunnen worden. Hiermee wordt voldaan aan belangrijke verplichtingen op grond van de AVG, zoals het inrichten en bijhouden van een Register van verwerkingen, de wijze waarop omgegaan wordt met datalekken, het houden van een DPIA, het opstellen van een interne en externe privacyverklaring en de wijze waarop rechten van betrokkenen zijn georganiseerd. > F

4.1 Beheer

Het privacy office van de NVAO is verantwoordelijk voor het beheer van dit privacy beleidskader.

De instrumenten en dit beleidskader zijn levende documenten die periodiek (moeten) worden geactualiseerd. Algemene vragen over dit beleid of suggesties tot wijziging of toevoeging aan het beleid, kunnen worden gericht aan het privacy office van de NVAO (privacy@nvaio.net).

4.2 Vaststelling

Dit privacybeleid is voor het eerst vastgesteld op 15 maart 2021 door het Algemeen Bestuur van de NVAO.

4.3 Wijzigingen en evaluatie

Privacybeleid is dynamisch beleid. Nieuwe ontwikkelingen volgen elkaar op en ook de organisatie zelf zal steeds in ontwikkeling zijn. Dit betekent dat het privacybeleid ook met regelmaat bijgesteld zal moeten worden. Dit beleid wordt periodiek herzien en bijgewerkt. De volgende tabel toont de (concept)versie geschiedenis van dit privacy beleid. Evaluatie vindt in beginsel ieder jaar plaats, tenzij anders bepaald.

Datum	Opmerkingen	Versie
16-10-2019	1 ^{ste} concept beleidsdocument	0.1
27-07-2020	Concept tbv FG	0.2
2-11-2020	Concept tbv Luut	0.3
28-1-2021	Concept tbv DB	0.4
16-2-2021	Goedkeuring cpt door DB	16-2-2021
15-3-2021	Goedkeuring AB en mandatering DB en ondermandaat PO	15-3-2021
15-4-2021	Aanvulling data en technische aanpassingen (IM vervangen door CISO/privacyverklaringen hernoemd, cookieverklaring toegevoegd en protocol rechten betrokkenen hernoemd)	15-4-2021
22-4-2021	Naast CISO de IM gezet (RASCI 1 kolom voor gezamenlijke taken)	22-4-2021
7-6-2021	Regeling Rechten Betrokkenen naam gewijzigd; interne werking	7-6-2021
10-6-2021	Naam oud-voorzitter verwijderd	10-6-2021

Bijlage 1: Begrippen

Wat zijn persoonsgegevens?

Niet alle data of gegevens zijn per definitie persoonsgegevens. Persoonsgegevens betreft alle informatie met betrekking tot een geïdentificeerde of identificeerbare natuurlijke persoon (de "betrokkene").

De betrokkene hoeft geen direct geïdentificeerd individu te zijn, maar zodra een individu uit een groep kan worden onderscheiden, zijn de gegevens persoonsgegevens. Het is dus niet altijd nodig om de naam te weten van de persoon in kwestie om te spreken van persoonsgegevens.

Alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare persoon moeten als persoonsgegevens worden beschouwd. Enkel transactiegegevens zijn bijvoorbeeld op zichzelf geen direct identificeerbare gegevens, maar worden persoonsgegevens wanneer deze verband houden met een geïdentificeerde of identificeerbare persoon, bijvoorbeeld omdat deze is gekoppeld aan een naam, een e-mailadres of een telefoonnummer.

De AVG heeft een speciaal regime voor bijzondere categorieën persoonsgegevens. Dit betreffen persoonsgegevens waaruit de raciale of etnische afkomst, politieke opvattingen, religieuze of filosofische overtuigingen blijken, lidmaatschap van een vakvereniging, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie, gezondheids- of medische gegevens, gegevens over iemands seksleven of seksuele geaardheid.

Strafrechtelijke persoonsgegevens zijn persoonsgegevens die te maken hebben met strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen. Hieronder vallen zowel veroordelingen als mogelijk gegronde verdenkingen. Dit wil zeggen dat er concrete aanwijzingen zijn dat iemand een strafbaar feit heeft gepleegd. Een voorbeeld hiervan is een opgestelde zwarte lijst van frauderende klanten bij een financiële instelling. Onder de AVG gelden speciale regels voor het verwerken van strafrechtelijke gegevens.

De verwerking, het verzamelen of gebruiken, van gevoelige persoonsgegevens, is verboden, tenzij een uitzondering op het algemene verbod van toepassing is. Het verzamelen en gebruiken van dergelijke gegevens zal daarom zoveel mogelijk worden vermeden. Vermijd ook het verzamelen en gebruik van gegevens van gevoelige groepen, zoals kinderen / minderjarigen, gehandicapten en ouderen, tenzij hiervoor duidelijk toestemming is gegeven door de bevoegde persoon.

Hieronder volgen voorbeelden van gegevens die over het algemeen als persoonsgegevens worden beschouwd:

Voornaam en / of initialen en achternaam	Financiële gegevens
E-mailadres	Betaling of transactiegegevens
Telefoonnummer	Rijbewijs
Foto	Strafrecht ketennummer
Geboortedatum / geboorteplaats	Identificatienummer werknemer
IP-adres	Werknemers informatie
Uitkomsten functioneringsgesprekken	Medische informatie
Burgerservicenummer	Biometrische gegevens
Unique Device Identifiers	MAC-adressen

Wat is een betrokkene?

De betrokkene is de persoon van wie persoonsgegevens worden verwerkt.

Wat is een verwerking?

Het 'verwerken van persoonsgegevens' of een 'verwerking van persoonsgegevens' betreft alle handelingen die men met persoonsgegevens kan verrichten. Denk hierbij aan het verzamelen, vastleggen, raadplegen, opvragen, ordenen, structureren, opslaan, bewerken of wijzigen, verstrekken en combineren. Ook het wissen of vernietigen van gegevens is een verwerking van persoonsgegevens.

Wat is een verwerkingsverantwoordelijke?

De verwerkingsverantwoordelijke is de natuurlijke persoon of rechtspersoon die (alleen of tezamen met anderen) bepaalt welke persoonsgegevens worden verzameld, waarom persoonsgegevens worden verwerkt (doel) en hoe persoonsgegevens worden verwerkt (middelen). Wanneer partijen gezamenlijk het doel en de middelen vaststellen voor de verwerking van persoonsgegevens dan spreken we van een gezamenlijke verantwoordelijkheid.

Wat is een verwerker?

Een verwerker is de natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Het gaat om derde partijen die voor de verwerkingsverantwoordelijke werken. Een verwerker handelt onder de verantwoordelijkheid van de verwerkingsverantwoordelijke en naar diens instructies, maar er is geen hiërarchische relatie (medewerkers zijn geen verwerkers). Daarnaast heeft de verwerker geen zeggenschap over de verwerkingen en mag de gegevens niet voor eigen doelen gebruiken.

N.B. BIJLAGE 2 IS EEN LOS DOCUMENT, HET LOSSE DOCUMENT IS LEIDEND.
BIJ VERSPREIDING VAN DIT PRIVACY BELEIDSKADER MOET DE MEEST RECENTE BIJLAGE
2 INSTRUMENTEN (ZONDER DE STATUS & PLANNING) WORDEN TOEGEVOEGD.

Bijlage 2: Instrumenten d.d. 27 mei 2021

Wet- en regelgeving

AVG Algemene Verordening Gegevensbescherming

UAVG Uitvoeringswet Algemene Verordening Gegevensbescherming

Websites

EDPS European Data Protection Supervisor, <https://edps.europa.eu/>

AP Autoriteit Persoonsgegevens, <https://autoriteitpersoonsgegevens.nl/>

Nr	Naam document	Vindplaats in H2 privacybeleid
1	Autorisatiebeleid	2.6
2	Beleid voor toezicht op logging	2.7
3	Beveiligingsbeleid	2.6
4	Checklist verwerkersovereenkomst	2.7
5	Cookieverklaring	2.5
6	DPIA Proces NVAO	2.1
7	DPIA-register	2.1
8	Format verwerkersovereenkomst	2.7
9	Handleiding Privacy by Design (versie 3.0 CIP)	2.2
10	Handreiking Bewaren van e-mail Rijksoverheid	2.4
11	Handreiking Veilige omgang met persoonsgegevens	2.5 en 2.6
12	Memo Quick Scan DPIA	2.1
13	Privacy Beleidskader	=document
14	Privacyverklaring medewerkers	2.5 en 2.8
16	Privacyverklaring NVAO/ CDHO/CMMBO	2.5 en 2.8
17	Protocol datalekken NVAO	2.6
18	Protocol Rechten Betrokkenen	2.3 en 2.8
19	Register datalekken en beveiligingsincidenten	2.6
20	Register van verwerkingen	2.1 en 2.7
21	Register Verwerkingsovereenkomsten	2.7
22	Rijksmodel GEB PIA	2.1
23	Selectielijst van de NVAO	2.4

Bijlage 3: RASCI model

Colofon

Privacy Beleidskader

Maart 2021

Samenstelling: NVAO



Nederlands-Vlaamse Accreditatieorganisatie
Accreditation Organisation of the Netherlands and Flanders

Parkstraat 83 · 2514 JG Den Haag
P.O. Box 85498 · 2508 CD The Hague
The Netherlands

T +31 (0)70 312 23 00
E info@nvao.net
www.nvao.net

1a

Privacybeleid NVAO
Concept 02
Concept 01

27 juli 20202019

Privacy Beleidskader
Nederlands Vlaamse Accreditatie Organisatie

Datum: 27072020
Status: conceptversie27072020

5.1 lid 2 e
Artikel 5.1 lid 2 e
Directeur Nederland
Voorzitter Algemeen Bestuur

Artikel 5.1 lid 2 e
Artikel 5.1 lid 2 e
Luut Kroes
Anne Flierman

Inhoud

Voorwoord

1. Privacy beleidskader
 - 1.1 Doel
 - 1.2 Scope NVAO /CDHO/CMBO
 - 1.3 Doelgroepen
 - 1.4 Verantwoordelijkheden beleidskader
 - 1.5 Wet- en regelgeving verwerking van persoonsgegevens
2. NVAO uitgangspunten voor een verantwoorde omgang met persoonsgegevens
3. Privacy governance
 - 3.1 Inleiding
 - 3.2 Privacy verantwoordelijkheden rollen en taken
 - 3.3 Privacy overlegstructuren
 - 3.4 Sturing regie en toezicht
 - 3.5 Privacytrainingen en bewustwording
4. Slot
 - 4.1 Wijzigingen

Bijlage 1 Terminologie en Achtergrond

Bijlage 2 RASCI model

Bijlage 3 Handreikingen(checklist, leidraad, stappenplan etc.) voor toepassen uitgangspunten omgang met persoonsgegevens

Voorwoord

De Nederlands-Vlaamse Accreditatieorganisatie (NVAO) is een kwaliteitszorgorganisatie die op deskundige en onafhankelijke wijze de kwaliteit van het hoger onderwijs in Nederland en Vlaanderen borgt en die de kwaliteitscultuur binnen de instellingen voor hoger onderwijs in Nederland en Vlaanderen bevordert. Zij accrediteert bestaande en nieuwe opleidingen en beoordeelt de kwaliteitszorg van instellingen in het hoger onderwijs. Daarmee is de NVAO bewaker van de kwaliteit van het hoger onderwijs. De besluiten van de NVAO leiden tot erkenning van diploma's en titels en waar van toepassing tot bekostiging van opleidingen. De NVAO baseert haar beoordeling op advies van erkende deskundigen.

De NVAO werd in 2003 opgericht bij Verdrag tussen Nederland en Vlaanderen. De taken van de NVAO zijn in wetgeving vastgelegd. De NVAO wil er toe bijdragen dat de kwaliteit van het hoger onderwijs in Vlaanderen en Nederland erkend wordt als internationaal aan de maat, maatschappelijk relevant en het vertrouwen geniet van studenten, werkgevers en de samenleving. Binnen de opdracht die in het accreditatieverdrag tussen Nederland en Vlaanderen aan de NVAO is toegekend, wil zij de kwaliteit van het hoger onderwijs borgen, verbeteringen stimuleren en een kwaliteitscultuur bevorderen.

Om dit werk goed te kunnen doen is verwerking van persoonsgegevens van medewerkers en de contactpersonen van ketenpartners en burgers noodzakelijk. De privacy van contactpersonen en relaties is erg belangrijk voor de NVAO en we hechten dan ook veel belang aan een correcte verwerking en gebruik van persoonsgegevens. De bescherming van persoonsgegevens is immers een grondrecht. De NVAO is verantwoordelijk voor de aantoonbare zorgvuldige omgang met persoonsgegevens.

De NVAO is een zelfstandig bestuursorgaan en opgericht naar Nederlands publiekrecht met de zetel in Den Haag. De NVAO valt onder verantwoordelijkheid van het Comité van Ministers.

Dit privacy beleidskader richt zich tot iedereen die werkzaamheden verricht voor de NVAO. In het privacy beleidskader wordt uitgelegd hoe de NVAO aantoonbaar zorgvuldig omgaat met persoonsgegevens, wat daarbij de uitgangspunten zijn en wat de rol van de medewerker is bij de bescherming van persoonsgegevens.¹

Datum Ondertekening

Anne Flierman

Voorzitter Algemeen Bestuur NVAO

¹ Voor een beknopte uitleg van begrippen (als persoonsgegevens en verwerking) zie bijlage 1.

1. NVAO Privacy beleidskader

Op het werk van het Nederlands Vlaamse Accreditatie Organisatie (NVAO) is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Daarnaast heeft de NVAO te maken met bijzondere wetgeving, waarin een grondslag voor verwerking van gegevens kan liggen. Denk hierbij bijvoorbeeld aan de gegevens die de NVAO nodig heeft van panelleden om hun deskundigheid voor deelname aan een panel te kunnen beoordelen. Voor de Afdeling Vlaanderen is dit geregeld in het Decreet, voor de Afdeling Nederland is dit vastgelegd in de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW).

Het NVAO Privacy beleidskader geeft aan waar de NVAO op het vlak van gegevensbescherming voor staat en wat de uitgangspunten voor de omgang met persoonsgegevens zijn. Met dit kader wil de NVAO ervoor zorgen dat de privacybescherming in lijn is met de wettelijke vereisten en die aansluit of geïntegreerd wordt bij de bestaande processen en systemen van de NVAO.

Bij alle uitgangspunten wordt steeds verwezen naar praktische ondersteunende instrumenten (checklists, stappenplan, procedures) van de NVAO dan wel (voor zover niet aanwezig) van OCW.

De uitleg van een aantal belangrijke begrippen uit de AVG is opgenomen in Bijlage 1.

1.1 Doel

Doel van dit beleidskader is een omgeving te creëren waarin elke medewerker van de NVAO:

- zijn of haar verantwoordelijkheid **1** kent als het gaat om privacy en het verwerken van persoonsgegevens,
- in staat is om het juiste beleid en de juiste procedures te volgen,
- contact kan opnemen met de juiste personen wanneer er vragen zijn.



1 Art 5.1 lid 2 e

Toevoegen: "en rechten" (koppeling naar interne privacyverklaring)

1.2 Scope

Het privacy beleidskader is bestemd voor de NVAO in zijn geheel. Alle handelingen binnen de NVAO met betrekking tot persoonsgegevens van burgers, medewerkers en contactpersonen vallen binnen het bereik van dit beleidskader.

CMMBO en CDHO

Deze organisaties hebben zelfstandige taken en verantwoordelijkheden. Er is een nauwe samenwerkingsrelatie tussen de NVAO en de CMMBO/CDHO. Niet alleen zitten de organisaties fysiek in het pand bij de NVAO, de ondersteuning van CDHO en CMBO is in dienst van de NVAO. Bovendien maken de drie organisaties gezamenlijk gebruik van de afdeling Ondersteuning van de NVAO (waaronder ICT, financiën en personeelszaken). Het privacybeleid van de NVAO omvat hiermee tevens de medewerkers werkzaam voor het secretariaat van CDHO en CDMBO. Het privacybeleid van de NVAO omvat niet de werkzaamheden van **2 commissieleden**, deze vallen onder verantwoordelijkheid van het Ministerie van Onderwijs, Cultuur en Wetenschap. Voor verwerkingen van de Commissie CDHO/CDMBO waar de NVAO verwerker is, wordt een verwerkingsovereenkomst gesloten.



2 Art 5.1 lid 2 e

Misschien nog specificeren? Zodat er geen verwarring kan ontstaan?

1.3 Doelgroepen

Dit beleidskader is van toepassing op alle bestuurders, medewerkers, tijdelijke werknemers en op alle andere personen die namens de NVAO werken.

Het beleidskader is van toepassing op personen werkzaam in een ondersteunende functie, managementfunctie, juridische functie, staffunctie, beleidsfunctie, of in een andere discipline.

De aard van de werkzaamheden bepaalt het type privacyvraagstukken en afwegingen die voor de betreffende persoon relevant zijn.

1.4 Verantwoordelijk voor bijhouden privacy 3 beleidskader

Het privacy office van de NVAO is verantwoordelijk voor het beheer van dit privacy beleidskader.

De instrumenten en dit beleidskader zijn levende documenten die periodiek (moeten) worden geactualiseerd.

Algemene vragen over dit beleid of suggesties tot wijziging of toevoeging aan het beleid, kunnen worden gericht aan het privacy office van de 4 NVAO.



3 Art 5.1 lid 2 e

Is het niet beter om deze alinea bij slot te zetten?

Beheer/Wijzigingen/vaststellen/inwerkingtreding/evaluatie etc.



4 Art 5.1 lid 2

Het is toch een intern beleidskader? Maar kan ook voor intern nuttig zijn.

1.5 Wet- en regelgeving verwerking van persoonsgegevens

A. 5 Europese en Nederlandse wet- en regelgeving op het terrein van privacy

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Vanaf dat moment geldt dezelfde privacywetgeving in de hele Europese Unie.

De AVG is rechtstreeks van toepassing. Daar waar de AVG ruimte laat voor nationale keuzes bij de uitvoering van de AVG, zijn deze ingevuld in de Uitvoeringswet AVG (UAVG).



5 Art 5.1 lid 2 e

Ik heb vanuit jullie eerdere wens om het iets lichter te maken A en C bij elkaar gevoegd.

Starten met AVG is op zich wel logisch in een Privacybeleidskader.

6 Op de verwerking van persoonsgegevens die in de basisregistratie personen (BRP) voorkomen, is de (U)AVG niet van toepassing. Op de verwerking van die persoonsgegevens ziet de Wet BRP. Er wordt nog gewerkt aan nieuwe regelgeving, de e-privacy verordening (EPV), waarin zaken als cookieregels en het spamverbod nader worden geregeld; deze regelgeving is nog niet van kracht 7 ².

² Verordening van het Europees Parlement en de Raad met betrekking tot de eerbiediging van het privéleven en de bescherming van persoonsgegevens in elektronische communicatie, en tot intrekking van Richtlijn 2002/58/EG.

 6 Art 5.1 lid 2 e

In hoeverre voor ons relevant.

 7 Art 5.1 lid 2 e

Begrijp ik hieruit dat jullie hier geen documentatie willen vermelden? Kan ik me op zich voorstellen. In de andere paragrafen is het wel heel handig ivm overzicht van de instrumenten die je hanteert.

Naast genoemde wetgeving zijn er aanvullende documenten vanuit het Europees Comité³ voor gegevensbescherming (Comité) waarmee (o.a.) verduidelijking wordt gegeven voor de toepassing van de AVG. Daarnaast vormt ook de uitleg van de AVG (veelal vastgelegd in beleidsregels) door de Autoriteit Persoonsgegevens (AP) een belangrijke bron voor de naleving van de AVG. De AP gaat ervan uit dat verwerkingsverantwoordelijken als de NVAO de beleidsregels toepassen en adviezen opvolgen, dan wel gemotiveerd afwijken (comply or explain).

Instrumenten:
-
- AVG en UAVG
- https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/handleiding_avg.pdf
-
- https://edps.europa.eu/
-

B. Specifieke context NVAO

De AVG laat zich voor de NVAO het beste plaatsen vanuit het perspectief van de hoofdprocessen van de NVAO:

- Het primaire proces
- Het personeelsproces
- Het betalingsproces

Het primaire proces

8 Accreditatieproces uitschrijven voor NL en VI in kort

³ European Data Protection Supervisor (EDPS).

De taken van de NVAO zijn belegd in verschillende instellingsbesluiten waarbij ook hun specifieke taken zijn vastgelegd.



8 Art 5.1 lid 2 e

Goed idee. Lijkt me zinvol om daar de elementen aan te stippen die met name verwerkingen van pgg betreffen. Zoals de panels.

In Nederland zijn de taken van de NVAO gebaseerd op de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW, hoofdstuk 5): het accrediteren van bestaande opleidingen, het toetsen van nieuwe opleidingen in het hoger onderwijs en het adviseren van de Minister in specifieke aangelegenheden zoals opgenomen in de WHW.

In Vlaanderen zijn de taken gebaseerd op de Codex Hoger Onderwijs (oktober 2013). Deze wetgeving dient als uitgangspunt voor accreditatie in het hoger onderwijs in Vlaanderen.

Het personeelsproces

Onder het personeelsproces worden alle verwerkingen geschaard die betrekking hebben op de persoonsgegevens van het eigen personeel van de NVAO.

Het betalingsproces

Onder het betalingsproces behoren alle verwerkingen die gerelateerd zijn aan het overmaken van geld aan leveranciers, commissieleden, personeel en eventuele andere partijen.

2. Uitgangspunten bij verwerking van persoonsgegevens

9 In hoofdstuk 2. staan de uitgangspunten voor onze omgang met persoonsgegevens, wat dat voor een medewerker betekent en welke documenten beschikbaar zijn om die uitgangspunten in het dagelijks werk toe te passen.



9 Art 5.1 lid 2 e

Nu ik het beleidskader heb ik toch het idee dat je ook prima kan beginnen met de uitgangspunten

2.1 Uitgangspunten voor een verantwoorde omgang met persoonsgegevens

Er zijn een achttal uitgangspunten opgesteld waaraan medewerkers van de NVAO te allen tijde aan dienen te voldoen. Deze uitgangspunten reflecteren de visie van de NVAO ten opzichte van de verwerking van persoonsgegevens en zijn afgeleid van de principes die zijn opgesteld door het OECD, die aan de basis heeft gelegen van de uitgangspunten van de AVG. ⁴ De uitgangspunten voor gegevensbescherming zijn van toepassing op *alle* verwerkingsactiviteiten met betrekking tot persoonsgegevens binnen de NVAO. Dit betekent dat alle verwerkingen van persoonsgegevens moeten voldoen aan onderstaande eisen.

⁴ Het OECD is de organisatie voor economische samenwerking en ontwikkeling. De OECD heeft in 1980 principes opgesteld en in 2013 zijn deze voor het laatst herzien.

1. De NVAO verwerkt alleen persoonsgegevens als voor de verwerking een rechtmatige grondslag aanwezig is en een duidelijk omschreven en gerechtvaardigd doel.

10 Persoonsgegevens mogen slechts worden verwerkt voor een voorafgaand aan de verwerking omschreven doel (of doeleinden). Onder verwerken valt (korte uitleg) (zie bijlage 1)



10 Art 5.1 lid 2 e

Ik weet niet hoe het met jullie zit, maar ik vind die instructies in combinatie met de instrumenten niet lekker werken. Levert veel herhaling op. En in het stuk erboven zie ik ook vaak mededelingen op instructieniveau. Ik heb bij dit onderdeel geprobeerd het al anders op te zetten. Wat vinden jullie, werkt dit beter?

- ⇒ Gebruik altijd een van de grondslagen uit artikel 6 van de AVG
- ⇒ Bij nieuwe werkzaamheden die de NVAO in het kader van zijn taken verricht, de voor de overheid geldende rechtsgrondslagen “noodzakelijk voor de uitvoering van een wettelijke plicht” en “noodzakelijk voor het uitoefenen van een publiekrechtelijke taak of uitoefenen van openbaar gezag”. Als je hierop beroept dan moet er wel ook nog een plicht of taak aan te wijzen zijn in een specifieke wet. De rechtsgrondslag moet dus in de WHW of in het Decreet zijn verankerd.
- ⇒ De grondslag “noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerker of van de verwerkingsverantwoordelijke of van een derde” kan niet worden gebruikt als er sprake is van verwerkingen door overheidsinstanties in het kader van de uitoefening van hun taken. Dit kan wel in beeld komen bij een verwerking in het kader van de bedrijfsvoering (denk bijvoorbeeld aan cameratoezicht rond het gebouw). Ditzelfde geldt voor de grondslag “toestemming”. De ongelijke machtsverhouding tussen betrokkene en de overheid staat over het algemeen in de weg aan de eis dat betrokkene de toestemming vrijelijk moet verlenen

Een (aanpassing van) verwerking moet steeds worden opgenomen in het register van verwerkingsactiviteiten. Dit register geeft een beschrijving van verwerkingsactiviteiten. De verantwoordelijke (de NVAO) moet dit op verzoek aan de AP kunnen laten zien. Neem bij een dergelijk verzoek contact op met de privacy officer die dit in afstemming met bestuurder verzorgt. Het register van verwerkingsactiviteiten bevat zelf geen persoonsgegevens.

- ⇒ Het doel van elke verwerking is concreet en vastgelegd in het register van verwerkingen. Als een bestand voor meer doelen wordt gebruikt dan wordt dat vermeld in de doelomschrijving. Doelen die duidelijk zijn omschreven maken het voor betrokkene inzichtelijk wat met de gegevens wordt gedaan. Bij verdere verwerking van persoonsgegevens voor een ander doel dan waarvoor de gegevens oorspronkelijk zijn verzameld, wordt altijd beoordeeld of dit nieuwe doel verenigbaar is met het oorspronkelijke doel. De verwerking moet voor betrokkenen duidelijk en transparant te zijn.

De NVAO is verplicht een Data Protection Impact Assessment, DPIA (ook wel genoemd Gegevensbeschermingseffectbeoordeling, GEB), uit te voeren bij de ontwikkeling van beleid en regelgeving waaruit verwerkingen van

persoonsgegevens voortvloeien. De AP heeft een lijst van verwerkingen opgesteld waarvoor de DPIA verplicht is.⁵ De DPIA is bedoeld om de effecten van de beoogde gegevensverwerking(en) voor betrokkenen te inventariseren en te beoordelen. Op basis van de DPIA kunnen maatregelen worden genomen om de risico's aan te pakken.

- ⇒ gebruik hiervoor het Rijksmodel GEB (PIA) of het model dat in Privacy Nexus is opgenomen. De privacy officer en de FG helpen je bij vragen over de opzet en uitvoering van de DPIA.

Instrumenten:

- Register van verwerkingen (Privacy Nexus)
- Privacy verklaring NVAO **11** (*intern/extern*) **12**
- Rijksmodel GEB (PIA)⁶
- DPIA-register (Privacy Nexus)
- Memo Quick Scan DPIA
- DPIA Proces NVAO



11 Art 5.1 lid 2 e

Ik heb cursief gemaakt wat nog in ontwikkeling is.



12 Art 5.1 lid 2 e

Ik zou deze eerder onder transparantie noemen. Je noemt het stuk ook niet hierboven.

2 De NVAO beperkt de verwerking tot die categorieën persoonsgegevens die nodig zijn voor het beschreven doel.

Alleen de voor het vooraf en precies omschreven doel noodzakelijke gegevens mogen worden verzameld. Gegevens mogen vervolgens niet verder worden verwerkt als dit onverenigbaar is met dat doel. Persoonsgegevens die niet meer nodig zijn (moeten) worden verwijderd of waar mogelijk geanonimiseerd.⁷

Bij de ontwikkeling van nieuwe (of wijziging van bestaande) producten en diensten wordt met gegevensbescherming rekening gehouden.

⁵⁵ <https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667>

⁶ <https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia>

⁷ De AVG is niet van toepassing op anonieme gegevens omdat deze gegevens niet terug te voeren zijn op een geïdentificeerde of identificeerbare natuurlijke persoon. Anonimisering is versleuteling die onomkeerbaar is, het niet meer mogelijk om deze later weer met personen in verband te brengen. Bij pseudonimisering kunnen anonieme gegevens met de juiste sleutel inzichtelijk gemaakt worden, waardoor herleiding naar natuurlijke personen weer mogelijk is. De AVG is wel van toepassing op gepseudonimiseerde gegevens.

- Verwerk niet meer gegevens dan die aantoonbaar noodzakelijk zijn voor het doel van de verwerking (*dataminimalisatie*). Bedenk waarom je gegevens voor die specifieke verwerking nodig hebt en of je daadwerkelijk *alle* gegevens nodig hebt.
- Nieuwe systemen worden geconfigureerd op een zodanige wijze dat alleen de voor het specifieke verwerkingsdoel noodzakelijke gegevens worden verwerkt. Privacy moet dus bij het ontwerp van een (nieuw) automatiseringssysteem als uitgangspunt worden genomen. (*privacy by design*).
- Ga bij het ontwikkelen van beleid, processen (en systemen) altijd uit van de meest privacybeschermende instellingen (*privacy by default*).
- Raadpleeg bij het ontwikkelen en uitwerken van beleid, processen en systemen de Handleiding Privacy by Design & by Default om meer zicht te krijgen op privacyvriendelijk ontwerp waarin de bescherming van persoonsgegevens is ingebouwd.⁸

Instrumenten:

- Handleiding Privacy by Design (versie 3.0 CIP)

3 NVAO verwerkt persoonsgegevens die accuraat en actueel zijn.

Dit betekent onder meer dat er sprake is van zorgvuldig beheer van gegevens (*betrouwbaarheid en integriteit*) en dat het voor betrokkenen mogelijk is om verzoeken met betrekking tot rectificatie van onjuiste persoonsgegevens in te dienen (*rechten van betrokkenen*).

Instructie

- Zorg dat de juistheid en actualiteit van de persoonsgegevens zoveel mogelijk gewaarborgd is. Bijvoorbeeld door periodieke controles en/of controle op de input. **13** Doe dit in ieder geval tijdens je werkzaamheden in en toezichts- of handhavingszaak.
- Zorg dat het mogelijk is om gegevens aan te passen daar waar zij onjuist, onvolledig of verouderd zijn.
- Geef invulling aan de rechten van betrokkenen conform het Regeling rechten van betrokkenen NVAO en Werkbeschrijving⁹ bij het verwerken van een (wijzigings)verzoek van een betrokkene



13 Art 5.1 lid 2 e

Dit is niet voor NVAO relevant. Wellicht handig om hier de panels te noemen.

Instrumenten:

- Regeling rechten van betrokkenen NVAO en Werkbeschrijving (i.o.)

4 NVAO bewaart gegevens niet langer dan noodzakelijk voor het beschreven doel.

Persoonsgegevens worden slechts bewaard zolang dit nodig is om de beschreven doelen te bereiken, of zolang als bepaald door een specifieke wet.

De NVAO heeft maximale bewaartermijnen bepaald en geïmplementeerd voor alle persoonsgegevens waarover de organisatie mag beschikken. Nadat een bewaartermijn is verstreken, moeten de persoonsgegevens verwijderd

⁸ https://www.cip-overheid.nl/media/1136/20170507-handleiding-privacy-by-design-v3_0.pdf

worden of geanonimiseerd¹⁰. Persoonsgegevens kunnen meerdere doelen dienen. Houd hiermee rekening bij het opstellen van de bewaartermijnen.

Instructie

- Bewaar persoonsgegevens niet langer dan noodzakelijk voor de doelen van de verwerking.
- Stel bewaartermijnen vast conform de selectielijst van de NVAO
- Wis gegevens wanneer deze niet langer noodzakelijk zijn voor het verwerkingsdoel.

Instrumenten:

- Selectielijst van de NVAO
- 14 Handreiking Bewaren van e-mail Rijksoverheid



14 Art 5.1 lid 2 e

nieuwe versie beschikbaar en ook interpretatie. Zie bijlage bij mail

5 De NVAO is, als dat mogelijk is, open en transparant over de verwerking van persoonsgegevens aan de betrokkene, de samenleving en ketenpartners.

Betrokkenen dient te weten wat er met zijn persoonsgegevens gebeurt wil hij zijn rechten kunnen uitoefenen. De informatie over de verwerking en de omgang met de gegevens en over de rechten van betrokkene dient eenvoudig toegankelijk en begrijpelijk te worden aangeboden. Dit gebeurt in een privacyverklaring. Zie voor de extern gerichte privacyverklaring de website van de NVAO en voor de intern gerichte privacyverklaring het intranet.

Instructie

- De NVAO verstrekt de vereiste informatie over onze verwerkingsactiviteiten via de privacyverklaring op www.nvao.net
- Deze 15 privacyverklaring wordt periodiek door het privacy office op haar actualiteit gecontroleerd.



15 Art 5.1 lid 2 e

Meervoud neem ik aan?

Instrumenten:

- Externe Privacyverklaring NVAO op www.nvao.net
- 16 Interne Privacyverklaring medewerkers NVAO (in ontwikkeling)
- Handreiking Veilige omgang met persoonsgegevens



16 Art 5.1 lid 2 e

Personeelshandboek vermelden?

6 De NVAO zorgt dat persoonsgegevens die aan ons zijn toevertrouwd, veilig en vertrouwelijk worden verwerkt.

¹⁰ Zie voetnoot 7

Op basis van wet- en regelgeving is de NVAO verplicht om passende technische en organisatorische maatregelen te treffen om de persoonsgegevens een passend beschermingsniveau te bieden tegen ongeautoriseerde verwerkingen. De NVAO heeft een Handreiking Veilige omgang met Persoonsgegevens opgesteld. In het kader van dat beleid worden passende organisatorische (bijvoorbeeld autorisatiebeleid) en technische maatregelen (bijvoorbeeld versleuteling) genomen ter beveiliging van de persoonsgegevens.

Een datalek is een inbreuk op de beveiliging van de persoonsgegevens die leidt tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking of toegang tot gegevens. Een datalek dat een risico voor de rechten van betrokkene inhoudt moet binnen 72 uur aan de AP worden gemeld en soms ook aan betrokkene. Hiervoor is het Protocol datalekken ontwikkeld.

Instructie

- Toegang tot persoonsgegevens wordt alleen verstrekt aan die mensen die toegang tot de gegevens nodig hebben en die toestemming hebben om gegevens verder te verwerken.
- Volg voor wat betreft de beveiliging van persoonsgegevens de Handreiking Veilige omgang met Persoonsgegevens
- Volg het Protocol datalekken NVAO voor de afhandeling van datalekken en raadpleeg voor meer informatie de privacy officer.
- **17** Via de e-mail worden veel bestanden uitgewisseld en dus ook vaak persoonsgegevens. Het is belangrijk om een passend beschermingsniveau toe te passen bij het versturen van dergelijke gegevens. Bij het versturen van bestanden met persoonsgegevens is het passend om deze gegevens versleuteld te versturen naar de ontvanger. Op die manier wordt het risico verkleind dat er per ongeluk bestanden naar de verkeerde ontvanger worden gestuurd. Als het nodig is om gegevens versleuteld te versturen naar de ontvanger, verstuur deze bijvoorbeeld door middel van een versleutelde omgeving.



17 Art 5.1 lid 2 e

Past beter bij tweede bullet

Instrumenten:

- **18** Gedragscode Rijk
- *Handreiking Veilige omgang met Persoonsgegevens (i.o.)*
- *Autorisatiebeleid (i.o.)*
- *Beveiligingsbeleid (i.o.)*
- Protocol datalekken NVAO
- Register datalekken en beveiligingsincidenten



18 Art 5.1 lid 2 e

Heet ie zo? Ken het stuk niet

7 De NVAO legt verantwoording af over de zorgvuldige verwerking van persoonsgegevens.

Dit betekent dat de NVAO passende maatregelen neemt en evalueert om de bescherming van persoonsgegevens te waarborgen en aan de hand van documentatie kan aantonen dat de privacyregels worden nageleefd. Deze verantwoordingsplicht (*accountability*) staat centraal in het nieuwe wettelijk privacykader.

De NVAO houdt als verwerkingsverantwoordelijke een register van verwerkingsactiviteiten bij. In dat register staat informatie over de gegevens die worden verwerkt. De persoonsgegevens zelf staan niet in het register, wel welke categorieën persoonsgegevens er worden verwerkt.

Bij het sluiten van overeenkomsten met derden neemt de NVAO de verplichtingen van de AVG in acht. De NVAO vergewist zich ervan dat derde partijen behoorlijk en zorgvuldig met persoonsgegevens omgaan. Dit hoeft niet noodzakelijkerwijs te gaan over partijen waarmee een verwerkersovereenkomst mee afgesloten dient te worden. Denk hierbij aan de Arbodienst die een eigen verwerkingsverantwoordelijkheid heeft. Waar nodig wordt een verwerkingsovereenkomst **19** gesloten.

**19 Art 5.1 lid 2 e****IK mis hier register van overeenkomsten met derden.***Instructie*

- Neem de nodige technische en organisatorische maatregelen om naleving van bovengenoemde uitgangspunten te kunnen waarborgen. Documenteer en toon de effectiviteit van deze maatregelen aan (door bijvoorbeeld evaluaties, monitoring, logging).
- Houd een registratie van de verwerkingen bij.
- Het privacy office is verantwoordelijk voor het beheer van dit register. Wijzigingen in verwerkingen, dienen door medewerkers en/of leden van het managementteam aan de privacy officer te worden doorgegeven. De managers van de afdelingen Nederland en Vlaanderen hebben een zelfstandige verantwoordelijkheid om bij nieuwe verwerkingen (activiteiten/andere ICT systemen) de privacy officer en de FG op de hoogte te stellen. De FG houdt toezicht op het op juiste wijze verwerken van de verwerkingen in het register van verwerkingsactiviteiten **20** (verwerkingenregister).

**20 Art 5.1 lid 2 e****Idem**

Instrumenten:

- Register van verwerkingen
- Format verwerkersovereenkomst
- Checklist verwerkersovereenkomst (zie model Privacy Company)
- *Beleid voor toezicht op logging (i.o)*
- Register verwerkersovereenkomsten

8 De NVAO respecteert de rechten van de betrokkenen

De NVAO respecteert de rechten van betrokkenen. Dat betekent dat systemen, processen en de interne organisatie zodanig worden ingericht dat op de juiste manier gehoor wordt gegeven aan verzoeken. Bekend moet zijn wanneer en hoe, indien van toepassing, verzoeken van betrokkenen tot inzage in hun gegevens (of andere rechten) worden gehonoreerd. De NVAO heeft een document Protocol t.a.v. beoordelen rechten van betrokkenen, waarin staat hoe met betrokkenen kan worden omgegaan. Tevens is er een model voor de beantwoording van inzageverzoeken.

Betrokkenen worden in de **21** privacyverklaring gewezen op hun rechten. Zij kunnen bij de AP een klacht indienen over de manier waarop NVAO met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.

**21 Art 5.1 lid 2 e**

In de privacyverklaring extern wordt de FG genoemd én de AP. Keuze maken.

Instructie

- Geef invulling aan de rechten van de betrokkenen zoals beschreven in het Protocol t.a.v. beoordelen rechten van betrokkenen bij het verwerken van een verzoek van een betrokkene. Om hieraan goed uitvoering te kunnen geven hanteert de NVAO een stappenplan en zijn taken/verantwoordelijkheden hierin benoemd. Ook op de website van de AP is meer informatie over dit onderwerp te vinden.¹¹

Instrumenten:

- 22 Regeling rechten van betrokkenen



22 Art 5.1 lid 2 e

gelijk trekken met gebruikte terminologie

¹¹ <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/privacyrechten>

https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/voorbeeldoverzicht_bij_inzageverzoek_def.pdf

3. Privacy governance

3.1 Inleiding

Doel van dit hoofdstuk over de privacy governance is inzicht te geven in de verantwoordelijkheden op het gebied van de privacybescherming binnen de NVAO. De governancestructuur helpt de NVAO om zorgvuldig met persoonsgegevens om te gaan en verantwoording af te kunnen leggen over genomen beslissingen. Een robuuste beheersorganisatie is van belang voor de implementatie en handhaving van de principes en doelstellingen uit het privacybeleid.

Omgevingsveld

De NVAO is een zelfstandig bestuursorgaan en valt onder de politieke verantwoordelijkheid van onder het Comité van Ministers. Hoewel de NVAO een *zelfstandig* bestuursorgaan is, blijft het Comité van Ministers politiek verantwoordelijk voor compliance met wet- en regelgeving en dus ook de AVG. Het Comité van Ministers vraagt de NVAO om periodiek te rapporteren over compliance met betrekking tot de **23** AVG.



23 Art 5.1 lid 2 e

zie ook eerdere opmerking. Goed om dat gewoon heel duidelijk te maken.

De AP is de toezichhoudende autoriteit met betrekking tot het voldoen aan de vereisten van de AVG. Wanneer betrokkenen klachten hebben over hoe de NVAO omgaat met persoonsgegevens, kunnen zij terecht bij de AP. De Nationale Ombudsman kan eventueel ook nog een bemiddelende rol spelen tussen de NVAO en personen waarvan de NVAO gegevens verwerkt.

3.2 **24** Privacyverantwoordelijkheden rollen en taken



24 Art 5.1 lid 2 e

Even kijken naar de structuur in deze paragraaf.

Privacy gaat de gehele NVAO aan en ziet ook op de gehele organisatie. Met elkaar werken we aan de naleving van het privacybeleid en draagt de NVAO als bestuursorgaan hiervoor verantwoordelijkheid.

De verantwoordelijkheid voor de uitvoering van de AVG en de verantwoording hierover ligt in de lijn. Het management, en meer specifiek het Dagelijks bestuur en de directeur, zijn zowel vanuit de AVG als vanuit de mandaatregeling verantwoordelijk voor de rechtmatige en zorgvuldige verwerking van persoonsgegevens.

In het RASCI model (zie bijlage 2) is uitgewerkt wie verantwoordelijk is voor welk onderdeel van de AVG. Meer in het algemeen staat hieronder beschreven bij wie, welke rollen en taken binnen de NVAO bij de uitvoering van de AVG zijn belegd. De personen/onderdelen die bij de uitvoering van de privacy zijn betrokken zijn de volgende:

- AB - Algemeen Bestuur van de NVAO
- DB - Dagelijks Bestuur van de NVAO
- Directeur NVAO/NL
- Directeur Vlaanderen
- Afdelingshoofd Nederland
- PO - Privacy officer
- FG - Functionaris voor gegevensbescherming

- Relatiebeheer
- CISO – Chief Information Security Office (beslispunt)
- HR - Hoofd HR
- C - communicatie
- OR- Ondernemingsraad
- Mw- medewerker

Algemeen Bestuur

Het Bestuur is eindverantwoordelijk

De lijn: AB, DB, MT

Overeenkomstig de mandaatstructuur binnen de NVAO zijn het bestuur, de directeur en hoofden van de afdelingen NVAO verder verantwoordelijk voor de strategische visie, de risicobeheersing en voor het borgen van de aantoonbare naleving van de wet- en regelgeving op het terrein van privacybescherming. Het MT is een overlegorgaan van de directeur Nederland, Directeur Vlaanderen, Afdelingshoofd Nederland, Hoofd HR en Hoofd Financiën. Beslissingen over de dagelijkse gang van zaken binnen de NVAO worden in het MT besproken. Vaak volgt hieruit een formele beslissing. Deze beslissing is dan (mandaattechnisch) toe te rekenen aan de Directeur Nederland. Het Afdelingshoofd Nederland heeft als MT-lid de juridische aspecten van privacy in zijn pakket en is daarmee als eerste het aanspreekpunt voor privacy.

De (niet met toezicht belaste) specialisten: PO, CISO en HR

Naast een privacy officer heeft de NVAO en **25** > te formaliseren) een CISO uitleg. De privacy officer en de CISO adviseren, ondersteunen en controleren de directie, het bestuur en de medewerkers bij privacy aspecten. Ook bepaalde beleidstaken en het organiseren van interne risicoanalyses behoren tot hun takenpakket. Primair is de privacy officer het aanspreekpunt voor de uitleg van de AVG binnen de NVAO en bij de implementatie en uitvoering van de AVG.



25 Art 5.1 lid 2 e

Nog even kijken naar deze zin

Daarnaast heeft HR een rol als het gaat om de zorgvuldige omgang met persoonsgegevens. Deze medewerker is het eerste aanspreekpunt bij personeelsgerelateerde vragen van medewerkers over de AVG.

Interne toezichtsorganen: FG en OR

Tenslotte kent de NVAO een Functionaris Gegevensbescherming (FG) en de Ondernemingsraad (OR). Zij zijn vanwege hun specifieke rollen en wettelijke taken bij aspecten van de privacy van de NVAO betrokken.

26 Meer informatie over de taken van de FG en de OR zijn te vinden op:

<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-uitkering/ondernemingsraad>

<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/functionaris-gegevensbescherming-fg>



26 Art 5.1 lid 2 e

Ik zou dit verplaatsen naar de voetnoot

controleren. Het is de eigen verantwoordelijkheid van het NVAO om intern toezicht te houden op de waarborging van privacybescherming, los van eventuele externe audits en evaluaties.

Functionaris Gegevensbescherming (FG)

De NVAO heeft een externe FG aangesteld overeenkomstig artikel 37 e.v. van de AVG. De FG rapporteert aan de voorzitter van het bestuur. In de AVG is de rol van de FG als volgt beschreven:

- informeren en adviseren van het lijnmanagement over hun verplichtingen uit hoofde wet- en regelgeving in het kader van privacy;
- toezien op de naleving van de relevante wetgeving, het privacybeleid en de inrichting van de interne privacy organisatie;
- advies leveren bij een DPIA, zowel de inhoudelijke beoordeling als de naleving van de voorgenomen beheermaatregelen;
- samenwerken met de AP, de centrale toezichthouder, in het geval van onderzoek;
- aanspreekpunt voor betrokkenen (burgers en medewerkers) voor alle aangelegenheden bij de verwerking van hun persoonsgegevens.

Jaarlijks kan de FG een werkplan privacy office opstellen in het kader van zijn toezichthoudende werkzaamheden.

27 Privacy officer

De NVAO heeft een privacy officer die de volgende taken verricht:

- ondersteunt de NVAO in het naleven van de eisen uit dit privacybeleid en de privacywetgeving.
- beheert het privacybeleid en kan op verzoek van de directie, het lbestuurof uit eigen beweging een voorstel tot aanpassing van het beleid doen;
- zorgt voor de dagelijkse afhandeling van privacy aangelegenheden voor de NVAO;
- beheert het register van verwerkingsactiviteiten
- stelt de jaarplanning op
- fungeert als vraagbaak voor het management ten aanzien van het verzamelen, registreren en leveren van persoonsgegevens. Hij raadpleegt indien nodig de Functionaris Gegevensbescherming of externe adviseurs over complexere verwerkingen en relaties met verwerkers.
- adviseert het management bij de analyse van mogelijke risico's die samenhangen met de verwerking van persoonsgegevens.



27 Art 5.1 lid 2 e

JZ/PO. Wellicht goed om meteen duidelijk te maken hoe dit bij NVAO zit: de medewerkers JZ zijn teven de PO's

Rol van de OR bij privacyvraagstukken

De ondernemingsraad vertegenwoordigt het personeel van de NVAO en beschermt hun belangen. De ondernemingsraad heeft daarvoor verschillende rechten en bevoegdheden, zoals het recht op informatie, het adviesrecht, het instemmingsrecht en het initiatiefrecht. Met name het adviesrecht, instemmingsrecht en het initiatiefrecht spelen een rol bij de uitvoering van de AVG. Artikel 27 WOR

Het kan zijn dat er nieuwe technische maatregelen worden getroffen om te voldoen aan de AVG. Denk bijvoorbeeld aan technische maatregelen om persoonsgegevens te beveiligen of om ervoor te zorgen dat alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor het verwerkingsdoel.

Op grond van de Wet op de Ondernemingsraden (WOR) dient een besluit tot het invoeren of wijzigen van een technologische voorziening ter advies aan de ondernemingsraad te worden voorgelegd. Dus als de NVAO wil overgaan tot de aanschaf van nieuwe ICT ter beveiliging van de persoonsgegevens, dan heeft de OR adviesrecht.

Een besluit tot vaststelling, wijziging of intrekking van een regeling over het verwerken van, alsmede de bescherming van de bij de NVAO werkzame personen is instemmingsplichtig. Het moet dus gaan om een regeling die tot doel heeft persoonsgegevens te verzamelen, bewaren, gebruiken, verstrekken of beveiligen. Dit geldt onder meer voor de vaststelling van dit privacybeleid en voor het melden van een datalek waarbij persoonsgegevens zijn betrokken.

De ondernemingsraad kan tenslotte gebruikmaken van haar initiatiefrecht om voorstellen te doen voor een (aanpassing van) privacybeleid.

28 Informatiemanagement

Het onderwerp privacy en gegevensbescherming heeft een multidisciplinair karakter. Het vraagt om een zorgvuldige afstemming met de 29 experts van juridische zaken, ICT, beveiliging, communicatie, de privacy en de FG. De informatiemanager heeft onder meer als taak de CISO-rol binnen de NVAO te vervullen. De CISO is in eerste instantie verantwoordelijk voor de informationele privacy. De CISO ondersteunt en adviseert de NVAO bij privacyvraagstukken. De CISO helpt onder meer door het geven van (zo mogelijk) advies op maat, het opbouwen van de noodzakelijke kennis over privacy wet- en regelgeving, het toepassen hiervan en het (mede-)ontwikkelen van producten zoals informatiebeleid en privacy convenanten.



28 Art 5.1 lid 2 e

Hier gaat het opeens niet meer over een rol. Suggestie: informatiemanager (CISO)



29 Art 5.1 lid 2 e

Dat zijn de PO's. Handig om dat meteen duidelijk te maken

3.3 Privacy overlegstructuren

Privacy moet als vast onderdeel opgenomen zijn op de agenda's van de reguliere overleggen tussen JZ/Directie alsook tussen JZ/Directie en HRM, Directie/Financiën, Dir/com, Dir/ICT en Dir/ICT-stuurgroep. Er is tenslotte ook nog een vast maandelijks overleg tussen de privacy officer en de Functionaris Gegevensbescherming.

De NVAO doet daarnaast mee aan overleggen van KleinLef organisaties op het gebied van privacy om de kennis omtrent privacy te delen en elkaar te helpen om beleid omtrent privacy te ontwikkelen.

3.4 Sturing, regie en 30 toezicht

Periodiek voert de NVAO met behulp van de tool in Privacy-Nexus self-assessments uit, waaruit blijkt wat de stand van zaken is met betrekking tot privacy.



30 Art 5.1 lid 2 e

Hier ook OR, PO en AP noemen? Onderscheid maken tussen intern en extern toezicht?

De FG ziet toe op de naleving van de relevante wetgeving, het privacybeleid en de inrichting van de interne privacy organisatie.

3.5 Privacy trainingen en bewustwording

Alle medewerkers krijgen bij hun aanstelling een korte introductie AVG van de PO/FG. Geheimhouding **31** (die eerdere eed die hierboven staat vermeld).



31 Art 5.1 lid 2 e

Verder uitwerken

Daarnaast vinden reguliere bewustwordingsacties plaats, door minimaal één keer per jaar aandacht voor een privacy onderwerp vanuit de privacy office en minimaal één bureaubijeenkomst per jaar over een AVG onderwerp. Daarnaast worden medewerkers ook geïnformeerd over de AVG en privacy, doordat dit onderwerp een integraal onderdeel uitmaakt van de besprekingen van het Dagelijks Bestuur. De verslagen hiervan zijn voor medewerkers te raadplegen.

4. Slot

Met dit privacybeleid brengt de NVAO in kaart welke maatregelen er zijn genomen om de persoonsgegevens van medewerkers en externen, waaronder o.a. panelleden, secretarissen en studenten, te beschermen. Daarnaast geeft het beleid inzicht in de wijze waarop de verantwoordelijkheden op grond van de AVG zijn belegd bij de NVAO. Ook is vastgelegd welke instrumenten de NVAO inzet om te voldoen aan belangrijke verplichtingen op grond van de AVG, zoals het inrichten en bijhouden van een register van verwerkingen, de wijze waarop omgegaan wordt met datalekken, het houden van een DPIA, het opstellen van een interne en externe privacyverklaring en de wijze waarop rechten van betrokkenen zijn georganiseerd. Privacybeleid is dynamisch beleid. Nieuwe ontwikkelingen volgen elkaar op en ook de organisatie zelf zal steeds in ontwikkeling zijn. Dit betekent dat het privacybeleid ook met regelmaat bijgesteld zal moeten worden. In een separate paragraaf (4.1) is een overzicht opgenomen van de versies van het privacybeleid van de NVAO.

4.1 Wijzigingen

Dit beleid wordt periodiek herzien en bijgewerkt. De volgende tabel toont de versie geschiedenis van dit privacy beleid.

Datum	Opmerkingen	Versie
16-10-2019	1 ^{ste} concept beleidsdocument	0.1
27-07-2020	Concept tbv FG	0.2

32 BIJLAGE 1: TERMINOLOGIE EN ACHTERGROND.**Wat zijn persoonsgegevens?**

Niet alle data of gegevens zijn per definitie persoonsgegevens. Persoonsgegevens betreft alle informatie met betrekking tot een geïdentificeerde of identificeerbare natuurlijke persoon (de "betrokkene").

**32 Art 5.1 lid 2 e**

Is het niet handiger om te volstaan met een begrippenlijst. Achtergrond is weer zo uitgebreid.

Snap niet helemaal toegevoegde waarde

De betrokkene hoeft geen direct geïdentificeerd individu te zijn, maar zodra een individu uit een groep kan worden onderscheiden, zijn de gegevens persoonsgegevens. Het is dus niet altijd nodig om de naam te weten van de persoon in kwestie om te spreken van persoonsgegevens.

Alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare persoon moeten als persoonsgegevens worden beschouwd. Enkel transactiegegevens zijn bijvoorbeeld op zichzelf geen direct identificeerbare gegevens, maar worden persoonsgegevens wanneer deze verband houden met een geïdentificeerde of identificeerbare persoon, bijvoorbeeld omdat deze is gekoppeld aan een naam, een e-mailadres of een telefoonnummer.

De AVG heeft een speciaal regime voor bijzondere categorieën persoonsgegevens. Dit betreffen persoonsgegevens waaruit de raciale of etnische afkomst, politieke opvattingen, religieuze of filosofische overtuigingen blijken, lidmaatschap van een vakvereniging, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie, gezondheids- of medische gegevens, gegevens over iemands seksleven of seksuele geaardheid.

Strafrechtelijke persoonsgegevens zijn persoonsgegevens die te maken hebben met strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen. Hieronder vallen zowel veroordelingen als mogelijk gegronde verdenkingen. Dit wil zeggen dat er concrete aanwijzingen zijn dat iemand een strafbaar feit heeft gepleegd. Een voorbeeld hiervan is een opgestelde zwarte lijst van frauderende klanten bij een financiële instelling. Onder de AVG gelden speciale regels voor het verwerken van strafrechtelijke gegevens.

De verwerking, het verzamelen of gebruiken, van gevoelige persoonsgegevens, is verboden, tenzij een uitzondering op het algemene verbod van toepassing is. Het verzamelen en gebruiken van dergelijke gegevens zal daarom zoveel mogelijk worden vermeden. Vermijd ook het verzamelen en gebruik van gegevens van gevoelige groepen, zoals kinderen / minderjarigen, gehandicapten en ouderen, tenzij hiervoor duidelijk toestemming is gegeven door de bevoegde persoon.

Hieronder volgen voorbeelden van gegevens die over het algemeen als persoonsgegevens worden beschouwd:

Voornaam en / of initialen en achternaam	Financiële gegevens
E-mailadres	Betaling of transactiegegevens
Telefoonnummer	Rijbewijs
Foto	Strafrecht ketennummer
Geboortedatum / geboorteplaats	Identificatienummer werknemer
IP-adres	Werknemers informatie
Uitkomsten functioneringsgesprekken	Medische informatie

Burgerservicenummer	Biometrische gegevens
Unique Device Identifiers	MAC-adressen

Wat is een betrokkene?

De betrokkene is de persoon van wie persoonsgegevens worden verwerkt.

Wat is een verwerking?

Het 'verwerken van persoonsgegevens' of een 'verwerking van persoonsgegevens' betreft alle handelingen die men met persoonsgegevens kan verrichten. Denk hierbij aan het verzamelen, vastleggen, raadplegen, opvragen, ordenen, structureren, opslaan, bewerken of wijzigen, verstrekken en combineren. Ook het wissen of vernietigen van gegevens is een verwerking van persoonsgegevens.

Wat is een verwerkingsverantwoordelijke?

De verwerkingsverantwoordelijke is de natuurlijke persoon of rechtspersoon die (alleen of tezamen met anderen) bepaalt welke persoonsgegevens worden verzameld, waarom persoonsgegevens worden verwerkt (doel) en hoe persoonsgegevens worden verwerkt (middelen). Wanneer partijen gezamenlijk het doel en de middelen vaststellen voor de verwerking van persoonsgegevens dan spreken we van een gezamenlijke verantwoordelijkheid.

Wat is een verwerker?

Een verwerker is de natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Het gaat om derde partijen die voor de verwerkingsverantwoordelijke werken. Een verwerker handelt onder de verantwoordelijkheid van de verwerkingsverantwoordelijke en naar diens instructies, maar er is geen hiërarchische relatie (medewerkers zijn geen verwerkers). Daarnaast heeft de verwerker geen zeggenschap over de verwerkingen en mag de gegevens niet voor eigen doelen gebruiken.

Bijlage 2: RASCI model

	#	Taken	AB	DB	Dir	FG	PO	CISO	AHN	HR	HF	M W
Gebruik van persoonsgegevens & AVG-naleving	1.	Het beslissen over het gebruik van persoonsgegevens voor zakelijke doeleinden ("doel en middelen")	33 A	A	C	C/I	R		c	I	I	I
	2.	Het uitvoeren van technische en organisatorische maatregelen om ervoor te zorgen dat de AVG wordt nageleefd	A	A	A?	C/I	C	R	R	I	I	I



33 Art

5.1 lid 2 e

**Je kan niet twee
A's hebben**

Privacy en gegevens- bescherming strategie en beleid	3.	Het bepalen van de privacy ambitie en strategie	A	A	C	C	R	C/I	C	C/ I	I	I
	4.	Het vaststellen van het privacy en gegevensbeschermingsbeleid	A	A	C	C	R	I	C	C	I	I
	5.	Afstemming privacybeleid met andere aanpalende (beleids)onderdelen (inkoop, HRM, IB)	34 I	I	A	C/I	R	C	C	C	C/ I	I
	6.	Het vaststellen en implementeren van de privacy governancestructuur	A	A	R	I	R	C/I	R	C/ I	C/ I	I
	7.	Het aanwijzen van hulpbronnen voor het uitvoeren van privacy werkzaamheden PM?? 35										
	8.	Het opstellen en borging van het autorisatiebeleid (incl. matrix)	A	A	C	C	C/S	R	C/S	C/ I	I	I



**34 Art 5.1 lid 2
e**

**Volgens mij is
deze bij nader
inzien
overbodig. Ook**



**35 Art 5.1 lid 2 e
Geld, budget e.d.**

**in verhouding
met 4 geeft hij
meer
verwarring dan
dat ie iets
toevoegt.**

Privacy maatregelen (privacy risicoclassificatie, DPIA, privacy by design etc.)	9.	Het verstrekken van advies op het gebied van privacy en gegevensbescherming	A	A	C	C/R	C/R	C/I	C/I	C/I	I	I
	10.	Het implementeren en borgen van privacy by design and default	A	A	R	C/I	R	R	C/I	I	I	I
	11.	Het opstellen van DPIA's	A	A	C	C	R	S/C /I	S/C /I	C/ I	S/ I	S/ I
	12.	Het vaststellen van DPIA	A	A	R/C	I	R	C/R	C/I	C/ I	I	I
	13.	Het ondersteunen en/of opstellen van leveranciersbeoordelingen (verwerkersovereenkomsten)	A	A	C	C/S	R	C/S	C/S	S	S	I
	14.	Adviseren over technologie en beveiliging omtrent gegevensverwerking	A	A	C	C	C/S	R	C	I	I	I

Vastleggen en documenteren	15.	Het maken en onderhouden van een verwerkingsregister	A	A	C	C/S /I	R	C/S	C/S	S	S	S
	16.	Het documenteren van DPIA's	A	A	I	I	R	I	I			
	17.	Het documenteren van verwerkingsovereenkomsten (DPA's)	A	A	I	I	R	I	I			
	18.	Het documenteren van datalekken	A	A	C	I	R	I	I			
	19.	Het vastleggen van toestemmingsverklaringen	A	A	C	I	R	C/S	C/S	C/ S/ I	I	S/ I
	20.	Het documenteren van vragen in het kader van rechten van betrokkenen	A	A	C	I	R	I	I			
	21.	Het opstellen en onderhouden van privacyverklaring (intern/extern)	A	A	C	C/S /I	R	S	C/S			

	22.	Vastleggen en onderhouden van processen en werkinstructies van privacyinstrumenten						36				
--	-----	--	--	--	--	--	--	----	--	--	--	--

36 Art 5.1 lid 2 e**Regel 22 niet bewerkbaar**

Verzoeken en incidenten (melding van datalek aan de toezichthoudende autoriteit en de betrokkene etc.)	23.	Het afhandelen van vragen en klachten gerelateerd aan (persoons)gegevensbescherming	A	A	C	C/S /I	R	C/S	C/S			
	24.	Het afhandelen van vragen over rechten van betrokkenen	A	A	C	C/S /I	R	C/S	C/S	S	S	S
	25.	Het behandelen van een incident*	A	A	C	C/S /I	R	C/S	C/S			
	26.	Het melden van een datalek aan de toezichthoudende autoriteit	A	A	C	C/S /I	R	C/S	C/S			
	27.	37										
	28.	Het communiceren van een datalek naar de betrokkene	C/A	A	R	C/S /I	C/S	C/S	C/S			
	29.	Het bijhouden van het incidentenregister*	A	A	C	I	R	C/S	I			
	30.	Het implementeren van mitigerende maatregelen na een incident*	A	A	R	C	C/S	C/S	I			
	31.	Het communiceren met de toezichthoudende autoriteit	A	A	C	R 38	C/R	S/C	S			

37 Art 5.1 lid 2 e**Eventueel OCW hier?****38 Art 5.1 lid 2 e****Bij melding datalek formeel maar doet Po ook, bij navraag is FG wel contactpersoon**

Training en bewustwording (het stimuleren van een privacy cultuur, training en workshops)	32.	Het uitvoeren en communiceren van bewustwordingsprogramma's m.b.t. privacy en gegevensbescherming	A	A	S/C	S/C	R	S/I	S/C /I	S/I	I	I
	33.	Het trainen van medewerkers betrokken bij de verwerking van persoonsgegevens	A	A	R/C 39	S/I	R		C/S			



e

Monitoring en handhaving	34.	Privacy-planning en control vastleggen (DPIA, DPA)									
	35.	Het periodiek rapporteren over privacy en gegevensbescherming aan management									
	36.	Het monitoren van AVG-naleving, incl (tijdige) vernietiging van gegevens									
	37.	Het handhaven van het privacybeleid									
	38.	Het nabespreken van een incident									

27

1 B

Privacy Beleidskader
Nederlands Vlaamse Accreditatie Organisatie



Status: conceptversie 03112020

Artikel 5.2 lid 1 e
Artikel 5.2 lid 1 e
Directeur Nederland
Voorzitter Algemeen Bestuur

Artikel 5.2 lid 1 e
Artikel 5.2 lid 1 e
Luut Kroes
Anne Flierman

Inhoud

Voorwoord

1. Privacy beleidskader
 - 1.1 Doel
 - 1.2 Scope NVAO /CDHO/CMMBO
 - 1.3 Doelgroepen
 - 1.4 Wet- en regelgeving verwerking van persoonsgegevens
 2. NVAO uitgangspunten voor omgang met persoonsgegevens
 - 2.1 Grondslag en doel
 - 2.2 Doelbinding
 - 2.3 Accuraat en actueel
 - 2.4 Bewaarbeperking
 - 2.5 Open en transparant
 - 2.6 Veilig en vertrouwelijk
 - 2.7 Verantwoordingsplicht
 - 2.8 Respect
 3. Privacy governance
 - 3.1 Inleiding
 - 3.2 Privacy verantwoordelijkheden rollen en taken
 - 3.3 Privacy overlegstructuren
 - 3.4 Sturing, regie en toezicht
 - 3.5 Privacy trainingen en bewustwording
 4. Slot
 - 4.1 Beheer
 - 4.2 Vaststellen
 - 4.3 Wijzigingen en evaluatie
- Bijlage 1 Begrippen
- Bijlage 2 Instrumenten (documenten, websites etc.)
- Bijlage 3 RASCI model
- Bijlage 4 Handreikingen (checklist, leidraad, stappenplan etc.) voor toepassen uitgangspunten omgang met persoonsgegevens P.M.

Voorwoord

De Nederlands-Vlaamse Accreditatieorganisatie (NVAO) is een kwaliteitszorgorganisatie die op deskundige en onafhankelijke wijze de kwaliteit van het hoger onderwijs in Nederland en Vlaanderen borgt en die de kwaliteitscultuur binnen de instellingen voor hoger onderwijs in Nederland en Vlaanderen bevordert. Zij accrediteert bestaande en nieuwe opleidingen en beoordeelt de kwaliteitszorg van instellingen in het hoger onderwijs. Daarmee is de NVAO bewaker van de kwaliteit van het hoger onderwijs. De besluiten van de NVAO leiden tot erkenning van diploma's en titels en waar van toepassing tot bekostiging van opleidingen. De NVAO baseert haar beoordeling op advies van erkende deskundigen.

De NVAO werd in 2003 opgericht bij Verdrag tussen Nederland en Vlaanderen. De taken van de NVAO zijn in wetgeving vastgelegd. De NVAO wil er toe bijdragen dat de kwaliteit van het hoger onderwijs in Vlaanderen en Nederland erkend wordt als internationaal aan de maat, maatschappelijk relevant en het vertrouwen geniet van studenten, werkgevers en de samenleving. Binnen de opdracht die in het accreditatieverdrag tussen Nederland en Vlaanderen aan de NVAO is toegekend, wil zij de kwaliteit van het hoger onderwijs borgen, verbeteringen stimuleren en een kwaliteitscultuur bevorderen.

Om dit werk goed te kunnen doen is verwerking van persoonsgegevens van medewerkers en de contactpersonen van ketenpartners en burgers noodzakelijk. De privacy van contactpersonen en relaties is erg belangrijk voor de NVAO en we hechten dan ook veel belang aan een correcte verwerking en gebruik van persoonsgegevens. De bescherming van persoonsgegevens is immers een grondrecht. De NVAO is verantwoordelijk voor de aantoonbare zorgvuldige omgang met persoonsgegevens.

De NVAO is een zelfstandig bestuursorgaan en opgericht naar Nederlands publiekrecht met de zetel in Den Haag. De NVAO valt onder verantwoordelijkheid van het Comité van Ministers.

Dit privacy beleidskader richt zich tot iedereen die werkzaamheden verricht voor de NVAO. In het privacy beleidskader wordt uitgelegd hoe de NVAO aantoonbaar zorgvuldig omgaat met persoonsgegevens, wat daarbij de uitgangspunten zijn en wat de rol van de medewerker is bij de bescherming van persoonsgegevens.¹

Datum Ondertekening

Anne Flierman

Voorzitter Algemeen Bestuur NVAO

¹ Voor een beknopte uitleg van begrippen (als persoonsgegevens en verwerking) zie bijlage 1.

1. NVAO Privacy beleidskader

Op het werk van het Nederlands Vlaamse Accreditatie Organisatie (NVAO) is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Daarnaast heeft de NVAO te maken met bijzondere wetgeving, waarin een grondslag voor verwerking van gegevens kan liggen. Denk hierbij bijvoorbeeld aan de gegevens die de NVAO nodig heeft van panelleden om hun deskundigheid voor deelname aan een panel te kunnen beoordelen. Voor de Afdeling Vlaanderen is dit geregeld in het Decreet, voor de Afdeling Nederland is dit vastgelegd in de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW).

Het NVAO Privacy beleidskader geeft aan waar de NVAO op het vlak van gegevensbescherming voor staat en wat de uitgangspunten voor de omgang met persoonsgegevens zijn. Met dit kader wil de NVAO ervoor zorgen dat de privacybescherming in lijn is met de wettelijke vereisten en die aansluit of geïntegreerd wordt bij de bestaande processen en systemen van de NVAO.

Bij alle uitgangspunten wordt steeds verwezen naar praktische ondersteunende instrumenten (checklists, stappenplan, procedures) van de NVAO dan wel (voor zover niet aanwezig) van OCW.

De uitleg van een aantal belangrijke begrippen uit de AVG is opgenomen in Bijlage 1: Begrippen.

1.1 Doel

Doel van dit beleidskader is een omgeving te creëren waarin elke medewerker van de NVAO:

- zijn of haar verantwoordelijkheid en rechten kent als het gaat om privacy en het verwerken van persoonsgegevens,
- in staat is om het juiste beleid en de juiste procedures te volgen,
- contact kan opnemen met de juiste personen wanneer er vragen zijn.

1.2 Scope

Het privacy beleidskader is bestemd voor de NVAO in zijn geheel. Alle handelingen binnen de NVAO met betrekking tot persoonsgegevens van burgers, bestuursleden, medewerkers, contactpersonen, zoals medewerkers kwaliteitszorg, panelleden en secretarissen, vallen allen binnen het bereik van dit beleidskader.

CMMBO en CDHO

Deze organisaties hebben zelfstandige taken en verantwoordelijkheden. Er is een nauwe samenwerkingsrelatie tussen de NVAO en de CMMBO/CDHO. Niet alleen zitten de organisaties fysiek in het pand bij de NVAO, de ondersteuning van CDHO en CMMBO is in dienst van de NVAO. Bovendien maken de drie organisaties gezamenlijk gebruik van de afdeling Ondersteuning van de NVAO (waaronder ICT, financiën en personeelszaken). Het privacybeleid van de NVAO omvat hiermee tevens de medewerkers werkzaam voor het secretariaat van CDHO en CMMBO. Het privacybeleid van de NVAO omvat niet de werkzaamheden van commissieleden CDHO en CMMBO, deze vallen onder verantwoordelijkheid van het Ministerie van Onderwijs, Cultuur en Wetenschap. Voor verwerkingen van de Commissie CDHO/CMMBO waar de NVAO verwerker is, wordt een verwerkingsovereenkomst gesloten.

1.3 Doelgroepen

Dit beleidskader is van toepassing op alle bestuurders, medewerkers, tijdelijke werknemers en op alle andere personen die namens de NVAO werken.

Het beleidskader is van toepassing op personen werkzaam in een ondersteunende functie, managementfunctie, juridische functie, staffunctie, beleidsfunctie, of in een andere discipline.

De aard van de werkzaamheden bepaalt het type privacyvraagstukken en afwegingen die voor de betreffende persoon relevant zijn.

1.4 Wet- en regelgeving verwerking van persoonsgegevens

A. Europese en Nederlandse wet- en regelgeving op het terrein van privacy

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Vanaf dat moment geldt dezelfde privacywetgeving in de hele Europese Unie.²

De AVG is rechtstreeks van toepassing. Daar waar de AVG ruimte laat voor nationale keuzes bij de uitvoering van de AVG, zijn deze ingevuld in de Uitvoeringswet AVG (UAVG).³

Naast genoemde wetgeving zijn er aanvullende documenten vanuit het Europees Comité⁴ voor gegevensbescherming waarmee (o.a.) verduidelijking wordt gegeven voor de toepassing van de AVG.

Daarnaast vormt ook de uitleg van de AVG (veelal vastgelegd in beleidsregels) door de Autoriteit Persoonsgegevens (AP) een belangrijke bron voor de naleving van de AVG. De AP gaat ervan uit dat verwerkingsverantwoordelijken als de NVAO de beleidsregels toepassen en adviezen opvolgen, dan wel gemotiveerd afwijken (comply or explain).

Links naar genoemde wetgeving en belangrijke documenten verband houdend met dit beleidskader zijn te vinden in Bijlage 2: Instrumenten.

B. Specifieke context NVAO

De AVG laat zich voor de NVAO het beste plaatsen vanuit het perspectief van de hoofdprocessen van de NVAO:

Het primaire proces

Het personeelsproces

Het betalingsproces

Het primaire proces

De NVAO is een kwaliteitszorgorganisatie die primair op deskundige en onafhankelijke wijze de kwaliteit van het hoger onderwijs in Nederland en Vlaanderen borgt en die de kwaliteitscultuur binnen de hogeronderwijsinstellingen in Nederland en Vlaanderen bevordert. Zij accrediteert bestaande en nieuwe opleidingen en beoordeelt de kwaliteitszorg van instellingen in het hoger onderwijs.

In Nederland zijn deze taken van de NVAO gebaseerd op de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW, hoofdstuk 5): het accrediteren van bestaande opleidingen, het toetsen van nieuwe opleidingen in het hoger onderwijs en het adviseren van de Minister in specifieke aangelegenheden zoals opgenomen in de WHW.

In Vlaanderen zijn deze taken gebaseerd op het structuurdecreet van april 2003, Decreet houdende vaststelling van het kwaliteitszorgstelsel in het hoger onderwijs. Deze wetgeving dient als uitgangspunt voor accreditatie in het hoger onderwijs in Vlaanderen.

Het personeelsproces

Onder het personeelsproces worden alle verwerkingen geschaard die betrekking hebben op de persoonsgegevens van het eigen personeel van de NVAO.

Het betalingsproces

Onder het betalingsproces behoren alle verwerkingen die gerelateerd zijn aan het overmaken van geld aan leveranciers, commissieleden, personeel en eventuele andere partijen.

² Een e-privacy verordening (EPV), waarin zaken als cookieregels en het spamverbod nader worden geregeld, is in ontwikkeling.

³ Verder heeft de rijksoverheid een Handreiking naleving AVG geformuleerd. De NVAO overweegt nog hoe deze handreiking in te zetten.

⁴ European Data Protection Supervisor (EDPS), <https://edps.europa.eu/>

2. NVAO uitgangspunten voor omgang met persoonsgegevens

In hoofdstuk 2 staan de uitgangspunten voor onze omgang met persoonsgegevens en wordt vervolgens toegelicht wat dat betekent voor een medewerker en welke documenten of websites beschikbaar zijn om die uitgangspunten in het dagelijks werk toe te passen.

Er zijn een achttal uitgangspunten opgesteld, waar medewerkers van de NVAO te allen tijde aan dienen te voldoen. Deze uitgangspunten reflecteren de visie van de NVAO ten opzichte van de verwerking van persoonsgegevens.⁵ De uitgangspunten voor gegevensbescherming zijn van toepassing op *alle* verwerkingsactiviteiten met betrekking tot persoonsgegevens binnen de NVAO.

Dit betekent dat alle verwerkingen van persoonsgegevens moeten voldoen aan de volgende acht eisen:

1. De NVAO verwerkt alleen persoonsgegevens als voor de verwerking een rechtmatige grondslag aanwezig is en een duidelijk omschreven en gerechtvaardigd doel.
2. De NVAO beperkt de verwerking tot die categorieën persoonsgegevens die nodig zijn voor het beschreven doel.
3. De NVAO verwerkt persoonsgegevens die accuraat en actueel zijn.
4. De NVAO bewaart gegevens niet langer dan noodzakelijk voor het beschreven doel.
5. De NVAO is, als dat mogelijk is, open en transparant over de verwerking van persoonsgegevens aan de betrokkene, de samenleving en ketenpartners.
6. De NVAO zorgt dat persoonsgegevens die aan ons zijn toevertrouwd, veilig en vertrouwelijk worden verwerkt.
7. De NVAO legt verantwoording af over de zorgvuldige verwerking van persoonsgegevens.
8. De NVAO respecteert de rechten van de betrokkenen.

⁵ Het OECD is de organisatie voor economische samenwerking en ontwikkeling. De OECD heeft in 1980 principes opgesteld en in 2013 zijn deze voor het laatst herzien.

Hieronder volgt een nadere instructie per uitgangspunt.

2.1 Grondslag en doel

De NVAO verwerkt alleen persoonsgegevens als voor de verwerking een rechtmatige grondslag aanwezig is en een duidelijk omschreven en gerechtvaardigd doel.

Instructies:

- ⇒ Persoonsgegevens mogen alleen verwerkt worden als een van de rechtmatige grondslagen uit artikel 6 van de AVG aanwezig is. Te denken valt bijvoorbeeld aan: verwerking van persoonsgegevens ter uitvoering van een overeenkomst.
- ⇒ Persoonsgegevens mogen eveneens alleen verwerkt worden indien de NVAO in het kader van zijn taken verwerkingen verricht, die "noodzakelijk voor de uitvoering van een wettelijke plicht" zijn en "noodzakelijk voor het uitoefenen van een publiekrechtelijke taak of uitoefenen van openbaar gezag". De rechtsgrondslag van een dergelijke taak moet in de WHW of in het Decreet zijn verankerd.
- ⇒ De grondslag "noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerker of van de verwerkingsverantwoordelijke of van een derde" kan niet worden gebruikt als er sprake is van verwerkingen door overheidsinstanties in het kader van de uitoefening van hun taken. Dit kan wel in beeld komen bij een verwerking in het kader van de bedrijfsvoering (denk bijvoorbeeld aan cameratoezicht rond het gebouw).
- ⇒ De ongelijke machtsverhouding tussen betrokkene en de overheid staat over het algemeen in de weg aan de eis dat betrokkene de toestemming vrijelijk moet verlenen.
- ⇒ Een (aanpassing van) verwerking moet steeds worden opgenomen in het Register van verwerkingen. Dit register geeft een beschrijving van verwerkingsactiviteiten. De verantwoordelijke (de NVAO) moet dit op verzoek aan de AP kunnen laten zien. Neem bij een dergelijk verzoek van de AP contact op met de privacy officer die dit in afstemming met bestuurder verzorgt. Het Register van verwerkingen bevat zelf geen persoonsgegevens.
- ⇒ Het doel van elke verwerking is concreet en vastgelegd in het Register van verwerkingen. Als een bestand voor meer doelen wordt gebruikt dan wordt dat vermeld in de doelomschrijving. Doelen die duidelijk zijn omschreven maken het voor betrokkene inzichtelijk wat met de gegevens wordt gedaan. Bij verdere verwerking van persoonsgegevens voor een ander doel dan waarvoor de gegevens oorspronkelijk zijn verzameld, wordt altijd beoordeeld of dit nieuwe doel verenigbaar is met het oorspronkelijke doel.
- ⇒ De NVAO is verplicht een Data Protection Impact Assessment, DPIA (ook wel genoemd Gegevensbeschermingseffect-beoordeling, GEB), uit te voeren bij de ontwikkeling van beleid en regelgeving waaruit verwerkingen van persoonsgegevens voortvloeien. De AP heeft een lijst van verwerkingen opgesteld waarvoor de DPIA verplicht is.⁶ De DPIA is bedoeld om de effecten van de beoogde gegevensverwerking(en) voor betrokkenen te inventariseren en te beoordelen. Op basis van de DPIA kunnen maatregelen worden genomen om de risico's aan te pakken. Gebruik hiervoor het Rijksmodel GEB (PIA) of het model dat in Privacy Nexus is opgenomen.

⁶ <https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667>

- ⇒ Vragen over het proces, de opzet en uitvoering van de DPIA kun je stellen aan de privacy officer en de Functionaris Gegevensbescherming. Raadpleeg eventueel het document DPIA Proces NVAO.

2.2 Doelbinding

De NVAO beperkt de verwerking tot die categorieën persoonsgegevens die nodig zijn voor het beschreven doel.

Instructies:

- ⇒ Alleen de voor het vooraf en precies omschreven doel noodzakelijke gegevens mogen worden verzameld. Gegevens mogen vervolgens niet verder worden verwerkt als dit onverenigbaar is met dat doel. Persoonsgegevens die niet meer nodig zijn (moeten) worden verwijderd of waar mogelijk geanonimiseerd.⁷ Bij de ontwikkeling van nieuwe (of wijziging van bestaande) producten en diensten wordt met gegevensbescherming rekening gehouden.
- ⇒ Verwerk niet meer gegevens dan die aantoonbaar noodzakelijk zijn voor het doel van de verwerking (*dataminimalisatie*). Bedenk waarom je gegevens voor die specifieke verwerking nodig hebt en of je daadwerkelijk alle gegevens nodig hebt.
- ⇒ Nieuwe systemen worden geconfigureerd op een zodanige wijze dat alleen de voor het specifieke verwerkingsdoel noodzakelijke gegevens worden verwerkt. Privacy moet dus bij het ontwerp van een (nieuw) automatiseringssysteem als uitgangspunt worden genomen. (*privacy by design*).
- ⇒ Ga bij het ontwikkelen van beleid, processen (en systemen) altijd uit van de meest privacybeschermende instellingen (*privacy by default*).
- ⇒ Raadpleeg bij het ontwikkelen en uitwerken van beleid, processen en systemen de Handleiding Privacy by Design & by Default om meer zicht te krijgen op privacyvriendelijk ontwerp waarin de bescherming van persoonsgegevens is ingebouwd.⁸

2.3 Accuraat en actueel

De NVAO verwerkt persoonsgegevens die accuraat en actueel zijn. Dit betekent onder meer dat er sprake is van zorgvuldig beheer van gegevens (*betrouwbaarheid en integriteit*) en dat het voor betrokkenen mogelijk is om verzoeken met betrekking tot rectificatie van onjuiste persoonsgegevens in te dienen (*rechten van betrokkenen*).

Instructies:

- ⇒ Zorg dat de juistheid en actualiteit van de persoonsgegevens zoveel mogelijk gewaarborgd is door periodieke controles en/of controle op bestaande gegevens of input, bijvoorbeeld wanneer panelleden opnieuw zitting nemen in een panel.

⁷ De AVG is niet van toepassing op anonieme gegevens omdat deze gegevens niet terug te voeren zijn op een geïdentificeerde of identificeerbare natuurlijke persoon. Anonimisering is versleuteling die onomkeerbaar is, het niet meer mogelijk om deze later weer met personen in verband te brengen. Bij pseudonimisering kunnen anonieme gegevens met de juiste sleutel inzichtelijk gemaakt worden, waardoor herleiding naar natuurlijke personen weer mogelijk is. De AVG is wel van toepassing op gepseudonimiseerde gegevens.

⁸ https://www.cip-overheid.nl/media/1136/20170507-handleiding-privacy-by-design-v3_0.pdf

- ⇒ Zorg dat het mogelijk is om gegevens aan te passen daar waar zij onjuist, onvolledig of verouderd zijn.
- ⇒ Raadpleeg desgewenst Protocol Rechten van Betrokkenen.

2.4 Bewaarbeperking

De NVAO bewaart gegevens niet langer dan noodzakelijk voor het beschreven doel of zolang als bepaald door een specifieke wet.

Instructies:

- ⇒ De NVAO heeft maximale bewaartermijnen bepaald en geïmplementeerd voor alle persoonsgegevens waarover de organisatie mag beschikken. Nadat een bewaartermijn is verstreken, moeten de persoonsgegevens verwijderd worden of geanonimiseerd⁹.
- ⇒ Persoonsgegevens kunnen meerdere doelen dienen. Houd hiermee rekening bij het opstellen van de bewaartermijnen.
- ⇒ Bewaar persoonsgegevens niet langer dan noodzakelijk voor de doelen van de verwerking.
- ⇒ Stel bewaartermijnen vast conform de Memo Bewaartermijn Persoonsgegevens in de AVG.
- ⇒ Wis gegevens wanneer deze niet langer noodzakelijk zijn voor het verwerkingsdoel.
- ⇒ Raadpleeg desgewenst de Handreiking Bewaren van e-mail Rijksoverheid en de Selectielijst van de NVAO.

2.5 Open en transparant

De NVAO is, als dat mogelijk is, open en transparant over de verwerking van persoonsgegevens aan de betrokkene, de samenleving en ketenpartners. Een betrokkene dient te weten wat er met zijn persoonsgegevens gebeurt. De informatie over de verwerking en de omgang met de gegevens en over de rechten van betrokkene dient eenvoudig toegankelijk en begrijpelijk te worden aangeboden. Dit gebeurt in een interne en een externe privacyverklaring.

Instructies:

- ⇒ De NVAO verstrekt de vereiste informatie over onze verwerkingsactiviteiten voor o.a. burgers en studenten via de externe privacyverklaring op www.nvao.net.
- ⇒ De NVAO verstrekt vereiste informatie voor bestuursleden en medewerkers via de interne privacyverklaring op intranet of Sharepoint.
- ⇒ Zowel de interne als de externe privacyverklaring worden periodiek door het privacy office op actualiteit gecontroleerd.

⁹ Zie voetnoot 7

- ⇒ Raadpleeg desgewenst de Handreiking Veilige omgang met persoonsgegevens of de Personeelsregeling.

2.6 Veilig en vertrouwelijk

De NVAO zorgt dat persoonsgegevens die aan ons zijn toevertrouwd, veilig en vertrouwelijk worden verwerkt.

Instructies:

- ⇒ De NVAO is verplicht (op basis van wet- en regelgeving) om passende technische en organisatorische maatregelen te treffen om persoonsgegevens een passend beschermingsniveau te bieden tegen ongeautoriseerde verwerkingen. De NVAO heeft hiertoe een Handreiking Veilige omgang met Persoonsgegevens opgesteld.
- ⇒ De NVAO verstrekt alleen toegang tot persoonsgegevens aan die mensen die toegang tot de gegevens nodig hebben en die toestemming hebben om gegevens verder te verwerken.
- ⇒ Datalekken moeten zoveel mogelijk worden voorkomen. Een datalek is een inbreuk op de beveiliging van de persoonsgegevens die leidt tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking of toegang tot gegevens.
- ⇒ Een datalek dat een risico voor de rechten van betrokkene inhoudt moet binnen 72 uur aan de Autoriteit Persoonsgegevens (AP) worden gemeld en soms ook aan betrokkene. Hiervoor is het Protocol datalekken NVAO opgesteld. Raadpleeg bij een (vermeend) datalek de privacy officer.
- ⇒ Via de e-mail worden veel bestanden uitgewisseld en dus ook vaak persoonsgegevens. Het is belangrijk om een passend beschermingsniveau toe te passen bij het versturen van dergelijke gegevens. Bij het versturen van bestanden met persoonsgegevens is het passend om deze gegevens versleuteld te versturen naar de ontvanger. Op die manier wordt het risico verkleind dat er per ongeluk bestanden naar de verkeerde ontvanger worden gestuurd. Als het nodig is om gegevens versleuteld te versturen naar de ontvanger, verstuur deze bijvoorbeeld door middel van een versleutelde omgeving.
- ⇒ De NVAO en in het bijzonder het privacy office houdt een register bij van datalekken en beveiligingsincidenten.
- ⇒ Raadpleeg eventueel het Autorisatiebeleid en het Beveiligingsbeleid.

2.7 Verantwoordingsplicht

De NVAO legt verantwoording af over de zorgvuldige verwerking van persoonsgegevens.

Instructies:

- ⇒ De NVAO neemt passende maatregelen om de bescherming van persoonsgegevens te waarborgen. Aan de hand van documentatie kan de NVAO aantonen dat de privacyregels worden nageleefd. Evaluatie, monitoring en logging van de maatregelen maakt ook onderdeel uit van de verantwoording. Deze verantwoordingsplicht (*accountability*) staat centraal in het nieuwe wettelijk privacykader.

- ⇒ Het privacy office van de NVAO beheert een Register van verwerkingen. In dat register staat informatie over de gegevens die worden verwerkt. De persoonsgegevens zelf staan niet in het register, wel welke categorieën persoonsgegevens er worden verwerkt.
- ⇒ Wijzigingen in verwerkingen moeten door medewerkers en/of leden van het managementteam aan de privacy officer worden doorgegeven.
- ⇒ De managers van de afdelingen Nederland en Vlaanderen hebben een zelfstandige verantwoordelijkheid om bij nieuwe verwerkingen (activiteiten/andere ICT systemen) de privacy officer en de FG op de hoogte te stellen.
- ⇒ De NVAO vergewist zich ervan dat derde partijen behoorlijk en zorgvuldig met persoonsgegevens omgaan. Dit hoeft niet noodzakelijkerwijs te gaan over partijen waarmee een verwerkersovereenkomst mee afgesloten dient te worden. Denk hierbij aan de Arbodienst die een eigen verwerkingsverantwoordelijkheid heeft. Waar nodig wordt een verwerkingsovereenkomst gesloten; deze wordt opgenomen in het Register Verwerkingsovereenkomsten (in de tool Nexus).
- ⇒ Raadpleeg Juridische Zaken bij vragen. Een Format verwerkersovereenkomst en Checklist verwerkersovereenkomst zijn beschikbaar.

2.8. Respect

De NVAO respecteert de rechten van de betrokkenen.

Instructies:

- ⇒ De NVAO richt systemen, processen en de interne organisatie zodanig in dat op de juiste manier gehoor wordt gegeven aan verzoeken van betrokkenen omtrent persoonsgegevens.
- ⇒ De NVAO hanteert een Protocol Rechten Betrokkenen, waarin de (belangrijkste) rechten van betrokkenen zijn/worden geformuleerd, zoals inzage, rectificatie, wissen, overdracht en beperking van verwerking. Ook wordt in dit protocol vermeld hoe een bepaald verzoek wordt behandeld en waar een betrokkene rekening mee kan houden. Op www.nvao.net kan een betrokkene deze informatie in begrijpelijke taal vinden.
- ⇒ De NVAO kan gebruik maken van een model voor de beantwoording van inzageverzoeken of van andere modellen om aan verzoeken te voldoen.
- ⇒ In de interne en externe privacyverklaringen worden o.a. de rechten van betrokkenen ten aanzien van hun persoonsgegevens omschreven. In beide privacyverklaringen wordt omschreven voor wie de betreffende privacyverklaring geldt.
- ⇒ Alle betrokkenen (intern en extern) kunnen bij de Autoriteit Persoonsgegevens (AP) een klacht indienen over de manier waarop de NVAO met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.

3. Privacy governance

3.1 Inleiding

Doel van dit hoofdstuk over de privacy governance is inzicht te geven in de verantwoordelijkheden op het gebied van de privacybescherming binnen de NVAO. De governancestructuur helpt de NVAO om zorgvuldig met persoonsgegevens om te gaan en verantwoording af te kunnen leggen over genomen beslissingen. Een robuuste beheersorganisatie is van belang voor de implementatie en handhaving van de principes en doelstellingen uit het privacybeleid.

Omgevingsveld

De NVAO is een zelfstandig bestuursorgaan en valt onder de politieke verantwoordelijkheid van het *Comité van Ministers*. Hoewel de NVAO een zelfstandig bestuursorgaan is, blijft het Comité van Ministers politiek verantwoordelijk voor compliance met wet- en regelgeving en dus ook de AVG.

De *Autoriteit Persoonsgegevens* (AP) is de toezichthoudende autoriteit met betrekking tot het voldoen aan de vereisten van de AVG. Wanneer betrokkenen klachten hebben over hoe de NVAO omgaat met persoonsgegevens, kunnen zij terecht bij de AP.

De *Nationale Ombudsman* kan eventueel ook nog een bemiddelende rol spelen tussen de NVAO en personen waarvan de NVAO gegevens verwerkt.

3.2 Privacy verantwoordelijkheden rollen en taken

Privacy gaat de gehele NVAO aan en ziet ook op de gehele organisatie. Met elkaar werken we aan de naleving van het privacybeleid en draagt de NVAO als bestuursorgaan hiervoor verantwoordelijkheid.

Welke organen en personen dragen bij aan het privacybeleid of spelen een rol?

- | | |
|---------|---------------------------------------|
| 1. AB | Algemeen Bestuur |
| 2. DB | Dagelijks Bestuur |
| 3. DN | Directeur Nederland |
| 4. DV | Directeur Vlaanderen |
| | |
| 5. FG | Functionaris voor gegevensbescherming |
| 6. PO | Privacy office |
| 7. IM | Informatiemanager |
| | |
| 8. AHN | Afdelingshoofd Nederland |
| 9. HR | Hoofd HR |
| 10. HF | Hoofd Financiën |
| | |
| 11. RB | Relatiebeheer |
| 12. Com | Communicatie |
| | |
| 13. OR | Ondernemingsraad |
| | |
| 14. Mw | medewerker |

N.B. 3, 4, 8, 9 en 10 vormen samen het Management Team, ofwel MT

In het RASCI model (zie Bijlage 3) is uitgewerkt wie verantwoordelijk is voor welk onderdeel van de AVG. Meer in het algemeen staat hieronder beschreven bij wie, welke rollen en taken binnen de NVAO bij de uitvoering van de AVG zijn belegd.

De lijn: AB, DB, MT

Overeenkomstig de mandaatstructuur binnen de NVAO zijn het bestuur, de directeuren, het afdelingshoofd NL, en de hoofden HR en Financiën verder verantwoordelijk voor de strategische visie, de risicobeheersing en voor het borgen van de aantoonbare naleving van de wet- en regelgeving op het terrein van privacybescherming. Het MT is een overlegorgaan van de Directeur Nederland, Directeur Vlaanderen, Afdelingshoofd Nederland, Hoofd HR en Hoofd Financiën. Beslissingen over de dagelijkse gang van zaken binnen de NVAO worden in het MT besproken. Vaak volgt hieruit een formele beslissing. Deze beslissing is dan (mandaattechnisch) toe te rekenen aan de Directeur Nederland. Het Afdelingshoofd Nederland heeft als MT-lid de juridische aspecten van privacy in zijn pakket en is daarmee als eerste het aanspreekpunt voor privacy.

De (niet met toezicht belaste) specialisten: PO, Informatiemanager en HR

Naast een privacy officer heeft de NVAO een Informatiemanager. De privacy officer en de Informatiemanager adviseren, ondersteunen en controleren de directie, het bestuur en de medewerkers bij privacy aspecten. Ook bepaalde beleidstaken en het organiseren van interne risicoanalyses behoren tot hun takenpakket. Primair is de privacy officer het aanspreekpunt voor de uitleg van de AVG binnen de NVAO en bij de implementatie en uitvoering van de AVG.

Daarnaast heeft HR een rol als het gaat om de zorgvuldige omgang met persoonsgegevens. HR is het eerste aanspreekpunt bij personeelsgerelateerde vragen van medewerkers over de AVG.

Taakomschrijvingen meer specifiek van de FG, het PO en de IM:

Functionaris Gegevensbescherming (FG)¹⁰

De NVAO heeft een interne FG aangesteld overeenkomstig artikel 37 e.v. van de AVG. De FG rapporteert aan de voorzitter van het bestuur. In de AVG is de rol van de FG als volgt beschreven:

- informeren en adviseren van het lijnmanagement over hun verplichtingen uit hoofde wet- en regelgeving in het kader van privacy;
- toezien op de naleving van de relevante wetgeving, het privacybeleid en de inrichting van de interne privacy organisatie;
- advies leveren bij een DPIA, zowel de inhoudelijke beoordeling als de naleving van de voorgenomen beheermaatregelen;
- samenwerken met de AP, de centrale toezichthouder, in het geval van onderzoek;
- aanspreekpunt voor betrokkenen (burgers en medewerkers) voor alle aangelegenheden bij de verwerking van hun persoonsgegevens.

Jaarlijks kan de FG een werkplan privacy office opstellen in het kader van zijn toezichthoudende werkzaamheden.

Privacy office (PO)

- De NVAO heeft een privacy office¹¹ dat de volgende taken verricht: informeren en adviseren van het lijnmanagement over hun verplichtingen uit hoofde wet- en regelgeving in het kader van privacy;
- toezien op de naleving van de relevante wetgeving, het privacybeleid en de inrichting van de interne privacy organisatie;
- advies leveren bij een DPIA, zowel de inhoudelijke beoordeling als de naleving van de voorgenomen beheermaatregelen;
- samenwerken met de AP, de centrale toezichthouder, in het geval van onderzoek;

¹⁰ <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/functionaris-gegevensbescherming-fg>

¹¹ Juridische Zaken fungeert als Privacy Office op het moment van inwerkingtreding van dit beleid; eventuele wijziging wordt gecommuniceerd.

- aanspreekpunt voor betrokkenen (burgers en medewerkers) voor alle aangelegenheden bij de verwerking van hun persoonsgegevens.

Informatiemanager (IM)

Het onderwerp privacy en gegevensbescherming heeft een multidisciplinair karakter. Het vraagt om een zorgvuldige afstemming met de experts van juridische zaken, ICT, beveiliging, communicatie, de privacy en de FG.

De informatiemanager heeft onder meer als taak:

- Opstellen informatievoorziening strategie en beleid en vertalen naar de techniek;
- Opstellen en actualiseren informatiebeveiligingsbeleid en de daaruit voortvloeiende plannen;
- Inrichten van de informatiebeveiligingsorganisatie en het coördineren en afhandelen van beveiligingsincidenten;
- Ophalen en vertalen van externe ontwikkelingen (wetgeving, technologie, bedrijfsvoering) naar consequenties en aanpassingen voor de informatievoorziening;
- Monitoren van relevante risico's voor de organisatie;
- Monitoren en borgen van de eisen en architectuur voor informatiebeveiliging en het consequent toepassen van Security-by-Design en Privacy-by-Design.

De IM is in eerste instantie verantwoordelijk voor de informationele privacy. De IM ondersteunt en adviseert de NVAO bij privacyvraagstukken. De IM helpt onder meer door het geven van (zo mogelijk) advies op maat, het opbouwen van de noodzakelijke kennis over privacy wet- en regelgeving, het toepassen hiervan en het (mede-)ontwikkelen van producten zoals informatiebeleid en privacy convenanten.

Wat is de rol van de OR¹² bij privacyvraagstukken?

De ondernemingsraad vertegenwoordigt het personeel van de NVAO en beschermt hun belangen. De ondernemingsraad heeft daarvoor verschillende rechten en bevoegdheden, zoals het recht op informatie, het adviesrecht, het instemmingsrecht en het initiatiefrecht. Met name het adviesrecht, instemmingsrecht en het initiatiefrecht spelen een rol bij de uitvoering van de AVG. Artikel 27 WOR

Het kan zijn dat er nieuwe technische maatregelen worden getroffen om te voldoen aan de AVG. Denk bijvoorbeeld aan technische maatregelen om persoonsgegevens te beveiligen of om ervoor te zorgen dat alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor het verwerkingsdoel.

Op grond van de Wet op de Ondernemingsraden (WOR) dient een besluit tot het invoeren of wijzigen van een technologische voorziening ter advies aan de ondernemingsraad te worden voorgelegd. Dus als de NVAO wil over gaan tot de aanschaf van nieuwe ICT ter beveiliging van de persoonsgegevens, dan heeft de OR adviesrecht.

Een besluit tot vaststelling, wijziging of intrekking van een regeling over het verwerken van, alsmede de bescherming van de bij de NVAO werkzame personen is instemmingsplichtig. Het moet dus gaan om een regeling die tot doel heeft persoonsgegevens te verzamelen, bewaren, gebruiken, verstrekken of beveiligen. Dit geldt onder meer voor de vaststelling van dit privacybeleid en voor het melden van een datalek waarbij persoonsgegevens zijn betrokken.

De ondernemingsraad kan tenslotte gebruikmaken van haar initiatiefrecht om voorstellen te doen voor een (een aanpassing van) het privacybeleid.

3.3 Privacy overlegstructuren

¹² <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-uitkering/ondernemingsraad>

Privacy moet als vast onderdeel opgenomen zijn op de agenda's van de reguliere overleggen tussen JZ/Directie alsook tussen JZ/Directie en HRM, Directie/Financiën, Dir/com, Dir/ICT en Dir/ICT-stuurgroep. Er is tenslotte ook nog een vast maandelijks overleg tussen het privacy office en de Functionaris Gegevensbescherming.

De NVAO doet daarnaast mee aan overleggen van KleinLef organisaties op het gebied van privacy om de kennis omtrent privacy te delen en elkaar te helpen om beleid omtrent privacy te ontwikkelen.

3.4 Sturing, regie en toezicht

Periodiek voert de NVAO met behulp van de tool in Privacy-Nexus self-assessments uit, waaruit blijkt wat de stand van zaken is met betrekking tot privacy.

De FG ziet toe op de naleving van de relevante wetgeving, het privacybeleid en de inrichting van de interne privacy organisatie.

Interne toezichtsorganen: FG en OR

Tenslotte kent de NVAO een Functionaris Gegevensbescherming (FG) en de Ondernemingsraad (OR). Zij zijn vanwege hun specifieke rollen en wettelijke taken bij aspecten van de privacy van de NVAO betrokken.

Externe toezichthouders, zoals de Autoriteit Persoonsgegevens (AP) en al dan niet ingehuurde auditors kunnen de inregeling en uitvoering van de AVG controleren. Het is de eigen verantwoordelijkheid van de NVAO om intern toezicht te houden op de waarborging van privacybescherming, los van eventuele externe audits en evaluaties.

3.5 Privacy trainingen en bewustwording

Alle medewerkers krijgen bij hun aanstelling een korte introductie AVG van de PO/FG. De tekst van de eed/belofte is in de Personeelsregeling opgenomen; hierin ligt de geheimhouding t.a.v. AVG besloten.

Daarnaast vinden reguliere bewustwordingsacties plaats, door minimaal één keer per jaar aandacht voor een privacy onderwerp vanuit het privacy office en minimaal één bureaubijeenkomst per jaar over een AVG onderwerp. Daarnaast worden medewerkers ook geïnformeerd over de AVG en privacy, doordat dit onderwerp een integraal onderdeel uitmaakt van de besprekingen van het Dagelijks Bestuur. De verslagen hiervan zijn voor medewerkers te raadplegen.

4. Slot

Met dit privacybeleid brengt de NVAO in kaart welke maatregelen er zijn genomen om de persoonsgegevens van medewerkers en externen, waaronder o.a. panelleden, secretarissen en studenten, te beschermen. Daarnaast geeft het beleid inzicht in de wijze waarop de verantwoordelijkheden op grond van de AVG zijn belegd bij de NVAO. Ook is per uitgangspunt vastgelegd welke instructies er zijn en welke documenten geraadpleegd kunnen worden. Hiermee wordt voldaan aan belangrijke verplichtingen op grond van de AVG, zoals het inrichten en bijhouden van een Register van verwerkingen, de wijze waarop omgegaan wordt met datalekken, het houden van een DPIA, het opstellen van een interne en externe privacyverklaring en de wijze waarop rechten van betrokkenen zijn georganiseerd.

4.1 Beheer

Het privacy office van de NVAO is verantwoordelijk voor het beheer van dit privacy beleidskader. De instrumenten en dit beleidskader zijn levende documenten die periodiek (moeten) worden geactualiseerd. Algemene vragen over dit beleid of suggesties tot wijziging of toevoeging aan het beleid, kunnen worden gericht aan het privacy office van de NVAO (privacy@nvao.net).

4.2 Vaststelling

Dit privacybeleid is voor het eerst vastgesteld op door het Algemeen Bestuur van de NVAO.

4.3 Wijzigingen en evaluatie

Privacybeleid is dynamisch beleid. Nieuwe ontwikkelingen volgen elkaar op en ook de organisatie zelf zal steeds in ontwikkeling zijn. Dit betekent dat het privacybeleid ook met regelmaat bijgesteld zal moeten worden. Dit beleid wordt periodiek herzien en bijgewerkt. De volgende tabel toont de (concept)versie geschiedenis van dit privacy beleid. Evaluatie vindt in beginsel ieder jaar plaats, tenzij anders bepaald.

Datum	Opmerkingen	Versie
16-10-2019	1 ^{ste} concept beleidsdocument	0.1
27-07-2020	Concept tbv FG	0.2
2-11-2020	Concept tbv Luut	0.3

BIJLAGE 1: BEGRIPPEN

Wat zijn persoonsgegevens?

Niet alle data of gegevens zijn per definitie persoonsgegevens. Persoonsgegevens betreft alle informatie met betrekking tot een geïdentificeerde of identificeerbare natuurlijke persoon (de "betrokkene").

De betrokkene hoeft geen direct geïdentificeerd individu te zijn, maar zodra een individu uit een groep kan worden onderscheiden, zijn de gegevens persoonsgegevens. Het is dus niet altijd nodig om de naam te weten van de persoon in kwestie om te spreken van persoonsgegevens.

Alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare persoon moeten als persoonsgegevens worden beschouwd. Enkel transactiegegevens zijn bijvoorbeeld op zichzelf geen direct identificeerbare gegevens, maar worden persoonsgegevens wanneer deze verband houden met een geïdentificeerde of identificeerbare persoon, bijvoorbeeld omdat deze is gekoppeld aan een naam, een e-mailadres of een telefoonnummer.

De AVG heeft een speciaal regime voor bijzondere categorieën persoonsgegevens. Dit betreffen persoonsgegevens waaruit de raciale of etnische afkomst, politieke opvattingen, religieuze of filosofische overtuigingen blijken, lidmaatschap van een vakvereniging, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie, gezondheids- of medische gegevens, gegevens over iemands seksleven of seksuele geaardheid.

Strafrechtelijke persoonsgegevens zijn persoonsgegevens die te maken hebben met strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen. Hieronder vallen zowel veroordelingen als mogelijk gegronde verdenkingen. Dit wil zeggen dat er concrete aanwijzingen zijn dat iemand een strafbaar feit heeft gepleegd. Een voorbeeld hiervan is een opgestelde zwarte lijst van frauderende klanten bij een financiële instelling. Onder de AVG gelden speciale regels voor het verwerken van strafrechtelijke gegevens.

De verwerking, het verzamelen of gebruiken, van gevoelige persoonsgegevens, is verboden, tenzij een uitzondering op het algemene verbod van toepassing is. Het verzamelen en gebruiken van dergelijke gegevens zal daarom zoveel mogelijk worden vermeden. Vermijd ook het verzamelen en gebruik van gegevens van gevoelige groepen, zoals kinderen / minderjarigen, gehandicapten en ouderen, tenzij hiervoor duidelijk toestemming is gegeven door de bevoegde persoon.

Hieronder volgen voorbeelden van gegevens die over het algemeen als persoonsgegevens worden beschouwd:

Voornaam en / of initialen en achternaam	Financiële gegevens
E-mailadres	Betaling of transactiegegevens
Telefoonnummer	Rijbewijs
Foto	Strafrecht ketennummer
Geboortedatum / geboorteplaats	Identificatienummer werknemer
IP-adres	Werknemers informatie
Uitkomsten functioneringsgesprekken	Medische informatie
Burgerservicenummer	Biometrische gegevens

Unique Device Identifiers	MAC-adressen
---------------------------	--------------

Wat is een betrokkene?

De betrokkene is de persoon van wie persoonsgegevens worden verwerkt.

Wat is een verwerking?

Het 'verwerken van persoonsgegevens' of een 'verwerking van persoonsgegevens' betreft alle handelingen die men met persoonsgegevens kan verrichten. Denk hierbij aan het verzamelen, vastleggen, raadplegen, opvragen, ordenen, structureren, opslaan, bewerken of wijzigen, verstrekken en combineren. Ook het wissen of vernietigen van gegevens is een verwerking van persoonsgegevens.

Wat is een verwerkingsverantwoordelijke?

De verwerkingsverantwoordelijke is de natuurlijke persoon of rechtspersoon die (alleen of tezamen met anderen) bepaalt welke persoonsgegevens worden verzameld, waarom persoonsgegevens worden verwerkt (doel) en hoe persoonsgegevens worden verwerkt (middelen). Wanneer partijen gezamenlijk het doel en de middelen vaststellen voor de verwerking van persoonsgegevens dan spreken we van een gezamenlijke verantwoordelijkheid.

Wat is een verwerker?

Een verwerker is de natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Het gaat om derde partijen die voor de verwerkingsverantwoordelijke werken. Een verwerker handelt onder de verantwoordelijkheid van de verwerkingsverantwoordelijke en naar diens instructies, maar er is geen hiërarchische relatie (medewerkers zijn geen verwerkers). Daarnaast heeft de verwerker geen zeggenschap over de verwerkingen en mag de gegevens niet voor eigen doelen gebruiken.

BIJLAGE 2. INSTRUMENTEN

Wet- en regelgeving

AVG Algemene Verordening Gegevensbescherming

UAVG Uitvoeringswet Algemene Verordening Gegevensbescherming

Websites

EDPS European Data Protection Supervisor, <https://edps.europa.eu/>

AP Autoriteit Persoonsgegevens, <https://autoriteitpersoonsgegevens.nl/>

Nr	Naam document	Bron met koppeling	Vindplaats in H2 privacybeleid	Gereed in map
	Autorisatiebeleid	?	2.6	
	Beveiligingsbeleid	?	2.6	
	Checklist verwerkersovereenkomst	Website voegen	2.7	√
	DPIA Proces NVAO	?	2.1	
	DPIA-register	Privacy Nexus (tool)	Zou in 2.1 moeten staan	In tool
	Externe Privacyverklaring NVAO	i.o.	2.5 en 2.8	cpt
	Format verwerkersovereenkomst	Privacy Company	2.7	√
	Handleiding Privacy by Design (versie 3.0 CIP)	Centrum informatiebeveiliging en privacybescherming ?	2.2	
	Handreiking Bewaren van e-mail Rijksoverheid	rijksoverheid	2.4	√
	Handreiking Veilige omgang met persoonsgegevens	?	2.5 en 2.6	
	Interne Privacyverklaring	intranet	2.5 en 2.8	
	Memo Quick Scan DPIA		Zou in 2.1 ...	
	Protocol datalekken NVAO	i.o.	2.6	cpt
	Register datalekken en beveiligingsincidenten		2.6	
	Protocol Rechten van betrokkenen NVAO	i.o.	2.3 en 2.8	cpt
	Register van verwerkingen	Privacy Nexus (tool)	2.1 en 2.7	Cpt in excel
	Register Verwerkingsovereenkomsten	Privacy Nexus (tool)	2.7	Nu op z-schijf
	Rijksmodel GEB	PIA	2.1	√
	Selectielijst van de NVAO	Staatscourant	2.4	√

N.B. INDIEN LINKS NIET WERKEN, GRAAG PRIVACY OFFICE RAADPLEGEN: NVAO - DOCUMENTEN\JURIDISCHE ZAKEN\AVG\PRIVACYBELEID\BIJLAGE 2 INSTRUMENTEN

BIJLAGE 3: RASCI MODEL

N.B. INDIEN LINKS NIET WERKEN, GRAAG PRIVACY OFFICE RAADPLEGEN: NVAO -
DOCUMENTEN\JURIDISCHE ZAKEN\AVG\PRIVACYBELEID\BIJLAGE 2 INSTRUMENTEN

BIJLAGE 3: RASCI MODEL

Zie los document in liggend beeld.

1C

Privacy Beleidskader
Nederlands Vlaamse Accreditatieorganisatie

Datum: 16-2-2021
Status: Goedgekeurd door DB d.d. 16 februari 2021

Artikel 5.2 lid 1 e
Artikel 5.2 lid 1 e
Directeur Nederland
Voorzitter Algemeen Bestuur

Artikel 5.2 lid 1 e
Artikel 5.2 lid 1 e
Luut Kroes
Anne Flierman

Concept 04

Inhoud

Voorwoord

1. Privacy beleidskader
 - 1.1 Doel
 - 1.2 Scope NVAO /CDHO/CMMBO
 - 1.3 Doelgroepen
 - 1.4 Wet- en regelgeving verwerking van persoonsgegevens
 2. NVAO uitgangspunten voor omgang met persoonsgegevens
 - 2.1 Grondslag en doel
 - 2.2 Doelbinding
 - 2.3 Accuraat en actueel
 - 2.4 Bewaarbeperking
 - 2.5 Open en transparant
 - 2.6 Veilig en vertrouwelijk
 - 2.7 Verantwoordingsplicht
 - 2.8 Respect
 3. Privacy governance
 - 3.1 Inleiding
 - 3.2 Privacy verantwoordelijkheden rollen en taken
 - 3.3 Privacy overlegstructuren
 - 3.4 Sturing, regie en toezicht
 - 3.5 Privacy trainingen en bewustwording
 4. Slot
 - 4.1 Beheer
 - 4.2 Vaststellen
 - 4.3 Wijzigingen en evaluatie
- Bijlage 1 Begrippen
Bijlage 2 Instrumenten (documenten, websites etc.)
Bijlage 3 RASCI model

Voorwoord

De Nederlands-Vlaamse Accreditatieorganisatie (NVAO) is een kwaliteitszorgorganisatie die op deskundige en onafhankelijke wijze de kwaliteit van het hoger onderwijs in Nederland en Vlaanderen borgt en die de kwaliteitscultuur binnen de instellingen voor hoger onderwijs in Nederland en Vlaanderen bevordert. Zij accrediteert bestaande en nieuwe opleidingen en beoordeelt de kwaliteitszorg van instellingen in het hoger onderwijs. Daarmee is de NVAO bewaker van de kwaliteit van het hoger onderwijs. De besluiten van de NVAO leiden tot erkenning van diploma's en titels en waar van toepassing tot bekostiging van opleidingen. De NVAO baseert haar beoordeling op advies van erkende deskundigen.

De NVAO werd in 2003 opgericht bij Verdrag tussen Nederland en Vlaanderen. De taken van de NVAO zijn in wetgeving vastgelegd. De NVAO wil ertoe bijdragen dat de kwaliteit van het hoger onderwijs in Vlaanderen en Nederland erkend wordt als internationaal aan de maat, maatschappelijk relevant en het vertrouwen geniet van studenten, werkgevers en de samenleving. Binnen de opdracht die in het accreditatieverdrag tussen Nederland en Vlaanderen aan de NVAO is toegekend, wil zij de kwaliteit van het hoger onderwijs borgen, verbeteringen stimuleren en een kwaliteitscultuur bevorderen.

Om dit werk goed te kunnen doen is verwerking van persoonsgegevens van medewerkers en de contactpersonen van ketenpartners en burgers noodzakelijk. De privacy van contactpersonen en relaties is erg belangrijk voor de NVAO en we hechten dan ook veel belang aan een correcte verwerking en gebruik van persoonsgegevens. De bescherming van persoonsgegevens is immers een grondrecht. De NVAO is verantwoordelijk voor de aantoonbare zorgvuldige omgang met persoonsgegevens.

De NVAO is een zelfstandig bestuursorgaan en opgericht naar Nederlands publiekrecht met de zetel in Den Haag. De NVAO valt onder verantwoordelijkheid van het Comité van Ministers. De NVAO heeft een nauwe samenwerking met de CDHO en CMMBO, die gebruik maken van de afdeling Ondersteuning en hostingsovereenkomsten hebben met de NVAO.

Dit privacy beleidskader richt zich tot iedereen die werkzaamheden verricht voor de NVAO en medewerkers van de CDHO en CMMBO. In het privacy beleidskader wordt uitgelegd hoe de NVAO aantoonbaar zorgvuldig omgaat met persoonsgegevens, wat daarbij de uitgangspunten zijn en wat de rol van de medewerker is bij de bescherming van persoonsgegevens.¹

Datum Ondertekening

Anne Flierman

Voorzitter Algemeen Bestuur NVAO

¹ Voor een beknopte uitleg van begrippen (als persoonsgegevens en verwerking) zie bijlage 1.

1. NVAO Privacy beleidskader

Op het werk van het Nederlands Vlaamse Accreditatieorganisatie (NVAO) is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Daarnaast heeft de NVAO te maken met bijzondere wetgeving, waarin een grondslag voor verwerking van gegevens kan liggen. Denk hierbij bijvoorbeeld aan de gegevens die de NVAO nodig heeft van panelleden om hun deskundigheid voor deelname aan een panel te kunnen beoordelen. Voor de Afdeling Vlaanderen is dit geregeld in de Codex Hoger Onderwijs, voor de Afdeling Nederland is dit vastgelegd in de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW).

Het NVAO Privacy beleidskader geeft aan waar de NVAO op het vlak van gegevensbescherming voor staat en wat de uitgangspunten voor de omgang met persoonsgegevens zijn. Met dit kader wil de NVAO ervoor zorgen dat de privacybescherming in lijn is met de wettelijke vereisten en die aansluit of geïntegreerd wordt bij de bestaande processen en systemen van de NVAO.

Bij alle uitgangspunten wordt steeds verwezen naar praktische ondersteunende instrumenten (checklists, stappenplan, procedures) van de NVAO dan wel (voor zover niet aanwezig) van OCW.

De uitleg van een aantal belangrijke begrippen uit de AVG is opgenomen in Bijlage 1: Begrippen.

1.1 Doel

Doel van dit beleidskader is een omgeving te creëren waarin elke medewerker van de NVAO:

- zijn of haar verantwoordelijkheid en rechten kent als het gaat om privacy en het verwerken van persoonsgegevens,
- in staat is om het juiste beleid en de juiste procedures te volgen,
- contact kan opnemen met de juiste personen wanneer er vragen zijn.

1.2 Scope

Het privacy beleidskader is bestemd voor de NVAO in zijn geheel. Alle handelingen binnen de NVAO met betrekking tot persoonsgegevens van burgers, bestuursleden, medewerkers, contactpersonen, zoals medewerkers kwaliteitszorg, panelleden en secretarissen, vallen allen binnen het bereik van dit beleidskader.

CMMBO en CDHO

Deze organisaties hebben zelfstandige taken en verantwoordelijkheden. Er is een nauwe samenwerkingsrelatie tussen de NVAO en de CMMBO/CDHO. Niet alleen zitten de organisaties fysiek in het pand bij de NVAO, de ondersteuning van CDHO en CMMBO is in dienst van de NVAO. Bovendien maken de drie organisaties gezamenlijk gebruik van de afdeling Ondersteuning van de NVAO (waaronder ICT, financiën en personeelszaken). Het privacybeleid van de NVAO omvat hiermee tevens de medewerkers werkzaam voor het secretariaat van CDHO en CMMBO. Het privacybeleid van de NVAO omvat niet de werkzaamheden van commissieleden CDHO en CMMBO, deze vallen onder verantwoordelijkheid van het Ministerie van Onderwijs, Cultuur en Wetenschap. Voor verwerkingen van de Commissie CDHO/CMMBO waar de NVAO verwerker is, wordt een verwerkingsovereenkomst gesloten.

1.3 Doelgroepen

Dit beleidskader is van toepassing op alle bestuurders, medewerkers, tijdelijke werknemers en op alle andere personen die namens de NVAO werken.

Het beleidskader is van toepassing op personen werkzaam in een ondersteunende functie, managementfunctie, juridische functie, staffunctie, beleidsfunctie, of in een andere discipline.

De aard van de werkzaamheden bepaalt het type privacyvraagstukken en afwegingen die voor de betreffende persoon relevant zijn.

1.4 Wet- en regelgeving verwerking van persoonsgegevens

A. Europese en Nederlandse wet- en regelgeving op het terrein van privacy

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Vanaf dat moment geldt dezelfde privacywetgeving in de hele Europese Unie.²

De AVG is rechtstreeks van toepassing. Daar waar de AVG ruimte laat voor nationale keuzes bij de uitvoering van de AVG, zijn deze ingevuld in de Uitvoeringswet AVG (UAVG).³

Naast genoemde wetgeving zijn er aanvullende documenten vanuit het Europees Comité⁴ voor gegevensbescherming waarmee (o.a.) verduidelijking wordt gegeven voor de toepassing van de AVG.

Daarnaast vormt ook de uitleg van de AVG (veelal vastgelegd in beleidsregels) door de Autoriteit Persoonsgegevens (AP) een belangrijke bron voor de naleving van de AVG. De AP gaat ervan uit dat verwerkingsverantwoordelijken als de NVAO de beleidsregels toepassen en adviezen opvolgen, dan wel gemotiveerd afwijken (comply or explain).

Links naar genoemde wetgeving en belangrijke documenten verband houdend met dit beleidskader zijn te vinden in Bijlage 2: Instrumenten.

B. Specifieke context NVAO

De AVG laat zich voor de NVAO het beste plaatsen vanuit het perspectief van de hoofdprocessen van de NVAO:

Het primaire proces

Het personeelsproces

Het betalingsproces

Het primaire proces

De NVAO is een kwaliteitszorgorganisatie die primair op deskundige en onafhankelijke wijze de kwaliteit van het hoger onderwijs in Nederland en Vlaanderen borgt en die de kwaliteitscultuur binnen de hogeronderwijsinstellingen in Nederland en Vlaanderen bevordert. Zij accrediteert bestaande en nieuwe opleidingen en beoordeelt de kwaliteitszorg van instellingen in het hoger onderwijs.

In Nederland zijn deze taken van de NVAO gebaseerd op de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW, hoofdstuk 5): het accrediteren van bestaande opleidingen, het toetsen van nieuwe opleidingen in het hoger onderwijs en het adviseren van de Minister in specifieke aangelegenheden zoals opgenomen in de WHW. Het is niet uitgesloten dat in de toekomst ook andere wet- en regelgeving als basis dient voor taken van de NVAO.

In Vlaanderen zijn deze taken gebaseerd op de Codex Hoger Onderwijs van oktober 2013. Deze wetgeving dient als uitgangspunt voor alle beoordelingsprocedures in het hoger onderwijs in Vlaanderen.

Het personeelsproces

Onder het personeelsproces worden alle verwerkingen geschaard die betrekking hebben op de persoonsgegevens van het eigen personeel van de NVAO.

Het betalingsproces

Onder het betalingsproces behoren alle verwerkingen die gerelateerd zijn aan het overmaken van geld aan leveranciers, commissieleden, personeel en eventuele andere partijen.

² Een e-privacy verordening (EPV), waarin zaken als cookieregels en het spamverbod nader worden geregeld, is in ontwikkeling.

³ Verder heeft de rijksoverheid een Handreiking naleving AVG geformuleerd. De NVAO overweegt nog hoe deze handreiking in te zetten.

⁴ European Data Protection Supervisor (EDPS), <https://edps.europa.eu/>

N.B. Verwerkingen van persoonsgegevens kunnen in digitale dan wel in papieren vorm plaatsvinden. De Handreiking veilige omgang met persoonsgegevens werkt dit verder uit.

2. NVAO uitgangspunten voor omgang met persoonsgegevens

In hoofdstuk 2 staan de uitgangspunten voor onze omgang met persoonsgegevens en wordt vervolgens toegelicht wat dat betekent voor een medewerker en welke documenten of websites beschikbaar zijn om die uitgangspunten in het dagelijks werk toe te passen. Ieder instrument (document of site) dat onderstreept is, is te vinden in bijlage 2 op alfabetische volgorde.

Er zijn een achttal uitgangspunten opgesteld, waar medewerkers van de NVAO te allen tijde aan dienen te voldoen. Deze uitgangspunten reflecteren de visie van de NVAO ten opzichte van de verwerking van persoonsgegevens.⁵ De uitgangspunten voor gegevensbescherming zijn van toepassing op *alle* verwerkingsactiviteiten met betrekking tot persoonsgegevens binnen de NVAO.

Dit betekent dat alle verwerkingen van persoonsgegevens moeten voldoen aan de volgende acht eisen:

- De NVAO verwerkt alleen persoonsgegevens als voor de verwerking een rechtmatige grondslag aanwezig is en een duidelijk omschreven en gerechtvaardigd doel.
- De NVAO beperkt de verwerking tot die categorieën persoonsgegevens die nodig zijn voor het beschreven doel.
- De NVAO verwerkt persoonsgegevens die accuraat en actueel zijn.
- De NVAO bewaart gegevens niet langer dan noodzakelijk voor het beschreven doel.
- De NVAO is, als dat mogelijk is, open en transparant over de verwerking van persoonsgegevens aan de betrokkene, de samenleving en ketenpartners.
- De NVAO zorgt dat persoonsgegevens die aan ons zijn toevertrouwd, veilig en vertrouwelijk worden verwerkt.
- De NVAO legt verantwoording af over de zorgvuldige verwerking van persoonsgegevens.
- De NVAO respecteert de rechten van de betrokkenen.

⁵ Het OECD is de organisatie voor economische samenwerking en ontwikkeling. De OECD heeft in 1980 principes opgesteld en in 2013 zijn deze voor het laatst herzien.

Hieronder volgt een nadere instructie per uitgangspunt.

2.1 Grondslag en doel

De NVAO verwerkt alleen persoonsgegevens als voor de verwerking een rechtmatige grondslag aanwezig is en een duidelijk omschreven en gerechtvaardigd doel.

Instructies:

- ⇒ Persoonsgegevens mogen alleen verwerkt worden als een van de rechtmatige grondslagen uit artikel 6 van de AVG aanwezig is. Te denken valt bijvoorbeeld aan: verwerking van persoonsgegevens ter uitvoering van een overeenkomst.
- ⇒ Persoonsgegevens mogen eveneens alleen verwerkt worden indien de NVAO in het kader van zijn taken verwerkingen verricht, die "noodzakelijk voor de uitvoering van een wettelijke plicht" zijn en "noodzakelijk voor het uitoefenen van een publiekrechtelijke taak of uitoefenen van openbaar gezag". De rechtsgrondslag van een dergelijke taak moet in de WHW of in de Codex Hoger Onderwijs zijn verankerd.
- ⇒ De grondslag "noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerker of van de verwerkingsverantwoordelijke of van een derde" kan niet worden gebruikt als er sprake is van verwerkingen door overheidsinstanties in het kader van de uitoefening van hun taken. Dit kan wel in beeld komen bij een verwerking in het kader van de bedrijfsvoering (denk bijvoorbeeld aan cameratoezicht rond het gebouw).
- ⇒ De ongelijke machtsverhouding tussen betrokkene en de overheid staat over het algemeen in de weg aan de eis dat betrokkene de toestemming vrijelijk moet verlenen.
- ⇒ Een (aanpassing van) verwerking moet steeds worden opgenomen in het Register van verwerkingen. Dit register geeft een beschrijving van verwerkingsactiviteiten. De verantwoordelijke (de NVAO) moet dit op verzoek aan de AP kunnen laten zien. Neem bij een dergelijk verzoek van de AP contact op met de privacy officer die dit in afstemming met de bestuurder verzorgt. Het Register van verwerkingen bevat zelf geen persoonsgegevens.
- ⇒ Het doel van elke verwerking is concreet en vastgelegd in het Register van verwerkingen. Als een bestand voor meer doelen wordt gebruikt dan wordt dat vermeld in de doelomschrijving. Doelen die duidelijk zijn omschreven maken het voor betrokkene inzichtelijk wat met de gegevens wordt gedaan. Bij verdere verwerking van persoonsgegevens voor een ander doel dan waarvoor de gegevens oorspronkelijk zijn verzameld, wordt altijd beoordeeld of dit nieuwe doel verenigbaar is met het oorspronkelijke doel.
- ⇒ De NVAO is verplicht een Data Protection Impact Assessment, DPIA (ook wel genoemd Gegevensbeschermingseffect-beoordeling, GEB), uit te voeren bij de ontwikkeling van beleid en regelgeving waaruit verwerkingen van persoonsgegevens voortvloeien. De AP heeft een lijst van verwerkingen opgesteld waarvoor de DPIA verplicht is.⁶ De DPIA is bedoeld om de effecten van de beoogde gegevensverwerking(en) voor betrokkenen te inventariseren en te beoordelen. Op basis van de DPIA kunnen maatregelen worden genomen om de risico's aan te pakken. Gebruik hiervoor het

⁶ <https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667>

Rijksmodel GEB (PIA) of het model dat in Privacy Nexus is opgenomen. In Privacy Nexus wordt ook het DPIA-register (bij)gehouden.

- ⇒ Vragen over het proces, de opzet en uitvoering van de DPIA kun je stellen aan de privacy officer en de Functionaris Gegevensbescherming. Raadpleeg eventueel het document DPIA Proces NVAO of de Memo Quick Scan DPIA om te beoordelen of een DPIA nodig is.

2.2 Doelbinding

De NVAO beperkt de verwerking tot die categorieën persoonsgegevens die nodig zijn voor het beschreven doel.

Instructies:

- ⇒ Alleen de voor het vooraf en precies omschreven doel noodzakelijke gegevens mogen worden verzameld. Gegevens mogen vervolgens niet verder worden verwerkt als dit onverenigbaar is met dat doel. Persoonsgegevens die niet meer nodig zijn (moeten) worden verwijderd of waar mogelijk geanonimiseerd.⁷ Bij de ontwikkeling van nieuwe (of wijziging van bestaande) producten en diensten wordt met gegevensbescherming rekening gehouden.
- ⇒ Verwerk niet meer gegevens dan die aantoonbaar noodzakelijk zijn voor het doel van de verwerking (*dataminimalisatie*). Bedenk waarom je gegevens voor die specifieke verwerking nodig hebt en of je daadwerkelijk alle gegevens nodig hebt.
- ⇒ Nieuwe systemen worden geconfigureerd op een zodanige wijze dat alleen de voor het specifieke verwerkingsdoel noodzakelijke gegevens worden verwerkt. Privacy moet dus bij het ontwerp van een (nieuw) automatiseringssysteem als uitgangspunt worden genomen. (*privacy by design*).
- ⇒ Ga bij het ontwikkelen van beleid, processen (en systemen) altijd uit van de meest privacybeschermende instellingen (*privacy by default*).
- ⇒ Raadpleeg bij het ontwikkelen en uitwerken van beleid, processen en systemen de Handleiding Privacy by Design & by Default om meer zicht te krijgen op privacyvriendelijk ontwerp waarin de bescherming van persoonsgegevens is ingebouwd.⁸

2.3 Accuraat en actueel

De NVAO verwerkt persoonsgegevens die accuraat en actueel zijn. Dit betekent onder meer dat er sprake is van zorgvuldig beheer van gegevens (*betrouwbaarheid en integriteit*) en dat het voor betrokkenen mogelijk is om verzoeken met betrekking tot rectificatie van onjuiste persoonsgegevens in te dienen (*rechten van betrokkenen*).

⁷ De AVG is niet van toepassing op anonieme gegevens omdat deze gegevens niet terug te voeren zijn op een geïdentificeerde of identificeerbare natuurlijke persoon. Anonimisering is versleuteling die onomkeerbaar is, het niet meer mogelijk om deze later weer met personen in verband te brengen. Bij pseudonisering kunnen anonieme gegevens met de juiste sleutel inzichtelijk gemaakt worden, waardoor herleiding naar natuurlijke personen weer mogelijk is. De AVG is wel van toepassing op gepseudonimiseerde gegevens.

⁸ https://www.cip-overheid.nl/media/1136/20170507-handleiding-privacy-by-design-v3_0.pdf

Instructies:

- ⇒ Zorg dat de juistheid en actualiteit van de persoonsgegevens zoveel mogelijk gewaarborgd is door periodieke controles en/of controle op bestaande gegevens of input, bijvoorbeeld wanneer panelleden opnieuw zitting nemen in een panel.
- ⇒ Zorg dat het mogelijk is om gegevens aan te passen daar waar zij onjuist, onvolledig of verouderd zijn.
- ⇒ Raadpleeg desgewenst Protocol Rechten van Betrokkenen.

2.4 Bewaarbeperking

De NVAO bewaart gegevens niet langer dan noodzakelijk voor het beschreven doel of zolang als bepaald door een specifieke wet.

Instructies:

- ⇒ De NVAO heeft maximale bewaartermijnen bepaald en geïmplementeerd voor alle persoonsgegevens waarover de organisatie mag beschikken. Nadat een bewaartermijn is verstreken, moeten de persoonsgegevens verwijderd worden of geanonimiseerd⁹.
- ⇒ Persoonsgegevens kunnen meerdere doelen dienen. Houd hiermee rekening bij het opstellen van de bewaartermijnen.
- ⇒ Bewaar persoonsgegevens niet langer dan noodzakelijk voor de doelen van de verwerking.
- ⇒ Stel bewaartermijnen vast conform de Memo Bewaartermijn Persoonsgegevens in de AVG.
- ⇒ Wis gegevens wanneer deze niet langer noodzakelijk zijn voor het verwerkingsdoel.
- ⇒ Raadpleeg desgewenst de Handreiking Bewaren van e-mail Rijksoverheid en de Selectielijst van de NVAO.

2.5 Open en transparant

De NVAO is, als dat mogelijk is, open en transparant over de verwerking van persoonsgegevens aan de betrokkene, de samenleving en ketenpartners. Een betrokkene dient te weten wat er met zijn persoonsgegevens gebeurt. De informatie over de verwerking en de omgang met de gegevens en over de rechten van betrokkene dient eenvoudig toegankelijk en begrijpelijk te worden aangeboden. Dit gebeurt in een interne en een (of meerdere) externe privacyverklaring(en).

⁹ Zie voetnoot 7

Concept 04

Instructies:

- ⇒ De NVAO verstrekt de vereiste informatie over onze verwerkingsactiviteiten voor o.a. studenten en overige burgers via de externe privacyverklaring op www.nvao.net.
- ⇒ De NVAO verstrekt vereiste informatie voor bestuursleden en medewerkers via de interne privacyverklaring op intranet of Sharepoint.
- ⇒ Zowel de interne als de externe privacyverklaring NVAO worden periodiek door het privacy office op actualiteit gecontroleerd.
- ⇒ Raadpleeg ook desgewenst de Handreiking Veilige omgang met persoonsgegevens of de Personeelsregeling.

2.6 Veilig en vertrouwelijk

De NVAO zorgt dat persoonsgegevens die aan ons zijn toevertrouwd, veilig en vertrouwelijk worden verwerkt.

Instructies:

- ⇒ De NVAO is verplicht (op basis van wet- en regelgeving) om passende technische en organisatorische maatregelen te treffen om persoonsgegevens een passend beschermingsniveau te bieden tegen ongeautoriseerde verwerkingen. De NVAO heeft hiertoe een Handreiking Veilige omgang met Persoonsgegevens opgesteld.
- ⇒ De NVAO verstrekt alleen toegang tot persoonsgegevens aan die mensen die toegang tot de gegevens nodig hebben en die toestemming hebben om gegevens verder te verwerken.
- ⇒ Datalekken moeten zoveel mogelijk worden voorkomen. Een datalek is een inbreuk op de beveiliging van de persoonsgegevens die leidt tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking of toegang tot gegevens.
- ⇒ Een datalek dat een risico voor de rechten van betrokkene inhoudt moet binnen 72 uur aan de Autoriteit Persoonsgegevens (AP) worden gemeld en soms ook aan betrokkene. Hiervoor is het Protocol datalekken NVAO opgesteld. Raadpleeg bij een (vermeend) datalek de privacy officer.
- ⇒ Via de e-mail worden veel bestanden uitgewisseld en dus ook vaak persoonsgegevens. Het is belangrijk om een passend beschermingsniveau toe te passen bij het versturen van dergelijke gegevens. Bij het versturen van bestanden met persoonsgegevens is het passend om deze gegevens versleuteld te versturen naar de ontvanger. Op die manier wordt het risico verkleind dat er per ongeluk bestanden naar de verkeerde ontvanger worden gestuurd. Als het nodig is om gegevens versleuteld te versturen naar de ontvanger, verstuur deze bijvoorbeeld door middel van een versleutelde omgeving.
- ⇒ De NVAO en in het bijzonder het privacy office houdt een register bij van datalekken en beveiligingsincidenten.
- ⇒ Raadpleeg eventueel het Autorisatiebeleid en het Beveiligingsbeleid.

2.7 Verantwoordingsplicht

De NVAO legt verantwoording af over de zorgvuldige verwerking van persoonsgegevens.

Instructies:

- ⇒ De NVAO neemt passende maatregelen om de bescherming van persoonsgegevens te waarborgen. Aan de hand van documentatie kan de NVAO aantonen dat de privacyregels worden nageleefd. Evaluatie, monitoring en logging van de maatregelen maakt ook onderdeel uit van de verantwoording. Deze verantwoordingsplicht (*accountability*) staat centraal in het nieuwe wettelijk privacykader.
- ⇒ Het privacy office van de NVAO beheert een Register van verwerkingen. In dat register staat informatie over de gegevens die worden verwerkt. De persoonsgegevens zelf staan niet in het register, wel welke categorieën persoonsgegevens er worden verwerkt.
- ⇒ Wijzigingen in verwerkingen moeten door medewerkers en/of leden van het managementteam aan de privacy officer worden doorgegeven.
- ⇒ De managers van de afdelingen Nederland en Vlaanderen hebben een zelfstandige verantwoordelijkheid om bij nieuwe verwerkingen (activiteiten/andere ICT systemen) de privacy officer en de FG op de hoogte te stellen.
- ⇒ De NVAO vergewist zich ervan dat derde partijen behoorlijk en zorgvuldig met persoonsgegevens omgaan. Dit hoeft niet noodzakelijkerwijs te gaan over partijen waarmee een verwerkersovereenkomst mee afgesloten dient te worden. Denk hierbij aan de Arbodienst die een eigen verwerkingsverantwoordelijkheid heeft. Waar nodig wordt een verwerkingsovereenkomst gesloten; deze wordt opgenomen in het Register Verwerkingsovereenkomsten (in de tool Nexus).
- ⇒ Raadpleeg Juridische Zaken bij vragen. Een Format verwerkersovereenkomst en Checklist verwerkersovereenkomst zijn beschikbaar.

2.8. Respect

De NVAO respecteert de rechten van de betrokkenen.

Instructies:

- ⇒ De NVAO richt systemen, processen en de interne organisatie zodanig in dat op de juiste manier gehoor wordt gegeven aan verzoeken van betrokkenen omtrent persoonsgegevens.
- ⇒ De NVAO hanteert een Protocol Rechten Betrokkenen, waarin de (belangrijkste) rechten van betrokkenen zijn/worden geformuleerd, zoals inzage, rectificatie, wissen, overdracht en beperking van verwerking. Ook wordt in dit protocol vermeld hoe een bepaald verzoek wordt behandeld en waar een betrokkene rekening mee kan houden. Op www.nvao.net kan een betrokkene deze informatie in begrijpelijke taal vinden.

- ⇒ De NVAO kan gebruik maken van een model voor de beantwoording van inzageverzoeken of van andere modellen om aan verzoeken te voldoen.
- ⇒ In de interne en externe privacyverklaringen worden o.a. de rechten van betrokkenen ten aanzien van hun persoonsgegevens omschreven. In beide privacyverklaringen wordt omschreven voor wie de betreffende privacyverklaring geldt.
- ⇒ Alle betrokkenen (intern en extern) kunnen bij de Autoriteit Persoonsgegevens (AP) een klacht indienen over de manier waarop de NVAO met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.

3. Privacy governance

3.1 Inleiding

Doel van dit hoofdstuk over de privacy governance is inzicht te geven in de verantwoordelijkheden op het gebied van de privacybescherming binnen de NVAO. De governancestructuur helpt de NVAO om zorgvuldig met persoonsgegevens om te gaan en verantwoording af te kunnen leggen over genomen beslissingen. Een robuuste beheersorganisatie is van belang voor de implementatie en handhaving van de principes en doelstellingen uit het privacybeleid.

Omgevingsveld

De NVAO is een zelfstandig bestuursorgaan en valt onder de politieke verantwoordelijkheid van het *Comité van Ministers*. Hoewel de NVAO een zelfstandig bestuursorgaan is, blijft het Comité van Ministers politiek verantwoordelijk voor compliance met wet- en regelgeving en dus ook de AVG.

De *Autoriteit Persoonsgegevens* (AP) is de toezichhoudende autoriteit met betrekking tot het voldoen aan de vereisten van de AVG. Wanneer betrokkenen klachten hebben over hoe de NVAO omgaat met persoonsgegevens, kunnen zij terecht bij de AP.

De *Nationale Ombudsman* kan eventueel ook nog een bemiddelende rol spelen tussen de NVAO en personen waarvan de NVAO gegevens verwerkt.

3.2 Privacy verantwoordelijkheden rollen en taken

Privacy gaat de gehele NVAO aan en ziet ook op de gehele organisatie. Met elkaar werken we aan de naleving van het privacybeleid en draagt de NVAO als bestuursorgaan hiervoor verantwoordelijkheid.

Welke organen en personen dragen bij aan het privacybeleid of spelen een rol?

- | | |
|---------|---------------------------------------|
| 1. AB | Algemeen Bestuur |
| 2. DB | Dagelijks Bestuur |
| 3. DN | Directeur Nederland |
| 4. DV | Directeur Vlaanderen |
| 5. FG | Functionaris voor gegevensbescherming |
| 6. PO | Privacy office |
| 7. IM | Informatiemanager |
| 8. AHN | Afdelingshoofd Nederland |
| 9. HR | Hoofd HR |
| 10. HF | Hoofd Financiën |
| 11. RB | Relatiebeheer |
| 12. Com | Communicatie |
| 13. OR | Ondernemingsraad |
| 14. Mw | medewerker |

N.B. 3, 4, 8 en 10 vormen samen het Management Team, ofwel MT

Concept 04

In het RASCI model (zie Bijlage 3) is uitgewerkt wie verantwoordelijk is voor welk onderdeel van de AVG. Meer in het algemeen staat hieronder beschreven bij wie, welke rollen en taken binnen de NVAO bij de uitvoering van de AVG zijn belegd.

De lijn: AB, DB, MT

Overeenkomstig de mandaatstructuur binnen de NVAO zijn het bestuur, de directeuren, het afdelingshoofd NL, en de hoofden HR en Financiën verder verantwoordelijk voor de strategische visie, de risicobeheersing en voor het borgen van de aantoonbare naleving van de wet- en regelgeving op het terrein van privacybescherming. Het MT is een overlegorgaan van de Directeur Nederland, Directeur Vlaanderen, Afdelingshoofd Nederland en Hoofd Financiën, waarbij ook het Hoofd HR aansluit. Beslissingen over de dagelijkse gang van zaken binnen de NVAO worden in het MT besproken. Vaak volgt hieruit een formele beslissing. Deze beslissing is dan (mandaattechnisch) toe te rekenen aan de Directeur Nederland.

De (niet met toezicht belaste) specialisten: PO, Informatiemanager en HR

Naast een privacy officer 1 heeft de NVAO een Informatiemanager. De privacy officer en de Informatiemanager adviseren, ondersteunen en controleren de directie, het bestuur en de medewerkers bij privacy aspecten. Ook bepaalde beleidstaken en het organiseren van interne risicoanalyses behoren tot hun takenpakket. Primair is de privacy officer het aanspreekpunt voor de uitleg van de AVG binnen de NVAO en bij de implementatie en uitvoering van de AVG.

1 Axel Aerden

De functie is niet NVAO-breed, is deze invulling dat dan wel?

Daarnaast heeft HR een rol als het gaat om de zorgvuldige omgang met persoonsgegevens. HR is het eerste aanspreekpunt bij personeelsgerelateerde vragen van medewerkers over de AVG.

Taakomschrijvingen meer specifiek van de FG, het PO en de IM:

Functionaris Gegevensbescherming (FG)¹⁰

De NVAO heeft een interne FG aangesteld overeenkomstig artikel 37 e.v. van de AVG. De FG rapporteert aan de voorzitter van het bestuur. In de AVG is de rol van de FG als volgt beschreven:

- informeren en adviseren van het lijnmanagement over hun verplichtingen uit hoofde wet- en regelgeving in het kader van privacy;
- toezien op de naleving van de relevante wetgeving, het privacybeleid en de inrichting van de interne privacy organisatie;
- advies leveren bij een DPIA, zowel de inhoudelijke beoordeling als de naleving van de voorgenomen beheermaatregelen;
- samenwerken met de AP, de centrale toezichthouder, in het geval van onderzoek;
- aanspreekpunt voor betrokkenen (burgers en medewerkers) voor alle aangelegenheden bij de verwerking van hun persoonsgegevens.

Jaarlijks kan de FG een werkplan privacy office opstellen in het kader van zijn toezichthoudende werkzaamheden.

Privacy office (PO)

De NVAO heeft een privacy officer die de volgende taken verricht:

- beheert het privacybeleid en kan op verzoek van de directie, het bestuur of uit eigen beweging een voorstel tot aanpassing van het beleid doen;

¹⁰ <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/functionaris-gegevensbescherming-fg>

Concept 04

- zorgt voor de dagelijkse afhandeling van privacy aangelegenheden voor de NVAO;
- beheert het register van verwerkingsactiviteiten;
- stelt de jaarplanning op;
- fungeert als vraagbaak voor het management ten aanzien van het verzamelen, registreren en leveren van persoonsgegevens. Hij raadpleegt indien nodig de Functionaris Gegevensbescherming of externe adviseurs over complexere verwerkingen en relaties met verwerkers.
- adviseert het management bij de analyse van mogelijke risico's die samenhangen met de verwerking van persoonsgegevens.

De NVAO heeft een privacy office¹¹ dat de volgende taken verricht: ondersteunt de NVAO in het naleven van de eisen uit dit privacybeleid en de privacywetgeving. leid en

Informatiemanager (IM)

Het onderwerp privacy en gegevensbescherming heeft een multidisciplinair karakter. Het vraagt om een zorgvuldige afstemming met de experts van juridische zaken, ICT, beveiliging, communicatie, de privacy en de FG.

De informatiemanager heeft onder meer als taak:

- Opstellen informatievoorziening strategie en beleid en vertalen naar de techniek;
- Opstellen en actualiseren informatiebeveiligingsbeleid en de daaruit voortvloeiende plannen;
- Inrichten van de informatiebeveiligingsorganisatie en het coördineren en afhandelen van beveiligingsincidenten;
- Ophalen en vertalen van externe ontwikkelingen (wetgeving, technologie, bedrijfsvoering) naar consequenties en aanpassingen voor de informatievoorziening;
- Monitoren van relevante risico's voor de organisatie;
- Monitoren en borgen van de eisen en architectuur voor informatiebeveiliging en het consequent toepassen van Security-by-Design en Privacy-by-Design.

De IM ondersteunt de afdelingen Nederland en Ondersteuning en is in eerste instantie verantwoordelijk voor de informationele privacy. De IM ondersteunt en adviseert de NVAO bij privacyvraagstukken. De IM helpt onder meer door het geven van (zo mogelijk) advies op maat, het opbouwen van de noodzakelijke kennis over privacy wet- en regelgeving, het toepassen hiervan en het (mede-)ontwikkelen van producten zoals informatiebeleid en privacy convenanten.

Wat is de rol van de OR¹² bij privacyvraagstukken?

De ondernemingsraad vertegenwoordigt het personeel van de NVAO en beschermt hun belangen. De ondernemingsraad heeft daarvoor verschillende rechten en bevoegdheden, zoals het recht op informatie, het adviesrecht, het instemmingsrecht en het initiatiefrecht. Met name het adviesrecht, instemmingsrecht en het initiatiefrecht spelen een rol bij de uitvoering van de AVG. Artikel 27 WOR

Het kan zijn dat er nieuwe technische maatregelen worden getroffen om te voldoen aan de AVG. Denk bijvoorbeeld aan technische maatregelen om persoonsgegevens te beveiligen of om ervoor te zorgen dat alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor het verwerkingsdoel.

Op grond van de Wet op de Ondernemingsraden (WOR) dient een besluit tot het invoeren of wijzigen van een technologische voorziening ter advies aan de ondernemingsraad te worden voorgelegd. Dus als de NVAO wil overgaan tot de aanschaf van nieuwe ICT ter beveiliging van de persoonsgegevens, dan heeft de OR adviesrecht.

¹¹ Juridische Zaken fungeert als Privacy Office op het moment van inwerkingtreding van dit beleid; eventuele wijziging wordt gecommuniceerd.

¹² <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-uitkering/ondernemingsraad>

Een besluit tot vaststelling, wijziging of intrekking van een regeling over het verwerken van, alsmede de bescherming van de bij de NVAO werkzame personen is instemmingsplichtig. Het moet dus gaan om een regeling die tot doel heeft persoonsgegevens te verzamelen, bewaren, gebruiken, verstrekken of beveiligen. Dit geldt onder meer voor de vaststelling van dit privacybeleid en voor het melden van een datalek waar bij persoonsgegevens zijn betrokken.

De ondernemingsraad kan tenslotte gebruikmaken van haar initiatiefrecht om voorstellen te doen voor een (een aanpassing van) het privacybeleid.

3.3 Privacy overlegstructuren

Privacy moet als vast onderdeel opgenomen zijn op de agenda's van de reguliere overleggen tussen JZ/Directie alsook tussen JZ/Directie en HRM, Directie/Financiën, Dir/com, Dir/ICT en Dir/ICT-stuurgroep. Er is tenslotte ook nog een vast maandelijks overleg tussen het privacy office en de Functionaris Gegevensbescherming.

De NVAO doet daarnaast mee aan overleggen van KleinLef organisaties op het gebied van privacy om de kennis omtrent privacy te delen en elkaar te helpen om beleid omtrent privacy te ontwikkelen.

3.4 Sturing, regie en toezicht

Periodiek voert de NVAO met behulp van de tool in Privacy-Nexus self-assessments uit, waaruit blijkt wat de stand van zaken is met betrekking tot privacy.

De FG ziet toe op de naleving van de relevante wetgeving, het privacybeleid en de inrichting van de interne privacy organisatie.

Interne toezichtsorganen: FG en OR

Tenslotte kent de NVAO een Functionaris Gegevensbescherming (FG) en de Ondernemingsraad (OR). Zij zijn vanwege hun specifieke rollen en wettelijke taken bij aspecten van de privacy van de NVAO betrokken.

Externe toezichthouders, zoals de Autoriteit Persoonsgegevens (AP) en al dan niet ingehuurd auditors kunnen de inregeling en uitvoering van de AVG controleren. Het is de eigen verantwoordelijkheid van de NVAO om intern toezicht te houden op de waarborging van privacybescherming, los van eventuele externe audits en evaluaties.

3.5 Privacy trainingen en bewustwording

Alle medewerkers krijgen bij hun aanstelling een korte introductie AVG van de PO/FG. De tekst van de eed/belofte is in de Personeelsregeling opgenomen; hierin ligt de geheimhouding t.a.v. AVG besloten.

Daarnaast vinden reguliere bewustwordingsacties plaats, door minimaal één keer per jaar aandacht voor een privacy onderwerp vanuit het privacy office en minimaal één bureaubijeenkomst per jaar over een AVG onderwerp. Daarnaast worden medewerkers ook geïnformeerd over de AVG en privacy, doordat dit onderwerp een integraal onderdeel uitmaakt van de besprekingen van het Dagelijks Bestuur. De verslagen hiervan zijn voor medewerkers te raadplegen.

4. Slot

Met dit privacybeleid brengt de NVAO in kaart welke maatregelen er zijn genomen om de persoonsgegevens van medewerkers en externen, waaronder o.a. panelleden, secretarissen en studenten, te beschermen. Daarnaast geeft het beleid inzicht in de wijze waarop de verantwoordelijkheden op grond van de AVG zijn belegd bij de NVAO. Ook is per uitgangspunt vastgelegd welke instructies er zijn en welke documenten geraadpleegd kunnen worden. Hiermee wordt voldaan aan belangrijke verplichtingen op grond van de AVG, zoals het inrichten en bijhouden van een Register van verwerkingen, de wijze waarop omgegaan wordt met datalekken, het houden van een DPIA, het opstellen van een interne en externe privacyverklaring en de wijze waarop rechten van betrokkenen zijn georganiseerd.

4.1 Beheer

Het privacy office van de NVAO is verantwoordelijk voor het beheer van dit privacy beleidskader. De instrumenten en dit beleidskader zijn levende documenten die periodiek (moeten) worden geactualiseerd. Algemene vragen over dit beleid of suggesties tot wijziging of toevoeging aan het beleid, kunnen worden gericht aan het privacy office van de NVAO (privacy@nvao.net).

4.2 Vaststelling

Dit privacybeleid is voor het eerst vastgesteld op door het Algemeen Bestuur van de NVAO.

4.3 Wijzigingen en evaluatie

Privacybeleid is dynamisch beleid. Nieuwe ontwikkelingen volgen elkaar op en ook de organisatie zelf zal steeds in ontwikkeling zijn. Dit betekent dat het privacybeleid ook met regelmaat bijgesteld zal moeten worden. Dit beleid wordt periodiek herzien en bijgewerkt. De volgende tabel toont de (concept)versie geschiedenis van dit privacy beleid. Evaluatie vindt in beginsel ieder jaar plaats, tenzij anders bepaald.

Datum	Opmerkingen	Versie
16-10-2019	1 ^{ste} concept beleidsdocument	0.1
27-07-2020	Concept tbv FG	0.2
2-11-2020	Concept tbv Luut	0.3
28-1-2021	Concept tbv DB	0.4

BIJLAGE 1: BEGRIPPEN

Wat zijn persoonsgegevens?

Niet alle data of gegevens zijn per definitie persoonsgegevens. Persoonsgegevens betreft alle informatie met betrekking tot een geïdentificeerde of identificeerbare natuurlijke persoon (de "betrokkene").

De betrokkene hoeft geen direct geïdentificeerd individu te zijn, maar zodra een individu uit een groep kan worden onderscheiden, zijn de gegevens persoonsgegevens. Het is dus niet altijd nodig om de naam te weten van de persoon in kwestie om te spreken van persoonsgegevens.

Alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare persoon moeten als persoonsgegevens worden beschouwd. Enkel transactiegegevens zijn bijvoorbeeld op zichzelf geen direct identificeerbare gegevens, maar worden persoonsgegevens wanneer deze verband houden met een geïdentificeerde of identificeerbare persoon, bijvoorbeeld omdat deze is gekoppeld aan een naam, een e-mailadres of een telefoonnummer.

De AVG heeft een speciaal regime voor bijzondere categorieën persoonsgegevens. Dit betreffen persoonsgegevens waaruit de raciale of etnische afkomst, politieke opvattingen, religieuze of filosofische overtuigingen blijken, lidmaatschap van een vakvereniging, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie, gezondheids- of medische gegevens, gegevens over iemands seksleven of seksuele geaardheid.

Strafrechtelijke persoonsgegevens zijn persoonsgegevens die te maken hebben met strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen. Hieronder vallen zowel veroordelingen als mogelijk gegronde verdenkingen. Dit wil zeggen dat er concrete aanwijzingen zijn dat iemand een strafbaar feit heeft gepleegd. Een voorbeeld hiervan is een opgestelde zwarte lijst van frauderende klanten bij een financiële instelling. Onder de AVG gelden speciale regels voor het verwerken van strafrechtelijke gegevens.

De verwerking, het verzamelen of gebruiken, van gevoelige persoonsgegevens, is verboden, tenzij een uitzondering op het algemene verbod van toepassing is. Het verzamelen en gebruiken van dergelijke gegevens zal daarom zoveel mogelijk worden vermeden. Vermijd ook het verzamelen en gebruik van gegevens van gevoelige groepen, zoals kinderen / minderjarigen, gehandicapten en ouderen, tenzij hiervoor duidelijk toestemming is gegeven door de bevoegde persoon.

Hieronder volgen voorbeelden van gegevens die over het algemeen als persoonsgegevens worden beschouwd:

Voornaam en / of initialen en achternaam	Financiële gegevens
E-mailadres	Betaling of transactiegegevens
Telefoonnummer	Rijbewijs
Foto	Strafrecht ketennummer
Geboortedatum / geboorteplaats	Identificatienummer werknemer
IP-adres	Werknemers informatie
Uitkomsten functioneringsgesprekken	Medische informatie

Concept 04

Burgerservicenummer	Biometrische gegevens
Unique Device Identifiers	MAC-adressen

Wat is een betrokkene?

De betrokkene is de persoon van wie persoonsgegevens worden verwerkt.

Wat is een verwerking?

Het 'verwerken van persoonsgegevens' of een 'verwerking van persoonsgegevens' betreft alle handelingen die men met persoonsgegevens kan verrichten. Denk hierbij aan het verzamelen, vastleggen, raadplegen, opvragen, ordenen, structureren, opslaan, bewerken of wijzigen, verstrekken en combineren. Ook het wissen of vernietigen van gegevens is een verwerking van persoonsgegevens.

Wat is een verwerkingsverantwoordelijke?

De verwerkingsverantwoordelijke is de natuurlijke persoon of rechtspersoon die (alleen of tezamen met anderen) bepaalt welke persoonsgegevens worden verzameld, waarom persoonsgegevens worden verwerkt (doel) en hoe persoonsgegevens worden verwerkt (middelen). Wanneer partijen gezamenlijk het doel en de middelen vaststellen voor de verwerking van persoonsgegevens dan spreken we van een gezamenlijke verantwoordelijkheid.

Wat is een verwerker?

Een verwerker is de natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Het gaat om derde partijen die voor de verwerkingsverantwoordelijke werken. Een verwerker handelt onder de verantwoordelijkheid van de verwerkingsverantwoordelijke en naar diens instructies, maar er is geen hiërarchische relatie (medewerkers zijn geen verwerkers). Daarnaast heeft de verwerker geen zeggenschap over de verwerkingen en mag de gegevens niet voor eigen doelen gebruiken.

BIJLAGE 2. INSTRUMENTEN

N.B. BIJLAGE 2 IS EEN LOS DOCUMENT, HET LOSSE DOCUMENT IS LEIDEND. BIJ VERSPREIDING VAN DIT PRIVACY BELEIDSKADER MOET DE MEEST RECENTE BIJLAGE 2 INSTRUMENTEN (ZONDER DE STATUS & PLANNING) WORDEN TOEGEVOEGD.

BIJLAGE 3: RASCI MODEL

N.B. BIJLAGE 3 IS EEN LOS DOCUMENT IN LIGGEND BEELD

BIJLAGE 3 van het Privacy Beleidskader

RASCI model

In dit model wordt tot uitdrukking gebracht welke entiteit (orgaan of afdeling) of welke functionaris in hoofdlijnen welke rol heeft aangaande AVG gerelateerde activiteiten. De rol (verantwoordelijkheden of taken) worden uitgedrukt in de letters R – A – S – C – I en hieronder toegelicht. De entiteiten en functionarissen die in de NVAO een rol spelen bij de AVG, zijn in dit model de volgende en afgekort als volgt:

• AB	Algemeen Bestuur
• DB	Dagelijks Bestuur
• DN	Directeur Nederland
• DV	Directeur Vlaanderen
• FG	Functionaris voor gegevensbescherming
• PO	Privacy office
• IM	Informatiemanager
• AHN	Afdelingshoofd Nederland
• HR	Hoofd HR
• HF	Hoofd Financiën
• RB	Relatiebeheer
• Com	Communicatie; diegenen wiens werkzaamheden hoofdzakelijk bestaan uit het beheren van content op internet, intranet, SharePoint
• OR	Ondernemingsraad
• Mw	medewerker, iedere persoon die voor de NVAO (mede inbegrepen CDHO en CMMBO) werkzaamheden verricht

R (Responsible):

De functionaris is verantwoordelijk voor de uitvoering van het proces/resultaat. De 'Responsible' is verantwoordelijk tegenover de eindverantwoordelijke(n).

A (Accountable):	Het orgaan dat toezicht houdt op het werk en het werk goedkeurt. Het orgaan dat de eindverantwoordelijkheid heeft. De 'Accountable' heeft het laatste woord.
S (Support):	De functionaris die de 'Responsible' en de 'Accountable' ondersteunt in de uitvoering van hun taken.
C (Consulted):	Beïnvloedt het werk. De functionaris die aanwijzingen geeft voor het beste resultaat. De persoon die vooraf geraadpleegd moet worden voordat er beslissingen worden genomen en overgegaan wordt tot actie.
I (Informed):	De functionaris die weet wat er gebeurt. De functionaris die geïnformeerd wordt over beslissingen, geboekte vooruitgang, resultaten et cetera. Need to know.

Algemene opmerkingen:

1. Het Algemeen Bestuur wordt jaarlijks geïnformeerd in een rapportage, heeft een toezichthoudende taak t.a.v. privacyzaken en heeft de eindverantwoordelijkheid. Het Algemeen Bestuur heeft als hoogste orgaan de meeste verantwoordelijkheid (A1).
2. Bij de NVAO is de dagelijkse leiding en verantwoordelijkheid t.a.v. privacy in de breedste zin, belegd bij het Dagelijks Bestuur, conform de mandaatregeling d.d. Het Dagelijks Bestuur heeft daarmee t.a.v. privacy een belangrijke verantwoordelijkheid (A2).
3. DN en DV hebben dezelfde rol ten aanzien van AVG gerelateerde zaken. DN voor Nederland. DV voor Vlaanderen. Het is hun verantwoordelijkheid om de supportrol (S) op te leggen indien hier onduidelijkheid over zou bestaan.
4. De R, S, C, I kunnen per activiteit aan meerdere functionarissen zijn toebedeeld. Dit model sluit niet uit dat wanneer een van deze rollen van toepassing is, een andere rol niet tegelijkertijd van toepassing kan zijn. Dit model geeft aan welke rol bij uitstek is toebedeeld. Anderen kunnen dus ook geconsulteerd worden als geen C vermeld staat.
5. FG, PO en IM krijgen afwisselend de R-, C- en I-rol. Support kan hierbij inbegrepen zijn. Wanneer S support van andere functionarissen nodig is, wordt dit met S aangeduid.
6. Medewerkers van Communicatie hebben dan een support-rol, wanneer Mw geïnformeerd moeten worden.
7. Evaluatie op termijn om de praktijk af te stemmen op dit model is gewenst.

Rubricering en nummering:

• Gebruik van persoonsgegevens & AVG-naleving	1-2
• Privacy en gegevensbescherming strategie en beleid	3-7
• Privacy maatregelen (privacy risicoclassificatie, DPIA, privacy by design etc.)	8-14
• Vastleggen en documenteren	15-23
• Verzoeken en incidenten (melding van datalek aan de toezichhoudende autoriteit, de betrokkene etc.)	24-31
• Training en bewustwording (het stimuleren van een privacy cultuur, training en workshops en bewustwording)	32-33
• Monitoring en handhaving	34-38

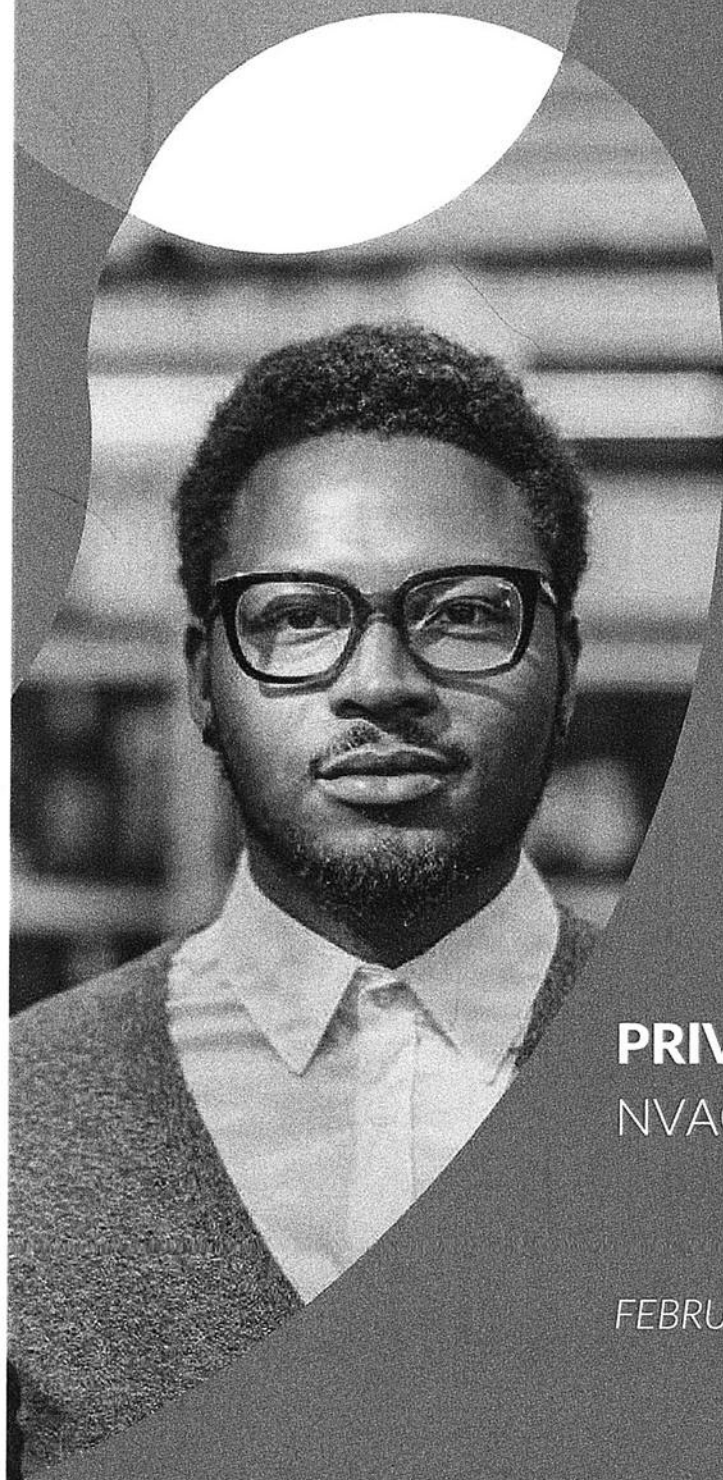
	Taken	AB	DB	DN	DV	FG	PO	IM	AHN	HR	HF	RB	Com	OR	MW
Gebruik van persoonsgegevens & AVG-naleving	1. Het beslissen over het gebruik van persoonsgegevens voor zakelijke doeleinden ("doel en middelen")	A1	A2	R	R	C	C	C	I	I	I	I	I	I	I
	2. Het uitvoeren van technische en organisatorische maatregelen om ervoor te zorgen dat de AVG wordt nageleefd	A1	A2	R	R	C	C	R	R	I	I	I	S	I	I
Privacy en gegevens- bescherming strategie en beleid															
	3. Het bepalen van de privacy ambitie en strategie	A1	A2	R	R	C	C/S	C/S	I	I	I	I	I	I	I
	4. Het vaststellen van het privacy en gegevensbeschermingsbeleid	A1	A2	R	R	C	C/S	C/S	C	C	C	I	I	C	I
	5. Het vaststellen en implementeren van de privacy governance-structuur	A1	A2	R	R	I	C	C	C	C	C	I	I	I	I
	6. Het aanwijzen van hulpbronnen (budget) voor het uitvoeren van privacy werkzaamheden	A1	A2	R	R	C	C	C	I	nvt	C	nvt	nvt	I	nvt
	7. Het opstellen en borging van het autorisatiebeleid (incl. matrix)	A1	A2	R	R	C	C	S	C	C	I	nvt	I	nvt	I

	Taken	AB	DB	DN	DV	FG	PO	IM	AHN	HR	HF	RB	Com	OR	MW
Privacy maatregelen (privacy risicoclassificatie, DPIA, privacy by design etc.)	8. Het verstrekken van advies op het gebied van privacy en gegevensbescherming	A1	A2	C	C	R	R	R	I	I	I	I	I	I	I
	9. Het implementeren en borgen van privacy by design and default	A1	A2	R	R	C	C/S	C/S	I	I	I	I	I	nvt	I
	10. Het opstellen van DPIA's	A1	A2	R	R	C	C	C	R	S	S	S	S	nvt	S
	11. Het vaststellen van DPIA (ondermandaat?/risicoacceptatie)	A1	A2	R	R	C	I	C	R	I	I	I	I	nvt	C
	12. Het ondersteunen en/of opstellen van leveranciers-beoordelingen (verwerkersovereenkomsten)	A1	A2	R	R	C	C	C	I	I	I	I	I	nvt	I
Vastleggen en documenteren	13. Het ondersteunen en/of opstellen van afspraken m.b.t. het delen van gegevens	A1	A2	R	R	C	C	C	R	S	S	S	S	I	I
	14. Adviseren over technologie en beveiliging omtrent gegevensverwerking	A1	A2	C	C	C	C	R	S	S	S	S	S	nvt	S
	15. Het maken en onderhouden van een verwerkings-register	A1	A2	C	C	C	R	C	S	S	S	S	S	nvt	S
	16. Het documenteren van DPIA's	A1	A2	I	I	I	R	I	I	I	I	I	I	nvt	I
	17. Het documenteren van verwerkings-overeenkomsten (DPA's)	A1	A2	I	I	I	R	I	I	I	I	I	I	nvt	I

	Taken	AB	DB	DN	DV	FG	PO	IM	AHN	HR	HF	RB	Com	OR	MW
Vastleggen en documenteren	18. Het documenteren van datalekken	A1	A2	C	C	I	R	I	I	I	I	I	I	nvt	I
	19. Het vastleggen van toestemmings-verklaringen vanuit HR perspectief	A1	A2	R	R	I	C	I	R	R	I	R	I	nvt	I
	20. Het vastleggen van toestemmingsverklaringen vanuit primair proces	A1	A2	I	I	I	C	I	I	I	I	R	I	nvt	R?/S?
	21. Het documenteren van vragen in het kader van rechten van betrokkenen	A1	A2	I	I	I	R	I	I	I	I	I	I	nvt	I
	22. Het opstellen en onderhouden van privacyverklaring (intern/extern)	A1	A2	C	C	C	R	C	I	I	I	I	S	nvt	I
	23. Vastleggen en onderhouden van processen en werkinstructies van privacy instrumenten	A1	A2	C	C	C	R	C	C	I	I	I	S	nvt	I
Verzoeken en incidenten	24. Het afhandelen van vragen en klachten gerelateerd aan (persoons) gegevensbescherming	A1	A2	C	C	C	R	C	C	I	I	I	S	nvt	I
	25. Het afhandelen van vragen over rechten van betrokkenen	A1	A2	C	C	C	R	C	C	I	I	I	S	nvt	I

	Taken	AB	DB	DN	DV	FG	PO	IM	AHN	HR	HF	RB	Com	OR	MW
Verzoeken en incidenten (melding van datalek aan de toezichhoudende autoriteit en de betrokkene etc.)	26. Het behandelen van een incident*	A1	A2	C	C	C	R	R	C	I	I	I	I	nvt	I
	27. Het melden van een datalek aan de toezichhoudende autoriteit	A1	A2	C	C	R	R	R	C	I	I	I	I	nvt	I
	28. Het communiceren van een datalek naar de betrokkene	A1	A2	R	R	C	C	C	I	I	I	I	I	nvt	I
	29. Het bijhouden van het incidentenregister*	A1	A2	C	C	C	R	R	C	I	I	I	I	nvt	I
	30. Het implementeren van mitigerende maatregelen na een incident*	A1	A2	R	R	C	C	C	R	I	I	I	I	nvt	I
Training en bewustwording (het stimuleren van een privacy cultuur, training en workshops)	31. Het communiceren met de toezichhoudende autoriteit	A1	A2	C	C	R	R	R	I	I	I	I	I	nvt	I
	32. Het uitvoeren en communiceren van bewustwordings-programma's m.b.t. privacy en gegevensbescherming	A1	A2	C	C	C	R	R	C	R/S	I	I	S	nvt	I
	33. Het trainen van medewerkers betrokken bij de verwerking van persoonsgegevens	A1	A2	R	R	C	C	C	R	R	I	I	I	nvt	I
Monitoring en handhaving	34. Privacy-planning en control vastleggen (DPIA, DPA)	A1	A2	R	R	C	C	C	C	I	I	I	I	nvt	I

Monitoring en handhaving	Taken	AB	DB	DN	DV	FG	PO	IM	AHN	HR	HF	RB	Com	OR	MW
	35. Het periodiek rapporteren over privacy en gegevensbescherming aan management	A1	A2	R	R	A3	C	C	I	I	I	I	I	nvt	I
	36. Het monitoren van AVG-naleving, incl (tijds) vernietiging van gegevens	A1	A2	R	R	A3	C	C	R	R	S	S	S	nvt	S
	37. Het handhaven van het privacybeleid	A1	A2	R	R	C	C	C	R	R	S	S	S	I	S
	38. Het nabespreken van een incident	A1	A2	R	R	C	C	C	R	R	S	I	I	I	S



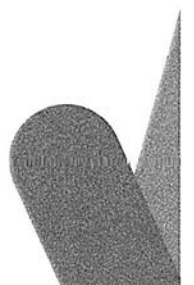
PRIVACY BELEIDSKADER

NVAO Nederland

FEBRUARI 2025

PRIVACY BELEIDSKADER
NVAO NEDERLAND

FEBRUARI 2025



Inleiding

De Nederlands-Vlaamse Accreditatieorganisatie (NVAO) is een kwaliteitszorgorganisatie die op deskundige en onafhankelijke wijze de kwaliteit van het hoger onderwijs in Nederland en Vlaanderen borgt en die de kwaliteitscultuur binnen de instellingen voor hoger onderwijs in Nederland en Vlaanderen bevordert. Zij accrediteert bestaande en nieuwe opleidingen en beoordeelt de kwaliteitszorg van instellingen in het hoger onderwijs. Daarmee is de NVAO bewaker van de kwaliteit van het hoger onderwijs. De besluiten van de NVAO leiden tot erkenning van diploma's en titels en waar van toepassing tot bekostiging van opleidingen. De NVAO baseert haar beoordeling op advies van erkende deskundigen.

De NVAO werd in 2003 opgericht bij Verdrag tussen Nederland en Vlaanderen. De NVAO is een zelfstandig bestuursorgaan en opgericht naar Nederlands publiekrecht met de zetel in Den Haag. De NVAO valt onder verantwoordelijkheid van het Comité van Ministers.

NVAO Nederland (NL) heeft een nauwe samenwerking met de Commissie Macrodoelmatigheid Hoger Onderwijs (CDHO) en de Commissie Macrodoelmatigheid mbo (CMMBO). De taken van de NVAO NL zijn in wetgeving vastgelegd. Binnen de opdracht die in het accreditatieverdrag tussen Nederland en Vlaanderen aan de NVAO is toegekend, wil zij de kwaliteit van het hoger onderwijs borgen, verbeteringen stimuleren en een kwaliteitscultuur bevorderen.

Om dit werk goed te kunnen doen is verwerking van persoonsgegevens van onder andere medewerkers, betrokkenen bij het accreditatieproces, contactpersonen van ketenpartners en burgers noodzakelijk. De privacy van deze mensen is erg belangrijk voor NVAO NL en we hechten dan ook veel belang aan een correcte verwerking en gebruik van persoonsgegevens. De bescherming van persoonsgegevens is immers een grondrecht. NVAO NL is verantwoordelijk voor de aantoonbare zorgvuldige omgang met persoonsgegevens.

Het privacy beleidskader van de NVAO (voor de verbijzondering) werd voor het eerst vastgesteld op 15 maart 2021 en herzien in november 2024 vanwege de verbijzondering van de NVAO.

De NVAO is juridisch gezien een ZBO naar Nederlands publiek recht, hetgeen betekent dat de organisatie, ongeacht of het de afdelingen betreft of het bestuur, gehouden is aan de Nederlandse regelgeving voor ZBO's. Feitelijk is er sinds de verbijzondering evenwel sprake van een totale splitsing in de bedrijfsvoering binnen de afdelingen (NL en VL) en hebben de afzonderlijke afdelingen eigen voorzieningen op het gebied van ICT, financiën en HR. Uitsluitend de bestuursondersteuning valt binnen het gemeenschappelijk deel van de NVAO en kent een eigen bedrijfsvoering. Voor het primaire proces, de belangrijkste taak van de NVAO, namelijk accrediteren van opleidingen en instellingen, is al op basis van het Verdrag bepaald dat de afzonderlijke afdelingen besluiten nemen op basis van de eigen regelgeving van Vlaanderen dan wel Nederland.

Dit privacy beleidskader richt zich daarmee tot iedereen die werkzaamheden verricht voor NVAO NL en medewerkers van het bureau van de CDHO en CMMBO. In dit privacy beleidskader wordt uitgelegd hoe de NVAO Afdeling Nederland aantoonbaar zorgvuldig omgaat met persoonsgegevens, wat daarbij de uitgangspunten zijn en wat de rol van de medewerker is bij de bescherming van persoonsgegevens¹.

¹ Voor een beknopte uitleg van begrippen (als persoonsgegevens en verwerking) zie bijlage 1.

Inhoud

1	Privacy Beleidskader.....	5
1.1	Doel.....	5
1.2	Doelgroep en Scope NVAO NL, CDHO en CMMBO.....	5
1.2.1	CMMBO en CDHO	5
1.3	Wet- en regelgeving verwerking van persoonsgegevens.....	5
1.3.1	Europese en Nederlandse wet- en regelgeving op het gebied van privacy.....	5
1.3.2	Context NVAO NL.....	6
2	NVAO uitgangspunten voor omgang met persoonsgegevens.....	7
2.1	Grondslag en doel.....	7
2.2	Doelbinding.....	8
2.3	Accuraat en actueel.....	9
2.4	Bewaarbeperking.....	10
2.5	Open en transparant	10
2.6	Veilig en vertrouwelijk	11
2.7	Verantwoordingsplicht.....	11
2.8	Respect.....	12
3	Privacy governance.....	13
3.1	Inleiding.....	13
3.2	Privacy verantwoordelijkheden, rollen en taken	13
3.3	Privacy overlegstructuren	16
3.4	Sturing, regie en toezicht.....	16
3.5	Privacy trainingen en bewustwording	16
4	Slot.....	17
4.1	Beheer	17
4.2	Vaststelling	17
4.3	Wijzigingen en evaluatie.....	17
5	Contactgegevens	19
	Bijlage 1: Begrippen	20
	Bijlage 2: Overzicht beleid en instrumenten	22
	Lijst van begrippen en afkortingen.....	23

1 Privacy Beleidskader

Het NVAO NL Privacy Beleidskader geeft aan waar de afdeling Nederland van de NVAO op het vlak van gegevensbescherming voor staat en wat de uitgangspunten voor de omgang met persoonsgegevens zijn. Met dit kader wil de afdeling Nederland van de NVAO ervoor zorgen dat de privacybescherming in lijn is met de wettelijke vereisten en dat deze aansluit bij of geïntegreerd wordt in de bestaande processen en systemen van NVAO NL.

Bij alle uitgangspunten wordt steeds verwezen naar praktische ondersteunende instrumenten (zoals checklists, stappenplannen en procedures) van NVAO NL, dan wel – voor zover niet aanwezig – van het Ministerie van Onderwijs, Cultuur en Wetenschap (OCW).

De uitleg van een aantal belangrijke begrippen uit de Algemene verordening gegevensbescherming (AVG) is opgenomen in Bijlage 1: Begrippen.

1.1 Doel

Het doel van dit Privacy Beleidskader is een omgeving te creëren waarin elke medewerker van NVAO NL:

- zijn of haar verantwoordelijkheid en rechten kent met betrekking tot privacy en de verwerking van persoonsgegevens,
- in staat is het juiste beleid en de juiste procedures te vinden en te volgen,
- contact kan opnemen met de juiste personen bij vragen.

1.2 Doelgroep en Scope NVAO NL, CDHO en CMMBO

Dit Privacy Beleidskader is van toepassing op iedereen die werkzaamheden verricht voor NVAO NL, evenals op medewerkers van het bureau van de CDHO en CMMBO. In dit kader wordt toegelicht hoe de afdeling Nederland van de NVAO aantoonbaar zorgvuldig omgaat met persoonsgegevens, welke uitgangspunten daarbij gelden en welke rol de medewerker speelt in de bescherming van persoonsgegevens.

1.2.1 CMMBO en CDHO

Deze organisaties hebben zelfstandige taken en verantwoordelijkheden. Er bestaat een nauwe samenwerkingsrelatie tussen NVAO NL en de CMMBO/CDHO, die is vastgelegd in een hostingovereenkomst. De organisaties bevinden zich niet alleen fysiek in het pand van de NVAO, maar ook de ondersteuning van de CDHO en CMMBO (namelijk de medewerkers van het bureau van de commissies) is in dienst van NVAO NL. Daarnaast maken de commissies gezamenlijk gebruik van de afdeling Nederland van de NVAO op het gebied van ICT, financiën en personeelszaken.

Het privacybeleid van NVAO NL omvat daarmee tevens de medewerkers die werkzaam zijn voor het bureau van de CDHO en CMMBO. Het privacybeleid van NVAO NL heeft echter geen betrekking op de werkzaamheden van de commissieleden van de CDHO en CMMBO, aangezien deze onder de verantwoordelijkheid van het Ministerie van OCW vallen. Voor de verwerkingen van de commissies (CDHO/CMMBO) waarbij NVAO NL als verwerker optreedt, is een verwerkingsovereenkomst gesloten.

1.3 Wet- en regelgeving verwerking van persoonsgegevens

1.3.1 Europese en Nederlandse wet- en regelgeving op het gebied van privacy
Sinds 25 mei 2018 is de AVG van toepassing. Vanaf dat moment geldt dezelfde privacywetgeving in de hele Europese Unie.

De AVG is rechtstreeks van toepassing. Waar de AVG ruimte laat voor nationale keuzes bij de uitvoering, zijn deze vastgelegd in de Uitvoeringswet AVG (UAVG)².

Naast deze wetgeving bestaan er aanvullende documenten van het Europees Comité³ voor gegevensbescherming, die onder andere verduidelijking bieden over de toepassing van de AVG.

Daarnaast vormt ook de uitleg van de AVG, veelal vastgelegd in beleidsregels, door de Autoriteit Persoonsgegevens (AP) een belangrijke bron voor de naleving van de AVG. De AP verwacht dat verwerkingsverantwoordelijken, zoals de NVAO (en specifiek afdeling Nederland), de beleidsregels toepassen en de adviezen opvolgen, dan wel gemotiveerd afwijken volgens het "comply or explain"-principe.

Links naar de genoemde wetgeving en relevante documenten in verband met dit Privacy Beleidskader zijn te vinden in Bijlage 2: Overzicht Beleid en Instrumenten.

1.3.2 Context NVAO NL

De AVG laat zich voor NVAO NL het best benaderen vanuit het perspectief van de drie hoofdprocessen van NVAO NL:

- Het primaire proces;
- Het personeelsproces;
- Het betalingsproces.

Het primaire proces

Voor NVAO NL zijn de taken gebaseerd op de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW, hoofdstuk 5). Deze taken omvatten:

- Het accrediteren van bestaande opleidingen;
- Het toetsen van nieuwe opleidingen in het hoger onderwijs;
- Het samenstellen van een commissie van deskundigen en het instemmen met een voordracht voor een commissie van deskundigen,
- Het rapporteren over de kwaliteit van opleidingen aan de minister en het adviseren van de minister in specifieke aangelegenheden zoals opgenomen in de WHW (artikel 5.2 WHW).

Het slotstuk van de accreditatieprocedure is de wettelijke plicht om de uitkomsten ervan te publiceren. Het is niet uitgesloten dat in de toekomst ook andere wet- en regelgeving als basis dient voor de taken van NVAO NL.

Het personeelsproces

Onder het personeelsproces vallen alle verwerkingen die betrekking hebben op persoonsgegevens van het personeel van NVAO NL en van personen die in opdracht van NVAO NL werkzaamheden verrichten.

Het betalingsproces

Onder het betalingsproces vallen alle verwerkingen die verband houden met het overmaken van geld aan leveranciers, commissieleden, personeel en eventuele andere partijen.

² Verder heeft de rijksoverheid een Handreiking naleving AVG geformuleerd. De NVAO overweegt nog hoe deze handreiking in te zetten.

³ European Data Protection Supervisor (EDPS), <https://edps.europa.eu/>

2 NVAO uitgangspunten voor omgang met persoonsgegevens

In dit hoofdstuk worden de uitgangspunten voor de omgang met persoonsgegevens uiteengezet. Vervolgens wordt toegelicht wat deze betekenen voor medewerkers en welke documenten of websites beschikbaar zijn om deze uitgangspunten in het dagelijks werk toe te passen.

Deze uitgangspunten weerspiegelen de visie van NVAO NL op de verwerking van persoonsgegevens. Ze zijn van toepassing op alle verwerkingsactiviteiten die betrekking hebben op persoonsgegevens binnen NVAO NL.

Dit betekent dat alle verwerkingen van persoonsgegevens moeten voldoen aan de volgende acht eisen:

- NVAO NL beperkt de verwerking tot die categorieën persoonsgegevens die nodig zijn voor het beschreven doel;
- NVAO NL verwerkt persoonsgegevens die accuraat en actueel zijn;
- NVAO NL bewaart gegevens niet langer dan noodzakelijk voor het beschreven doel;
- NVAO NL is, indien mogelijk, open en transparant over de verwerking van persoonsgegevens naar de betrokkenen, de samenleving en ketenpartners;
- NVAO NL zorgt ervoor dat persoonsgegevens die aan ons zijn toevertrouwd, veilig en vertrouwelijk worden verwerkt;
- NVAO NL legt verantwoording af over de zorgvuldige verwerking van persoonsgegevens;
- NVAO NL respecteert de rechten van betrokkenen.

Hieronder volgt een nadere instructie per uitgangspunt.

2.1 Grondslag en doel

NVAO NL verwerkt alleen persoonsgegevens als er een rechtmatige grondslag en een duidelijk omschreven en gerechtvaardigd doel voor de verwerking aanwezig zijn.

Instructies:

- Persoonsgegevens mogen alleen worden verwerkt als een van de rechtmatige grondslagen uit artikel 6 van de AVG van toepassing is. Denk bijvoorbeeld aan verwerking op basis van toestemming of een wettelijke verplichting;
- Persoonsgegevens mogen ook alleen worden verwerkt als NVAO NL in het kader van zijn taken verwerkingen uitvoert die "noodzakelijk zijn voor de uitvoering van een wettelijke plicht" of "noodzakelijk zijn voor het uitoefenen van een publiekrechtelijke taak of het openbaar gezag". De rechtsgrondslag voor een dergelijke taak moet in de WHW zijn verankerd. Voor NVAO NL vormt de uitvoering van haar publieke taak bij meerdere verwerkingen van persoonsgegevens in het primaire proces een grondslag voor de verwerking;
- De grondslag "noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerker, de verwerkingsverantwoordelijke of een derde" kan niet worden gebruikt voor verwerkingen door overheidsinstanties in het kader van de uitoefening van hun taken. Deze grondslag kan echter wel van toepassing zijn bij verwerkingen binnen de bedrijfsvoering, zoals cameratoezicht rond het gebouw. Indien van toepassing, hanteert de afdeling Nederland bij afwegingen over de rechtsgrond "gerechtvaardigd belang" het normenkader gerechtvaardigd belang;
- De ongelijke machtsverhouding tussen de betrokkene en de overheid belemmert over het algemeen de eis dat toestemming vrijelijk moet worden verleend. Binnen de Afdeling Nederland is voor de rechtsgrond "toestemming" in de relatie tussen

werkgever en werknemer geborgd dat toestemming vrijwillig en ondubbelzinnig kan worden gegeven en ingetrokken. Bovendien heeft het niet geven van toestemming op geen enkele wijze verdere gevolgen voor de betrokkene. Dit is vastgelegd in het formulier "Toestemming AVG" (bijlage 2).

- Elke verwerking of wijziging daarvan moet worden opgenomen in het Register van verwerkingen. Dit register bevat een beschrijving van de verwerkingsactiviteiten. De verantwoordelijke (NVAO NL) moet dit register op verzoek aan de AP kunnen tonen. Bij een dergelijk verzoek van de AP dient contact te worden opgenomen met de Privacy Officer (PO), die dit in afstemming met de directie en het (waarnemend) bestuur verzorgt. Het Register van verwerkingen bevat zelf geen persoonsgegevens.
- Het doel van elke verwerking is concreet en vastgelegd in het Register van verwerkingen. Als een bestand voor meerdere doelen wordt gebruikt, wordt dit vermeld in de doelomschrijving. Duidelijk omschreven doelen maken het voor de betrokkene inzichtelijk wat er met de gegevens wordt gedaan. Bij verdere verwerking van persoonsgegevens voor een ander doel dan waarvoor ze oorspronkelijk zijn verzameld, wordt altijd beoordeeld of dit nieuwe doel verenigbaar is met het oorspronkelijke doel;
- NVAO NL is verplicht een Data Protection Impact Assessment (DPIA), ook wel Gegevensbeschermingseffect-beoordeling (GEB) genoemd, uit te voeren bij de ontwikkeling van beleid en regelgeving waaruit verwerkingen van persoonsgegevens voortvloeien. De AP heeft een lijst opgesteld van verwerkingen waarvoor een DPIA verplicht is. De DPIA heeft als doel de effecten van de beoogde gegevensverwerking(en) voor betrokkenen te inventariseren en te beoordelen. Op basis van de DPIA kunnen maatregelen worden genomen om de risico's te beheersen. Hiervoor kan het Rijksmodel GEB (PIA) of het model in Privacy Nexus worden gebruikt (zie ook bijlage 2). In Privacy Nexus wordt tevens het DPIA-register bijgehouden. Bij een DPIA is het verplicht om advies in te winnen bij de Functionaris Gegevensbescherming (FG);
- Vragen over het proces, de opzet en de uitvoering van de DPIA kunnen worden gesteld aan de PO en de FG. Raadpleeg eventueel het document *DPIA Proces NVAO NL* of gebruik de *Quick Scan PrePIA* om te beoordelen of een DPIA nodig is (zie bijlage 2).

2.2 Doelbinding

NVAO NL beperkt de verwerking tot de categorieën persoonsgegevens die noodzakelijk zijn voor het beschreven doel.

Instructies:

- Alleen de gegevens die noodzakelijk zijn voor het vooraf en precies omschreven doel mogen worden verzameld. Gegevens mogen vervolgens niet verder worden verwerkt als dit onverenigbaar is met dat doel. Persoonsgegevens die niet meer nodig zijn, moeten worden verwijderd of, waar mogelijk, geanonimiseerd⁴. Bij de ontwikkeling van nieuwe of de wijziging van bestaande producten en diensten wordt rekening gehouden met gegevensbescherming;
- Verwerk niet meer gegevens dan aantoonbaar noodzakelijk zijn voor het doel van de verwerking (dataminimalisatie). Denk kritisch na over waarom je bepaalde gegevens nodig hebt voor deze specifieke verwerking en of alle gegevens daadwerkelijk noodzakelijk zijn;

⁴ De AVG is niet van toepassing op anonieme gegevens, omdat deze niet kunnen worden teruggevoerd op een geïdentificeerde of identificeerbare natuurlijke persoon. Anonimisering houdt in dat gegevens onomkeerbaar worden versleuteld, zodat ze niet meer met personen in verband kunnen worden gebracht. Bij pseudonimisering blijven de gegevens wel herleidbaar naar natuurlijke personen, mits de juiste sleutel wordt gebruikt. Hierdoor vallen gepseudonimiseerde gegevens wél onder de AVG.

- Nieuwe systemen worden zo geconfigureerd dat alleen de gegevens worden verwerkt die noodzakelijk zijn voor het specifieke verwerkingsdoel. Privacy moet daarom vanaf de ontwerpfase van een (nieuw) automatiseringssysteem als uitgangspunt worden genomen (*privacy by design*);
- Hanteer bij de ontwikkeling van beleid, processen en systemen altijd de meest privacybeschermende instellingen (*privacy by default*);
- Raadpleeg bij de ontwikkeling en uitwerking van beleid, processen en systemen de *Handleiding Privacy by Design & by Default* voor meer inzicht in privacyvriendelijk ontwerp, waarbij de bescherming van persoonsgegevens is ingebouwd.

2.3 Accuraat en actueel

NVAO NL verwerkt persoonsgegevens die accuraat en actueel zijn. Dit betekent onder meer dat gegevens zorgvuldig worden beheerd (*betrouwbaarheid en integriteit*) en dat betrokkenen verzoeken kunnen indienen voor de rectificatie van onjuiste persoonsgegevens (*rechten van betrokkenen*).

Om te borgen dat de verwerkte persoonsgegevens betrouwbaar en actueel zijn, worden in het primaire proces alle wijzigingen die door contactpersonen van instellingen, evaluatiebureaus en zelfstandigen worden doorgegeven direct verwerkt. Dit geldt ook voor panelleden van de accreditatie nieuwe opleiding (TNO) en de instellingstoets kwaliteitszorg (ITK), van wie wijzigingen in de verstrekte gegevens worden doorgegeven en verwerkt.

De afdeling Nederland van NVAO verwerkt deze wijzigingen direct in het systeem voor het primaire proces. Via een beveiligde functionaliteit in het personeels- en salarissysteem (AFAS) kunnen externen die in opdracht van de Afdeling Nederland werken hun persoonsgegevens zelfstandig bijhouden. Dit geldt ook voor medewerkers in dienst van NVAO NL, die al hun persoonsgegevens zelf kunnen beheren in AFAS.

Secretarissen die werkzaamheden verrichten in het accreditatieproces worden jaarlijks gevraagd hun gegevens te controleren en aan te geven of zij hun registratie in het register van secretarissen willen verlengen.

In de privacyverklaringen van NVAO NL (intern en extern) is vastgelegd hoe betrokkenen hun rechten onder de AVG kunnen uitoefenen, zoals het recht op informatie, inzage, rectificatie, verwijdering, beperking van verwerking, gegevensoverdracht en bezwaar. Voor de afhandeling hiervan wordt binnen NVAO NL gewerkt met het *Protocol rechten van betrokkenen* (zie ook paragraaf 2.8).

Instructies:

- Waarborg de juistheid en actualiteit van persoonsgegevens zoveel mogelijk door periodieke controles en/of verificatie van bestaande gegevens of nieuwe input, bijvoorbeeld wanneer panelleden opnieuw zitting nemen in een panel;
- Zorg ervoor dat gegevens kunnen worden aangepast wanneer ze onjuist, onvolledig of verouderd zijn;
- Raadpleeg indien gewenst het *Protocol Rechten van Betrokkenen*.

2.4 Bewaarbeperking

NVAO NL bewaart gegevens niet langer dan noodzakelijk voor het beschreven doel of zolang als wettelijk vereist.

- Voor het primaire proces, het personeelsproces en het betalingsproces zijn de bewaartermijnen vastgelegd in de *Selectielijst* NVAO, die geldig is tot 2032. Deze lijst hanteert, waar van toepassing, de wettelijke termijnen voor personele en financiële aangelegenheden;
- Nadat een bewaartermijn is verstreken, wordt een steekproef van de accreditatiedossiers overgedragen aan het Nationaal Archief (NA). De dossiers die niet worden overgedragen, worden na afloop van de bewaartermijn vernietigd, overeenkomstig de *Selectielijst* NVAO.

In aanvulling op de *Selectielijst* en ter overbrugging naar een nieuw vorm te geven *Selectielijst* hanteert NVAO NL een bewaartermijnenlijst voor zaken die niet in de *Selectielijst* zijn geregeld. Het uitgangspunt van deze lijst is dat voor procedures die verband houden met het accreditatieproces aansluiting wordt gezocht bij verwante procedures.

Voor overige procedures die geen onderdeel uitmaken van de *Selectielijst*, zoals verzoeken op grond van de AVG of de Wet open overheid (Woo), is een bewaartermijn opgenomen in de bewaartermijnenlijst. Daarbij wordt zoveel mogelijk aangesloten op de termijnen van de *Selectielijst*.

Ter illustratie: voor de nieuwe taak *Kwaliteitsafspraken* is aansluiting gezocht bij het ITK-proces, waarvoor een bewaartermijn van 18 jaar geldt. Daarna vindt steekproefsgewijze overdracht aan het NA plaats en worden de overige dossiers vernietigd.

Waar een langere bewaartermijn minder voor de hand ligt vanuit het oogpunt van de AVG (*niet langer bewaren dan strikt noodzakelijk; indien geen doelbinding meer, dan niet langer bewaren*), is een aangepaste bewaartermijn vastgesteld op basis van de situatie.

Instructies:

- Persoonsgegevens kunnen meerdere doelen dienen; houd hier rekening mee bij het vaststellen van bewaartermijnen;
- Bewaar persoonsgegevens niet langer dan noodzakelijk voor de doelen van de verwerking;
- Stel bewaartermijnen vast en wis gegevens wanneer deze niet langer noodzakelijk zijn voor het verwerkingsdoel;
- Raadpleeg indien gewenst de *Selectielijst* NVAO.

2.5 Open en transparant

NVAO NL is, waar mogelijk, open en transparant over de verwerking van persoonsgegevens jegens betrokkenen en ketenpartners. Betrokkenen moeten weten wat er met hun persoonsgegevens gebeurt. NVAO NL verstrekt informatie over de verwerking en omgang met persoonsgegevens, evenals over de rechten van betrokkenen, op een toegankelijke en begrijpelijke manier. Dit gebeurt via een interne en externe privacyverklaring en een cookieverklaring.

Instructies:

- NVAO NL verstrekt de vereiste informatie aan medewerkers (inclusief de medewerkers van CDHO en CMMBO) en aan personen die in opdracht van NVAO NL diensten verrichten via de interne privacyverklaring op intranet of SharePoint. Indien nodig wordt aanvullende toelichting gegeven over nieuwe of bestaande verwerkingen;
- De privacyverklaringen van NVAO NL (intern en extern) worden periodiek door de afdeling Nederland gecontroleerd op actualiteit.

2.6 Veilig en vertrouwelijk

NVAO NL zorgt ervoor dat de aan haar toevertrouwde persoonsgegevens veilig en vertrouwelijk worden verwerkt.

Instructies:

- NVAO NL is op basis van wet- en regelgeving verplicht om passende technische en organisatorische maatregelen te treffen om persoonsgegevens adequaat te beschermen tegen ongeautoriseerde verwerkingen. Hiertoe heeft NVAO NL een beleidskader voor informatiebeveiliging (IB) opgesteld.
NVAO NL verstrekt alleen toegang tot persoonsgegevens aan personen die deze gegevens nodig hebben en gemachtigd zijn om ze te verwerken. Op systeem- en applicatieniveau zijn hiervoor autorisatiematrices opgesteld (zie bijlage 2). Voor de fysieke toegang tot ruimten en documenten is eveneens een overzicht van geautoriseerde personen en functies opgesteld;
- Datalekken moeten zoveel mogelijk worden voorkomen. Een datalek is een inbreuk op de beveiliging van persoonsgegevens die leidt tot vernietiging, verlies, wijziging, of ongeoorloofde verstrekking of toegang tot gegevens;
- Een datalek dat een risico inhoudt voor de rechten van betrokkenen, moet binnen 72 uur worden gemeld bij de AP en in sommige gevallen ook aan de betrokkene. Hiervoor is het *Protocol Beveiligingsincidenten en Datalekken NVAO NL* opgesteld. Raadpleeg bij een (vermeend) datalek de PO. Voor een eerste beoordeling van het incident of datalek gebruikt de afdeling Nederland het formulier *Quick Scan*;
- Via e-mail worden veel bestanden uitgewisseld, waaronder vaak persoonsgegevens. Bij voorkeur en indien mogelijk werkt NVAO NL binnen een beveiligde omgeving waarin bestanden veilig kunnen worden gedeeld (bijvoorbeeld via SharePoint). Indien verzending per e-mail noodzakelijk is, moet een passend beschermingsniveau worden toegepast. Bij het versturen van bestanden met persoonsgegevens is het raadzaam deze versleuteld naar de ontvanger te sturen. Dit verkleint het risico dat bestanden per ongeluk bij de verkeerde ontvanger terechtkomen;
- Om een datalek te voorkomen dat wordt veroorzaakt door de optie 'Suggesties' in Outlook, wordt medewerkers van afdeling Nederland geadviseerd deze optie uit te schakelen en bewust een keuze te maken bij het selecteren van een geadresseerde.
- NVAO NL, en in het bijzonder het Privacy Office van afdeling Nederland, houdt een register bij van datalekken en beveiligingsincidenten die afdeling Nederland betreffen;
- Wanneer een verwerker wordt ingeschakeld, wordt een verwerkingsovereenkomst afgesloten. NVAO NL hanteert hiervoor het rijksmodel, inclusief een procedure voor de aanpak van een datalek;
- Raadpleeg indien nodig het *Informatiebeveiligingsbeleid NVAO NL*.

2.7 Verantwoordingsplicht

NVAO NL legt verantwoording af over de zorgvuldige verwerking van persoonsgegevens.

Instructies:

- NVAO NL neemt passende maatregelen om de bescherming van persoonsgegevens te waarborgen. Aan de hand van documentatie kan NVAO NL aantonen dat de privacyregels worden nageleefd. Evaluatie en monitoring van de maatregelen maken eveneens deel uit van de verantwoording. Deze verantwoordingsplicht (*accountability*) staat centraal in het wettelijk privacykader;
- Het Privacy Office van NVAO NL beheert een *Register van Verwerkingsactiviteiten*. Dit register bevat informatie over de gegevens die worden verwerkt. De persoonsgegevens zelf worden niet in het register opgenomen, maar wel de categorieën persoonsgegevens die worden verwerkt;

- Wijzigingen in verwerkingen moeten door medewerkers en/of de directie aan het Privacy Office worden doorgegeven;
- De directie van afdeling Nederland heeft de zelfstandige verantwoordelijkheid om bij nieuwe verwerkingen (activiteiten of andere ICT-systemen) de PO van afdeling Nederland en, indien nodig, de FG op de hoogte te stellen;
- NVAO NL vergewist zich ervan dat derde partijen persoonsgegevens op een behoorlijke en zorgvuldige manier verwerken. Dit betreft niet uitsluitend partijen waarmee een verwerkersovereenkomst moet worden afgesloten. Denk bijvoorbeeld aan de Arbodienst, die een eigen verwerkingsverantwoordelijkheid heeft. Waar nodig wordt een verwerkingsovereenkomst gesloten, die wordt opgenomen in het *Register Verwerkingsovereenkomsten* (*Privacy Nexus*; tijdelijk wordt dit in tabelvorm bijgehouden).

2.8 Respect

NVAO NL respecteert de rechten van de betrokkenen.

Instructies:

- NVAO NL richt systemen, processen en de interne organisatie zodanig in dat op de juiste manier gehoor wordt gegeven aan verzoeken van betrokkenen omtrent persoonsgegevens;
- NVAO NL hanteert een *Protocol Rechten Betrokkenen*, waarin de (belangrijkste) rechten van betrokkenen zijn geformuleerd, zoals inzage, rectificatie, wissen, overdracht en beperking van verwerking. In dit protocol wordt ook beschreven hoe een verzoek wordt behandeld en waar een betrokkene rekening mee kan houden. Dit protocol heeft interne werking en is bedoeld om handvatten te bieden voor het Privacy Office;
- NVAO NL kan gebruik maken van een model voor de beantwoording van inzageverzoeken of andere modellen om aan verzoeken te voldoen.
In de interne en externe privacyverklaringen worden onder andere de rechten van betrokkenen ten aanzien van hun persoonsgegevens omschreven. In deze privacyverklaringen wordt ook aangegeven voor wie de betreffende privacyverklaring geldt.
Alle betrokkenen (intern en extern) kunnen bij de AP een klacht indienen over de manier waarop NVAO NL met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.

3 Privacy governance

3.1 Inleiding

Doel van dit hoofdstuk over de privacy governance is om inzicht te geven in de verantwoordelijkheden op het gebied van privacybescherming binnen NVAO NL. De governancestructuur helpt NVAO NL zorgvuldig om te gaan met persoonsgegevens en verantwoording af te leggen over genomen beslissingen. Een robuuste beheersorganisatie is essentieel voor de implementatie en handhaving van de principes en doelstellingen uit het privacybeleid van afdeling Nederland.

Omgevingsveld

NVAO is een zelfstandig bestuursorgaan en valt onder de politieke verantwoordelijkheid van het Comité van Ministers. Hoewel NVAO een zelfstandig bestuursorgaan is, blijft het Comité van Ministers politiek eindverantwoordelijk voor de naleving van wet- en regelgeving, inclusief de AVG.

De AP is de toezichthoudende autoriteit met betrekking tot de naleving van de vereisten van de AVG. Wanneer betrokkenen klachten hebben over hoe NVAO NL omgaat met persoonsgegevens, kunnen zij terecht bij de AP.

De Nationale Ombudsman kan eventueel ook een bemiddelende rol spelen tussen NVAO NL en personen van wie de NVAO NL persoonsgegevens verwerkt.

3.2 Privacy verantwoordelijkheden, rollen en taken

Wat is de rol van de FG?

De functie van de FG binnen NVAO NL is voornamelijk gericht op het waarborgen van de privacy en bescherming van persoonsgegevens, in overeenstemming met de AVG en andere relevante wet- en regelgeving

Adviesfunctie: De FG adviseert de organisatie over de naleving van de AVG. Dit omvat het geven van advies over hoe NVAO NL persoonsgegevens kan verwerken in overeenstemming met de wet.

Toezicht houden: De FG houdt toezicht op de naleving van de AVG binnen de organisatie. Dit kan inhouden dat de FG audits uitvoert en processen evalueert om ervoor te zorgen dat gegevens effectief en veilig worden beheerd.

DPIA: In bepaalde situaties, wanneer er een hoog risico is voor de rechten en vrijheden van betrokkenen, is de FG betrokken bij het uitvoeren van een DPIA.

Contactpunt voor toezichthouders: De FG fungeert als het contactpunt voor toezichthouders, zoals de AP, en als aanspreekpunt voor betrokkenen wiens persoonsgegevens worden verwerkt.

Relevante wetsartikelen

Aanwijzing van de FG

Artikel 37: Dit artikel beschrijft wanneer een FG moet worden aangesteld (bijvoorbeeld wanneer de organisatie een publieke autoriteit is of wanneer de kernactiviteiten van de organisatie het beheer van gegevens vereisen).

Taken van de FG

Artikel 39: Dit artikel beschrijft de specifieke taken van de FG, zoals het informeren en adviseren

van de organisatie, toezicht houden op de naleving van de AVG, en samenwerken met de toezichthoudende autoriteit.

Onafhankelijkheid van de FG

Artikel 38: Dit artikel stelt dat de FG onafhankelijk moet kunnen optreden en niet ontslagen of gestraft mag worden voor de uitvoering van zijn taken.

Wat is de rol van het Privacy Office?

De rol van de Privacy Office binnen NVAO NL is van cruciaal belang in het waarborgen van de privacy en de bescherming van persoonsgegevens.

Beleid en advies: Het ontwikkelen van beleid en richtlijnen met betrekking tot privacy, en het adviseren van de organisatie over privacygerelateerde onderwerpen.

Gegevensbescherming: Toezien op de naleving van privacywetgeving en ervoor zorgen dat persoonsgegevens veilig worden verwerkt.

Training en bewustwording: Het organiseren van trainingen en workshops voor medewerkers over privacy en gegevensbescherming, om bewustwording te creëren en best practices te bevorderen.

Risicoanalyse: Het uitvoeren van risicoanalyses met betrekking tot de verwerking van persoonsgegevens en het implementeren van maatregelen om risico's te verkleinen.

Verwerkingsovereenkomsten: Het beheren van contracten en overeenkomsten met derde partijen die persoonsgegevens verwerken in opdracht van NVAO NL.

Klachten en incidenten: Het behandelen van klachten en meldingen over privacy-inbreuken of datalekken, en het zorgen voor een juiste opvolging en rapportage.

Door deze rol te vervullen, draagt de Privacy Office bij aan een verantwoord en transparant gebruik van persoonsgegevens binnen NVAO NL en helpt daarmee het vertrouwen van zowel instellingen als individuele personen in de organisatie te waarborgen.

Naast de Privacy Office heeft NVAO NL een Information Security Officer (ISO). De Privacy Office en de ISO adviseren en ondersteunen de directie en medewerkers bij privacyaspecten. Op verzoek van de directie kan ook advies en ondersteuning worden gegeven aan het bestuur. Bepaalde beleids- en organisatie-taken, zoals het uitvoeren van interne risicoanalyses, behoren ook tot hun takenpakket. Primair is de Privacy Office het aanspreekpunt voor de uitleg van de AVG binnen NVAO NL en bij de implementatie en uitvoering van de AVG.

NVAO NL heeft een PO die de volgende taken verricht:

- Beheert het privacybeleid en kan op verzoek van de directie, of via de directie op verzoek van het bestuur, of uit eigen beweging een voorstel tot aanpassing van het beleid doen;
- Zorgt voor de dagelijkse afhandeling van privacy-aangelegenheden voor NVAO NL;
- Beheert het register van verwerkingsactiviteiten;
- Stelt de jaarplanning op;
- Fungeert als vraagbaak voor de directieleden van Afdeling Nederland ten aanzien van het verzamelen, registreren en leveren van persoonsgegevens. Hij raadpleegt indien nodig de FG of externe adviseurs over complexere verwerkingen en relaties met verwerkers;
- Adviseert de directieleden van NVAO NL bij de analyse van mogelijke risico's die samenhangen met de verwerking van persoonsgegevens.

Wat is de rol van de ISO?

De rol van de ISO binnen NVAO NL is cruciaal voor het waarborgen van de IB binnen de afdeling en de organisatie. Het vereist een zorgvuldige afstemming met experts op het gebied van juridische zaken, het privacy office, ICT, beveiliging, communicatie, directie en de FG. Hoewel de specifieke taken en verantwoordelijkheden kunnen variëren, omvatten de belangrijkste taken van een ISO doorgaans het volgende:

De ISO heeft onder meer als taak:

Risicobeheer: Het identificeren, analyseren en beheren van risico's met betrekking tot IB. Dit omvat het uitvoeren van risicoanalyses en het aanbevelen van passende maatregelen om deze risico's te minimaliseren.

Bewustwording en Training: Het bevorderen van bewustwording rondom IB binnen de organisatie, waaronder het organiseren van trainingen en informatiesessies voor personeel.

Compliance: Zorgen voor naleving van relevante wet- en regelgeving, normen en richtlijnen op het gebied van IB.

Incidentbeheer: Het beheren van beveiligingsincidenten, inclusief het opstellen van procedures voor het melden en afhandelen van incidenten.

Toegangsbeheer: Toezicht houden op de toegangsrechten tot informatie en systemen, en ervoor zorgen dat deze op een veilige manier worden beheerd.

Samenwerking: Samenwerken met andere afdelingen en stakeholders om een geïntegreerde benadering van IB te waarborgen.

Rapportage: Het monitoren van de effectiviteit van de informatiebeveiligingsmaatregelen en het rapporteren aan het management over de status en eventuele verbeterpunten.

Aanvullend:

De ISO ondersteunt en adviseert NVAO NL bij privacyvraagstukken. De ISO helpt onder meer door het geven van (indien mogelijk) advies op maat, het opbouwen van de noodzakelijke kennis over IB en privacy, wet- en regelgeving, het toepassen hiervan en het (mede) ontwikkelen van producten zoals informatiebeleid en privacyconvenanten. Verder is de ISO verantwoordelijk voor het monitoren en borgen van de eisen en architectuur voor IB, en het consequent toepassen van security-by-design en privacy-by-design.

Wat is de rol van de Ondernemingsraad (OR) bij privacyvraagstukken?

De OR van de afdeling Nederland (OR-NL) vertegenwoordigt het personeel van NVAO NL en beschermt hun belangen. De OR-NL heeft daarvoor verschillende rechten en bevoegdheden, zoals het recht op informatie, het adviesrecht, het instemmingsrecht en het initiatiefrecht. Met name het adviesrecht, instemmingsrecht en initiatiefrecht spelen een rol bij de uitvoering van de AVG (Artikel 27 WOR).

Het kan zijn dat er nieuwe technische maatregelen worden getroffen om te voldoen aan de AVG. Denk bijvoorbeeld aan technische maatregelen om persoonsgegevens te beveiligen of om ervoor te zorgen dat alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor het verwerkingsdoel.

Op grond van de Wet op de Ondernemingsraden (WOR) dient een besluit tot het invoeren of wijzigen van een technologische voorziening ter advies aan de OR te worden voorgelegd. Dit betekent dat als NVAO NL nieuwe ICT wil aanschaffen ter beveiliging van persoonsgegevens, zowel de OR-NL als de Centrale Ondernemingsraad (COR) adviesrecht hebben.

Een besluit tot vaststelling, wijziging of intrekking van een regeling over het verwerken van, alsmede de bescherming van persoonsgegevens van de bij NVAO NL werkzame personen is instemmingsplichtig. Het moet dus gaan om een regeling die tot doel heeft persoonsgegevens te verzamelen, bewaren, gebruiken, verstrekken of beveiligen. Dit geldt onder meer voor de vaststelling van dit privacybeleid en voor het melden van een datalek waarbij persoonsgegevens zijn betrokken.

Tenslotte kan de OR gebruikmaken van haar initiatiefrecht om voorstellen te doen voor (een aanpassing van) het privacybeleid.

Wat is de rol van HR?

Daarnaast speelt HR een rol in de zorgvuldige omgang met persoonsgegevens. Direct bij indiensttreding worden in het kader van awareness afspraken gemaakt met het Privacy Office (zie paragraaf 3.5). HR is het eerste aanspreekpunt voor personeelsgerelateerde vragen van medewerkers over de AVG en stemt zo nodig af met het Privacy Office.

3.3 Privacy overlegstructuren

Wekelijks vindt overleg plaats tussen de directie en het Privacy Office over de voortgang van AVG-onderwerpen. Ook is het onderwerp van gesprek in periodiek overleg met de WOO-coördinator van NVAO NL en de directie. Vanuit de directie wordt deelgenomen aan kwartaaloverleg met de FG. De directie informeert het bestuur over actuele onderwerpen en de voortgang hiervan. Jaarlijks vindt in het dagelijks bestuur een bespreking van de jaarrapportage van de FG plaats. Acties die uit de rapportage voortkomen, worden belegd binnen de afdeling waar de betreffende actie betrekking op heeft.

NVAO NL neemt actief deel aan overleggen van KleinLef-organisaties (AVG-werkgroep, Rijksbrede Benchmark Groep) op het gebied van privacy, om kennis over privacy te delen en elkaar te helpen bij het ontwikkelen van privacybeleid.

3.4 Sturing, regie en toezicht

Periodiek voert NVAO NL, met behulp van de tool in Privacy-Nexus of in een afzonderlijke meting op een instrument/beleidsonderdeel, self-assessments uit, waaruit de stand van zaken met betrekking tot privacy blijkt. In de jaarplanning wordt opgenomen welke acties hierop gepland staan. Ook kunnen zaken ongepland bijgesteld worden indien een specifieke situatie daartoe aanleiding geeft. De jaarplanning wordt dan op basis hiervan bijgesteld.

Interne toezichtsorganen: FG en OR

Tenslotte kent NVAO NL een FG en de OR-NL. Zij zijn vanwege hun specifieke rollen en wettelijke taken betrokken bij aspecten van de privacy binnen NVAO NL.

Externe toezichthouders, zoals de AP en eventueel ingehuurd auditors, kunnen de inregeling en uitvoering van de AVG controleren. Het is de eigen verantwoordelijkheid van NVAO NL om intern toezicht te houden op de waarborging van privacybescherming, los van eventuele externe audits en evaluaties.

3.5 Privacy trainingen en bewustwording

Alle medewerkers krijgen bij hun aanstelling een korte introductie over de AVG van het Privacy Office. De tekst van de eed/belofte is opgenomen in de Personeelsregeling (zie bijlage 2); hierin is de geheimhouding ten aanzien van de AVG verankerd.

Daarnaast vinden reguliere bewustwordingsacties plaats, waarbij minimaal twee keer per jaar aandacht wordt besteed aan een privacyonderwerp vanuit het Privacy Office voor afdeling Nederland. Het Privacy Office volgt regelmatig trainingen op het gebied van de AVG en houdt de voortgang hiervan bij in de jaarplanning, ten behoeve van de directie en de FG.

4 Slot

Met dit privacybeleid brengt NVAO NL in kaart welke maatregelen er zijn genomen om de persoonsgegevens van medewerkers en externen, waaronder onder andere panelleden, secretarissen en studenten, te beschermen. Daarnaast biedt het beleid inzicht in de wijze waarop de verantwoordelijkheden op grond van de AVG binnen NVAO NL zijn belegd. Ook is per uitgangspunt vastgelegd welke instructies er zijn en welke documenten geraadpleegd kunnen worden. Hiermee wordt voldaan aan belangrijke verplichtingen op grond van de AVG, zoals het inrichten en bijhouden van een Register van Verwerkingen, de wijze waarop wordt omgegaan met datalekken, het uitvoeren van een DPIA, het opstellen van een interne en externe privacyverklaring, en de wijze waarop de rechten van betrokkenen zijn georganiseerd.

4.1 Beheer

Het Privacy Office van NVAO NL is verantwoordelijk voor het beheer van dit privacybeleidskader.

De instrumenten en dit beleidskader zijn levende documenten die periodiek (moeten) worden geactualiseerd, mede naar aanleiding van vragen, incidenten, klachten, enzovoort. Algemene vragen over dit beleid of verzoeken en/of suggesties tot wijziging of toevoeging aan het beleid kunnen worden gericht aan het Privacy Office van NVAO NL (privacy@nvaio.net).

4.2 Vaststelling

Dit privacybeleid is voor het eerst vastgesteld op 15 maart 2021 door het Algemeen Bestuur (AB) van de NVAO en is, in verband met de verbijzondering, opnieuw voorgelegd aan de directie en de OR-NL. Het voorliggende beleid is vastgesteld op 6 november 2024, ten behoeve van toezending aan de FG voor de jaarrapportage. Naar aanleiding van de inbreng van de FG zijn enkele aanpassingen doorgevoerd en is de aangepaste versie vastgesteld op 12 februari 2025.

4.3 Wijzigingen en evaluatie

Privacybeleid is dynamisch beleid. Nieuwe ontwikkelingen volgen elkaar op en ook de organisatie zelf zal steeds in ontwikkeling zijn. Dit betekent dat het privacybeleid regelmatig bijgewerkt zal moeten worden. Dit beleid wordt periodiek herzien en aangepast. De volgende tabel toont de (concept)versiegeschiedenis van dit privacybeleid. In de jaarplanning van het Privacy Office (opvraagbaar) zijn per kwartaal eventuele herzieningen opgenomen.

Datum	Opmerkingen	Versie
16 oktober 2019	1 ^e concept beleidsdocument	0.1
27 juli 2020	Concept t.b.v. FG	0.2
2 november 2020	Concept t.b.v. directeur NL	0.3
28 januari 2021	Concept t.b.v. Dagelijks Bestuur (DB)	0.4
16 februari 2021	Goedkeuring door DB	16-2-2021
15 maart 2021	Goedkeuring AB en mandatering DB en ondermandaat Privacy Office	15-3-2021
15 april 2021	Aanvulling data en technische aanpassingen (IM vervangen door CISO/privacyverklaringen hernoemd, cookieverklaring toegevoegd en protocol rechten betrokkenen hernoemd)	15-4-2021
22 april 2021	Naast CISO de IM gezet (RASCI 1 kolom voor gezamenlijke taken)	22-4-2021
7 juni 2021	Regeling rechten betrokkenen naam gewijzigd; interne werking	7-6-2021
10 juni 2021	Naam oud-voorzitter verwijderd	10-6-2021
18 oktober 2024	Vernieuwd concept beleid naar directie/OR	Oktober 2024
6 november 2024	Bespreking vernieuwd concept.	November 2024
12 februari 2025	Actuele versie	Februari 2025

5 Contactgegevens

Voor vragen naar aanleiding van deze privacyverklaring, voor verzoeken zoals inzage in uw persoonsgegevens of klachten, kan contact worden opgenomen met privacy@nvao.net.

Bijlage 1: Begrippen

Wat zijn persoonsgegevens?

Niet alle data of gegevens zijn per definitie persoonsgegevens. Persoonsgegevens betreft alle informatie met betrekking tot een geïdentificeerde of identificeerbare natuurlijke persoon (de "betrokkene").

De betrokkene hoeft geen direct geïdentificeerd individu te zijn, maar zodra een individu uit een groep kan worden onderscheiden, zijn de gegevens persoonsgegevens. Het is dus niet altijd nodig om de naam van de persoon in kwestie te weten om te spreken van persoonsgegevens.

Alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare persoon moeten als persoonsgegevens worden beschouwd. Enkel transactiegegevens zijn bijvoorbeeld op zichzelf geen direct identificeerbare gegevens, maar worden persoonsgegevens wanneer deze verband houden met een geïdentificeerde of identificeerbare persoon, bijvoorbeeld omdat deze is gekoppeld aan een naam, een e-mailadres of een telefoonnummer.

De AVG heeft een speciaal regime voor bijzondere categorieën persoonsgegevens. Dit betreft persoonsgegevens waaruit de raciale of etnische afkomst, politieke opvattingen, religieuze of filosofische overtuigingen blijken, lidmaatschap van een vakvereniging, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie, gezondheids- of medische gegevens, gegevens over iemands seksleven of seksuele geaardheid.

Strafrechtelijke persoonsgegevens zijn persoonsgegevens die te maken hebben met strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen. Hieronder vallen zowel veroordelingen als mogelijk gegronde verdenkingen. Dit wil zeggen dat er concrete aanwijzingen zijn dat iemand een strafbaar feit heeft gepleegd. Een voorbeeld hiervan is een opgestelde zwarte lijst van frauderende klanten bij een financiële instelling. Onder de AVG gelden speciale regels voor het verwerken van strafrechtelijke gegevens.

De verwerking, het verzamelen of gebruiken van gevoelige persoonsgegevens is verboden, tenzij een uitzondering op het algemene verbod van toepassing is. Het verzamelen en gebruiken van dergelijke gegevens zal daarom zoveel mogelijk worden vermeden. Vermijd ook het verzamelen en gebruik van gegevens van gevoelige groepen, zoals kinderen / minderjarigen, gehandicapten en ouderen, tenzij hiervoor duidelijk toestemming is gegeven door de bevoegde persoon.

Voorbeelden van gegevens die over het algemeen als persoonsgegevens worden beschouwd:

Voornaam en/of initialen en achternaam	Financiële gegevens
E-mailadres	Betaling of transactiegegevens
Telefoonnummer	Rijbewijs
Foto	Strafrecht ketennummer
Geboortedatum / geboorteplaats	Identificatienummer werknemer
IP-adres	Werknemers informatie
Uitkomsten functioneringsgesprekken	Medische informatie
Burgerservicenummer	Biometrische gegevens
Unique Device Identifiers	MAC-adressen

Wat is een betrokkene?

De betrokkene is de persoon van wie persoonsgegevens worden verwerkt.

Wat is een verwerking?

Het 'verwerken van persoonsgegevens' of een 'verwerking van persoonsgegevens' betreft alle handelingen die men met persoonsgegevens kan verrichten. Denk hierbij aan het verzamelen, vastleggen, raadplegen, opvragen, ordenen, structureren, opslaan, bewerken of wijzigen, verstrekken en combineren. Ook het wissen of vernietigen van gegevens valt onder een verwerking van persoonsgegevens.

Wat is een verwerkingsverantwoordelijke?

De verwerkingsverantwoordelijke is de natuurlijke persoon of rechtspersoon die (alleen of tezamen met anderen) bepaalt welke persoonsgegevens worden verzameld, waarom persoonsgegevens worden verwerkt (doel) en hoe persoonsgegevens worden verwerkt (middelen). Wanneer partijen gezamenlijk het doel en de middelen vaststellen voor de verwerking van persoonsgegevens, spreken we van een gezamenlijke verantwoordelijkheid.

Wat is een verwerker?

Een verwerker is de natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Het gaat om derde partijen die voor de verwerkingsverantwoordelijke werken. Een verwerker handelt onder de verantwoordelijkheid van de verwerkingsverantwoordelijke en naar diens instructies, maar er is geen hiërarchische relatie (medewerkers zijn geen verwerkers). Daarnaast heeft de verwerker geen zeggenschap over de verwerkingen en mag de gegevens niet voor eigen doeleinden gebruiken.

Bijlage 2: Overzicht beleid en instrumenten

Wet- en regelgeving

AVG Algemene Verordening Gegevensbescherming

UAVG Uitvoeringswet Algemene Verordening Gegevensbescherming

Websites

EDPS European Data Protection Supervisor, <https://edps.europa.eu/>

AP Autoriteit Persoonsgegevens, <https://autoriteitpersoonsgegevens.nl/>

Nr	Documenten	Vindplaats in H2 privacybeleid	Vindplaats In organisatie
1	Privacybeleidskader NVAO NL	Dit document	Intranet
2	Informatiebeveiligingsbeleid NVAO NL	2.6	ISO
	Instrumenten voor verantwoording		
3	Cookieverklaring	2.5	website
4	Privacyverklaring NVAO NL medewerkers + medewerkers CDHO/CMMBO	2.5 en 2.8	Intranet
5	Privacyverklaring extern afdeling NL	2.1	website
6	Protocol beveiligingsincidenten en datalekken NVAO NL	2.6	Intranet
7	Register datalekken en beveiligingsincidenten	2.6	Privacy nexus
8	Protocol Rechten Betrokkenen	2.3 en 2.8	Opvraagbaar PO
9	Register van verwerkingen	2.1 en 2.7	Privacy Nexus/tabel
10	Register Verwerkingsovereenkomsten	2.7	Privacy Nexus
11	DPIA-register	2.1	Privacy Nexus
	Overige instrumenten ter ondersteuning van verantwoording		
12	Format verwerkersovereenkomst	2.7	Opvraagbaar bij PO
13	Format toestemming	2.1	Opvraagbaar bij PO
14	Bewaartermijnenlijst	2.4	Opvraagbaar bij PO
15	Memo Quick Scan DPIA	2.1	Opvraagbaar PO
16	Rijksmodel GEB PIA 3.0 /Pre)pia model	2.1	Opvraagbaar Po
17	Selectielijst van de NVAO	2.4	website NA
18	Autorisatiematix	2.6	Opvraagbaar Po
19	Personeelsregeling	3.5	Intranet

Lijst van begrippen en afkortingen

AB	Algemeen Bestuur
AFAS	Personeels- en salarissysteem
AP	Autoriteit Persoonsgegevens
AVG	Algemene verordening gegevensbescherming
CDHO	Commissie Doelmatigheid Hoger Onderwijs
CMMBO	Commissie Doelmatigheid MBO
COR	Centrale Ondernemingsraad
DB	Dagelijks Bestuur
DPIA	Data Protection Impact Assessment
FG	Functionaris Gegevensbescherming
GEB	Gegevensbeschermingseffect-beoordeling
IB	Informatiebeveiliging
ITK	Instellingstoets Kwaliteitszorg
ISO	Information Security Officer
NA	Nationaal Archief
NL	Nederland
NVAO	Nederlands-Vlaamse Accreditatieorganisatie
OCW	Ministerie van Onderwijs, Cultuur en Wetenschap
OR	Ondernemingsraad
PO	Privacy Officer
TNO	Toets Nieuwe Opleiding
UAVG	Uitvoeringswet AVG
VL	Vlaanderen
WHW	Wet op het hoger onderwijs en wetenschappelijk onderzoek
Woo	Wet open overheid
WOR	Wet op de Ondernemingsraden
ZBO	Zelfstandig bestuursorgaan

Colofon

Privacy beleidskader
Februari 2025
Samenstelling: NVAO Nederland

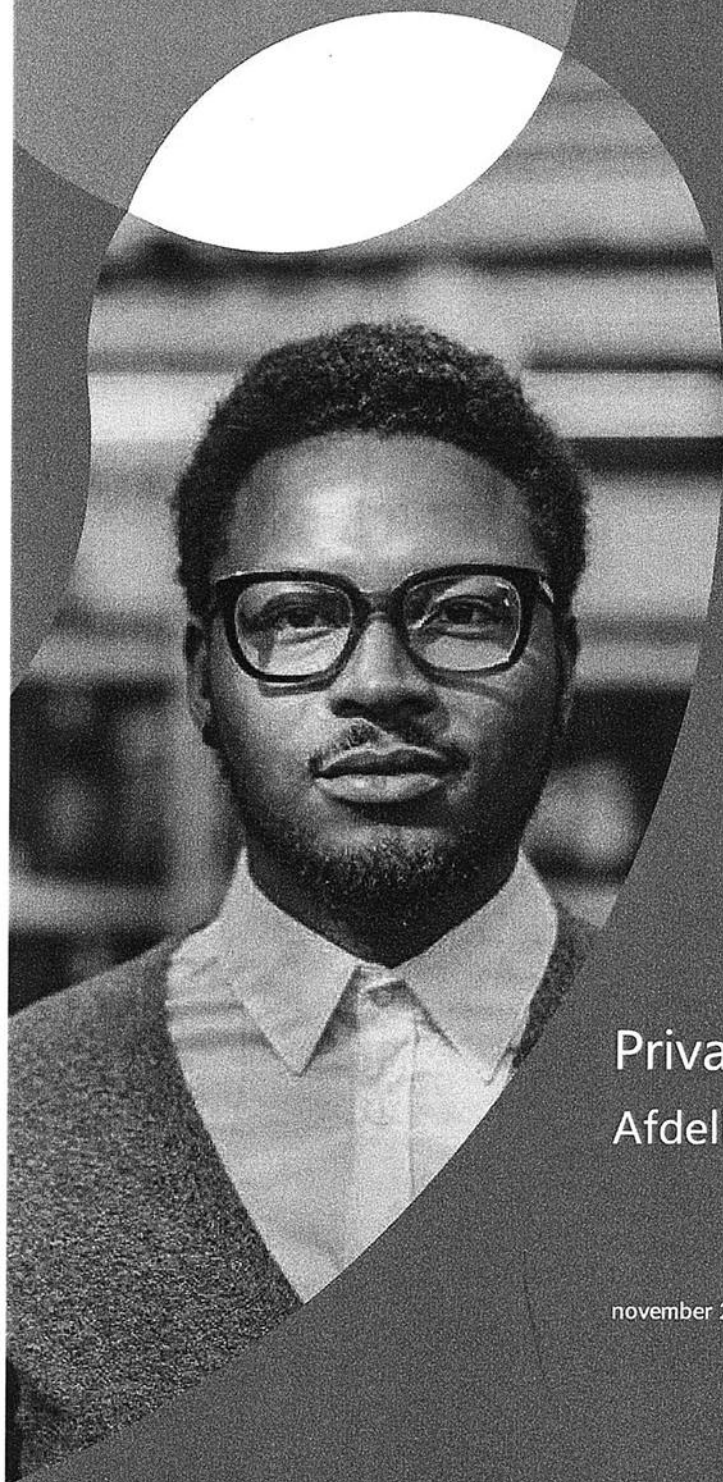


Nederlands-Vlaamse Accreditatieorganisatie
Accreditation Organisation of the Netherlands and Flanders

Parkstraat 83 · 2514 JG Den Haag
P.O. Box 85498 · 2508 CD The Hague
The Netherlands

T +31 (0)70 312 23 00
E info@nvao.net
www.nvao.net

2A



Privacy Beleidskader

Afdeling Nederland

november 2024

Privacy Beleidskader

Afdeling Nederland

CONCEPT
November 2024



Inleiding

De Nederlands-Vlaamse Accreditatieorganisatie (NVAO) is een kwaliteitszorgorganisatie die op deskundige en onafhankelijke wijze de kwaliteit van het hoger onderwijs in Nederland en Vlaanderen borgt en die de kwaliteitscultuur binnen de instellingen voor hoger onderwijs in Nederland en Vlaanderen bevordert. Zij accrediteert bestaande en nieuwe opleidingen en beoordeelt de kwaliteitszorg van instellingen in het hoger onderwijs. Daarmee is de NVAO bewaker van de kwaliteit van het hoger onderwijs. De besluiten van de NVAO leiden tot erkenning van diploma's en titels en waar van toepassing tot bekostiging van opleidingen. De NVAO baseert haar beoordeling op advies van erkende deskundigen.

De NVAO werd in 2003 opgericht bij Verdrag tussen Nederland en Vlaanderen. De taken van de NVAO zijn in wetgeving vastgelegd. De NVAO wil ertoe bijdragen dat de kwaliteit van het hoger onderwijs in Vlaanderen en Nederland erkend wordt als internationaal aan de maat, maatschappelijk relevant en het vertrouwen geniet van studenten, werkgevers en de samenleving. Binnen de opdracht die in het accreditatieverdrag tussen Nederland en Vlaanderen aan de NVAO is toegekend, wil zij de kwaliteit van het hoger onderwijs borgen, verbeteringen stimuleren en een kwaliteitscultuur bevorderen.

Om dit werk goed te kunnen doen is verwerking van persoonsgegevens van medewerkers en de contactpersonen van ketenpartners en burgers noodzakelijk. De privacy van contactpersonen en relaties is erg belangrijk voor de NVAO en we hechten dan ook veel belang aan een correcte verwerking en gebruik van persoonsgegevens. De bescherming van persoonsgegevens is immers een grondrecht. De NVAO is verantwoordelijk voor de aantoonbare zorgvuldige omgang met persoonsgegevens.

De NVAO is een zelfstandig bestuursorgaan en opgericht naar Nederlands publiekrecht met de zetel in Den Haag. De NVAO valt onder verantwoordelijkheid van het Comité van Ministers. De NVAO heeft een nauwe samenwerking met de CDHO en CMMBO.

Het privacy beleidskader van de NVAO werd voor het eerst vastgesteld op 15 maart 2021 en herzien in november 2024 vanwege de verbijzondering van de NVAO. De NVAO is juridisch gezien een ZBO naar Nederlands publiek recht, hetgeen betekent dat de organisatie, ongeacht of het de Afdelingen betreft of het bestuur, gehouden is aan de Nederlandse regelgeving voor ZBO's. Feitelijk is er sinds de verbijzondering evenwel sprake van een totale splitsing in de bedrijfsvoering binnen de Afdelingen en hebben de afzonderlijke afdelingen eigen voorzieningen op het gebied van ict, financiën en hr. Voor het primaire proces, de belangrijkste taak van de NVAO, namelijk accrediteren van opleidingen en instellingen, is al op basis van het Verdrag bepaald dat de afzonderlijke Afdelingen besluiten nemen op basis van de eigen regelgeving van Vlaanderen dan wel Nederland.

Dit privacy beleidskader richt zich daarmee tot iedereen die werkzaamheden verricht voor de NVAO **Afdeling Nederland** en medewerkers van het bureau van de CDHO en CMMBO. In dit privacy beleidskader wordt uitgelegd hoe de NVAO Afdeling Nederland aantoonbaar zorgvuldig omgaat met persoonsgegevens, wat daarbij de uitgangspunten zijn en wat de rol van de medewerker is bij de bescherming van persoonsgegevens¹.

¹ Voor een beknopte uitleg van begrippen (als persoonsgegevens en verwerking) zie bijlage 1.

Inhoud

- 1. Privacy beleidskader
 - 1.1 Doel
 - 1.2 Scope NVAO /CDHO/CMMBO
 - 1.3 Doelgroepen
 - 1.4 Wet- en regelgeving verwerking van persoonsgegevens
- 2. NVAO uitgangspunten voor omgang met persoonsgegevens
 - 2.1 Grondslag en doel
 - 2.2 Doelbinding
 - 2.3 Accuraat en actueel
 - 2.4 Bewaarbeperking
 - 2.5 Open en transparant
 - 2.6 Veilig en vertrouwelijk
 - 2.7 Verantwoordingsplicht
 - 2.8 Respect
- 3. Privacy governance
 - 3.1 Inleiding
 - 3.2 Privacy verantwoordelijkheden rollen en taken
 - 3.3 Privacy overlegstructuren
 - 3.4 Sturing, regie en toezicht
 - 3.5 Privacy trainingen en bewustwording
- 4. Slot
 - 4.1 Beheer
 - 4.2 Vaststellen
 - 4.3 Wijzigingen en evaluatie
- Bijlage 1 Begrippen
- Bijlage 2 Instrumenten voor verantwoording (documenten, websites etc.)

1 Privacy Beleidskader

Op het werk van het Nederlands Vlaamse Accreditatieorganisatie (NVAO) is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Daarnaast heeft de NVAO te maken met bijzondere wetgeving, waarin een grondslag voor verwerking van gegevens kan liggen. Denk hierbij bijvoorbeeld aan de gegevens die de NVAO nodig heeft van panelleden om hun deskundigheid voor deelname aan een panel te kunnen beoordelen. Voor de Afdeling Nederland is dit vastgelegd in de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW).

Het NVAO Privacy beleidskader geeft aan waar de Afdeling Nederland van de NVAO op het vlak van gegevensbescherming voor staat en wat de uitgangspunten voor de omgang met persoonsgegevens zijn. Met dit kader wil de Afdeling Nederland van de NVAO ervoor zorgen dat de privacybescherming in lijn is met de wettelijke vereisten en die aansluit of geïntegreerd wordt bij de bestaande processen en systemen van de NVAO. Bij alle uitgangspunten wordt steeds verwezen naar praktische ondersteunende instrumenten (checklists, stappenplan, procedures) van de NVAO dan wel (voor zover niet aanwezig) van OCW.

De uitleg van een aantal belangrijke begrippen uit de AVG is opgenomen in Bijlage 1: Begrippen.

1.1 Doel

Doel van dit beleidskader is een omgeving te creëren waarin elke medewerker van de Afdeling Nederland van de NVAO:

- zijn of haar verantwoordelijkheid en rechten kent als het gaat om privacy en het verwerken van persoonsgegevens,
- in staat is om het juiste beleid en de juiste procedures te volgen,
- contact kan opnemen met de juiste personen wanneer er vragen zijn.

1.2 Scope

Dit privacy beleidskader is bestemd voor de NVAO afdeling Nederland. Alle handelingen binnen de Afdeling Nederland van de NVAO met betrekking tot persoonsgegevens van medewerkers, contactpersonen, zoals medewerkers kwaliteitszorg, panelleden en secretarissen betrokken bij Nederlandse accreditatieprocedures, vallen binnen het bereik van dit beleidskader. Binnen de scope van dit beleid vallen ook de handelingen van Nederlandse leden van het DB en AB

CMMBO en CDHO

Deze organisaties hebben zelfstandige taken en verantwoordelijkheden. Er is een nauwe samenwerkingsrelatie, vastgelegd in een hostingovereenkomst, tussen de NVAO (Afdeling Nederland) en de CMMBO/CDHO. Niet alleen zitten de organisaties fysiek in het pand bij de NVAO, de ondersteuning van CDHO en CMMBO (namelijk de medewerkers van het Bureau van de commissies) is in dienst van de NVAO. Bovendien maken de commissies gezamenlijk gebruik van de afdeling Nederland van de NVAO voor wat betreft ICT, financiën en personeelszaken. Het privacybeleid van de NVAO omvat hiermee tevens de medewerkers werkzaam voor het bureau van CDHO en CMMBO. Het privacybeleid van de NVAO omvat *niet* de werkzaamheden van commissieleden CDHO en CMMBO, deze vallen onder verantwoordelijkheid van het Ministerie van Onderwijs, Cultuur en Wetenschap. Voor verwerkingen van de commissies (CDHO/CMMBO) waar de NVAO verwerker is, is een verwerkingsovereenkomst gesloten.

1.3 Doelgroepen

Dit beleidskader is van toepassing op alle medewerkers, tijdelijke werknemers en op alle andere personen die namens de NVAO Afdeling Nederland werkzaamheden verrichten.

1.4 Wet- en regelgeving verwerking van persoonsgegevens

1.4.1 Europese en Nederlandse wet- en regelgeving op het gebied van privacy

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Vanaf dat moment geldt dezelfde privacywetgeving in de hele Europese Unie. De AVG is rechtstreeks van toepassing. Daar waar de AVG ruimte laat voor nationale keuzes bij de uitvoering van de AVG, zijn deze ingevuld in de Uitvoeringswet AVG (UAVG)².

Naast genoemde wetgeving zijn er aanvullende documenten vanuit het Europees Comité³ voor gegevensbescherming waarmee (o.a.) verduidelijking wordt gegeven voor de toepassing van de AVG.

Daarnaast vormt ook de uitleg van de AVG (veelal vastgelegd in beleidsregels) door de Autoriteit Persoonsgegevens (AP) een belangrijke bron voor de naleving van de AVG. De AP gaat ervan uit dat verwerkingsverantwoordelijken als de NVAO (en dus ook specifiek afdeling Nederland) de beleidsregels toepassen en adviezen opvolgen, dan wel gemotiveerd afwijken (comply or explain).

Links naar genoemde wetgeving en belangrijke documenten verband houdend met dit beleidskader zijn te vinden in Bijlage 2: Instrumenten voor verantwoording.

1.4.2 Specifieke context NVAO

De AVG laat zich voor de NVAO het beste plaatsen vanuit het perspectief van de hoofdprocessen van de NVAO:

- Het primaire proces
- Het personeelsproces
- Het betalingsproces

Het primaire proces

De NVAO is een kwaliteitszorgorganisatie die primair op deskundige en onafhankelijke wijze de kwaliteit van het hoger onderwijs in Nederland en Vlaanderen borgt en die de kwaliteitscultuur binnen de hogere onderwijsinstellingen in Nederland en Vlaanderen bevordert. Zij accrediteert bestaande en nieuwe opleidingen en beoordeelt de kwaliteitszorg van instellingen in het hoger onderwijs.

Voor de Afdeling Nederland zijn deze taken van de NVAO gebaseerd op de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW, hoofdstuk 5): het accrediteren van bestaande opleidingen, het toetsen van nieuwe opleidingen in het hoger onderwijs, het samenstellen van een commissie van deskundigen en het instemmen met een voordracht voor een commissie van deskundigen, als ook rapporteren over de kwaliteit van opleidingen aan en het adviseren van de Minister in specifieke aangelegenheden zoals opgenomen in de WHW (artikel 5.2 WHW). Slotstuk van de accreditatieprocedure is de wettelijke plicht tot het publiceren van de uitkomsten ervan. Het is niet uitgesloten dat in de toekomst ook andere wet- en regelgeving als basis dient voor taken van de NVAO.

Het personeelsproces

Onder het personeelsproces worden alle verwerkingen geschaard die betrekking hebben op de persoonsgegevens van het eigen personeel van de NVAO en van personen die in opdracht van de NVAO werkzaamheden verrichten.

² Verder heeft de rijksoverheid een Handreiking naleving AVG geformuleerd. De NVAO overweegt nog hoe deze handreiking in te zetten.

³ European Data Protection Supervisor (EDPS), <https://edps.europa.eu/>

Het betalingsproces

Onder het betalingsproces behoren alle verwerkingen die gerelateerd zijn aan het overmaken van geld aan leveranciers, commissieleden, personeel en eventuele andere partijen.

2 NVAO uitgangspunten voor omgang met persoonsgegevens

In hoofdstuk 2 staan de uitgangspunten voor onze omgang met persoonsgegevens en wordt vervolgens toegelicht wat dat betekent voor een medewerker en welke documenten of websites beschikbaar zijn om die uitgangspunten in het dagelijks werk toe te passen. De uitgangspunten waar de medewerkers aan dienen te voldoen worden in bijlage 2 afzonderlijk benoemd.

Deze uitgangspunten reflecteren de visie van de NVAO ten opzichte van de verwerking van persoonsgegevens. De uitgangspunten voor gegevensbescherming zijn van toepassing op *alle* verwerkingsactiviteiten met betrekking tot persoonsgegevens binnen de NVAO. De uitgangspunten van de NVAO gelden onverminderd voor de Afdeling Nederland.

Dit betekent dat alle verwerkingen van persoonsgegevens moeten voldoen aan de volgende acht eisen:

- De NVAO verwerkt alleen persoonsgegevens als voor de verwerking een rechtmatige grondslag aanwezig is en een duidelijk omschreven en gerechtvaardigd doel.
- De NVAO beperkt de verwerking tot die categorieën persoonsgegevens die nodig zijn voor het beschreven doel.
- De NVAO verwerkt persoonsgegevens die accuraat en actueel zijn.
- De NVAO bewaart gegevens niet langer dan noodzakelijk voor het beschreven doel.
- De NVAO is, als dat mogelijk is, open en transparant over de verwerking van persoonsgegevens aan de betrokkene, de samenleving en ketenpartners.
- De NVAO zorgt dat persoonsgegevens die aan ons zijn toevertrouwd, veilig en vertrouwelijk worden verwerkt.
- De NVAO legt verantwoording af over de zorgvuldige verwerking van persoonsgegevens.
- De NVAO respecteert de rechten van de betrokkenen.

Hieronder volgt een nadere instructie per uitgangspunt.

2.1 Grondslag en doel

De NVAO (Afdeling Nederland) verwerkt alleen persoonsgegevens als voor de verwerking een rechtmatige grondslag aanwezig is en een duidelijk omschreven en gerechtvaardigd doel.

Instructies:

- Persoonsgegevens mogen alleen verwerkt worden als een van de rechtmatige grondslagen uit artikel 6 van de AVG aanwezig is. Te denken valt bijvoorbeeld aan: verwerking van persoonsgegevens middels toestemming, verwerking van persoonsgegevens of een wettelijke verplichting.
- Persoonsgegevens mogen eveneens alleen verwerkt worden indien de NVAO afdeling Nederland in het kader van zijn taken verwerkingen verricht, die “noodzakelijk voor de uitvoering van een wettelijke plicht” zijn en “noodzakelijk voor het uitoefenen van een publiekrechtelijke taak of uitoefenen van openbaar gezag”. De rechtsgrondslag van een dergelijke taak moet in de WHW zijn verankerd. Voor de NVAO is de uitvoering van haar publieke taak bij meerdere verwerkingen van persoonsgegevens in het primaire proces een grondslag voor de verwerking.
- De grondslag “noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerker of van de verwerkingsverantwoordelijke of van een derde” kan niet worden gebruikt als er sprake is van verwerkingen door overheidsinstanties in het kader van de uitoefening van hun taken. Dit kan wel in beeld komen bij een verwerking in het kader van de bedrijfsvoering (denk bijvoorbeeld aan cameratoezicht rond het gebouw). De Afdeling Nederland hanteert bij afwegingen voor de rechtsgrond gerechtvaardigd belang het normenkader gerechtvaardigd belang ([normuitleg_gerechtvaardigd_belang.pdf \(autoriteitpersoonsgegevens.nl\)](#))
- De ongelijke machtsverhouding tussen betrokkene en de overheid staat over het algemeen in de weg aan de eis dat betrokkene de toestemming vrijelijk moet verlenen. Voor de rechtsgrond toestemming in de verhouding werkgever en werknemer is binnen de Afdeling Nederland geborgd (formulier toestemming AVG bijlage) dat toestemming vrijwillig en ondubbelzinnig kan worden gegeven en ingetrokken en dat het niet geven van toestemming op geen enkele wijze verdere gevolgen heeft voor betrokkene.
- Een verwerking of de aanpassing hiervan moet steeds worden opgenomen in het Register van verwerkingen. Dit register geeft een beschrijving van verwerkingsactiviteiten. De verantwoordelijke (de NVAO Afdeling Nederland) moet dit op verzoek aan de AP kunnen laten zien. Neem bij een dergelijk verzoek van de AP contact op met de privacy officer die dit in afstemming met Directie en bestuursvoorzitter NI verzorgt. Het Register van verwerkingen bevat zelf geen persoonsgegevens.
- Het doel van elke verwerking is concreet en vastgelegd in het Register van verwerkingen. Als een bestand voor meer doelen wordt gebruikt dan wordt dat vermeld in de doelomschrijving. Doelen die duidelijk zijn omschreven maken het voor betrokkene inzichtelijk wat met de gegevens wordt gedaan. Bij verdere verwerking van persoonsgegevens voor een ander doel dan waarvoor de gegevens oorspronkelijk zijn verzameld, wordt altijd beoordeeld of dit nieuwe doel verenigbaar is met het oorspronkelijke doel.
- De NVAO is verplicht een Data Protection Impact Assessment, DPIA (ook wel genoemd Gegevensbeschermingseffect-beoordeling, GEB), uit te voeren bij de ontwikkeling van beleid en regelgeving waaruit verwerkingen van persoonsgegevens voortvloeien. De AP heeft een lijst van verwerkingen opgesteld waarvoor de DPIA verplicht is ⁴. De DPIA is bedoeld om de effecten van de beoogde gegevensverwerking(en) voor betrokkenen te inventariseren en te beoordelen. Op basis van de DPIA kunnen maatregelen worden

⁴ <https://www.autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667>

genomen om de risico's aan te pakken. Gebruik hiervoor het Rijksmodel GEB (PIA) of het model dat in Privacy Nexus is opgenomen. In Privacy Nexus wordt ook het DPIA-register (bij)gehouden. Bij een DPIA wordt verplicht advies aan de FG gevraagd.

- Vragen over het proces, de opzet en uitvoering van de DPIA kun je stellen aan de privacy officer en de Functionaris Gegevensbescherming. Raadpleeg eventueel het document DPIA Proces NVAO- NL of gebruik de Quick Scan PrePIA om te beoordelen of een DPIA nodig is.

2.2 Doelbinding

De NVAO Afdeling Nederland beperkt de verwerking tot die categorieën persoonsgegevens die nodig zijn voor het beschreven doel.

Instructies:

- Alleen de voor het vooraf en precies omschreven doel noodzakelijke gegevens mogen worden verzameld. Gegevens mogen vervolgens niet verder worden verwerkt als dit onverenigbaar is met dat doel. Persoonsgegevens die niet meer nodig zijn (moeten) worden verwijderd of waar mogelijk geanonimiseerd ⁵. Bij de ontwikkeling van nieuwe (of wijziging van bestaande) producten en diensten wordt met gegevensbescherming rekening gehouden.
- Verwerk niet meer gegevens dan die aantoonbaar noodzakelijk zijn voor het doel van de verwerking (*dataminimalisatie*). Bedenk waarom je gegevens voor die specifieke verwerking nodig hebt en of je daadwerkelijk alle gegevens nodig hebt.
- Nieuwe systemen worden geconfigureerd op een zodanige wijze dat alleen de voor het specifieke verwerkingsdoel noodzakelijke gegevens worden verwerkt. Privacy moet dus bij het ontwerp van een (nieuw) automatiseringssysteem als uitgangspunt worden genomen. (*privacy by design*).
- Ga bij het ontwikkelen van beleid, processen (en systemen) altijd uit van de meest privacybeschermende instellingen (*privacy by default*).
- Raadpleeg bij het ontwikkelen en uitwerken van beleid, processen en systemen de Handleiding Privacy by Design & by Default om meer zicht te krijgen op privacy vriendelijk ontwerp waarin de bescherming van persoonsgegevens is ingebouwd ⁶.

2.3 Accuraat en actueel

De NVAO Afdeling Nederland verwerkt persoonsgegevens die accuraat en actueel zijn. Dit betekent onder meer dat er sprake is van zorgvuldig beheer van gegevens (*betrouwbaarheid en integriteit*) en dat het voor betrokkenen mogelijk is om verzoeken met betrekking tot rectificatie van onjuiste persoonsgegevens in te dienen (*rechten van betrokkenen*). Om te borgen dat persoonsgegevens die we verwerken betrouwbaar en actueel zijn, worden in het primaire proces alle wijzigingen die worden doorgegeven door contactpersonen van instellingen, van evaluatiebureaus en door zelfstandigen, direct gewijzigd. Ook voor panelleden van TNO's en

⁵ De AVG is niet van toepassing op anonieme gegevens omdat deze gegevens niet terug te voeren zijn op een geïdentificeerde of identificeerbare natuurlijke persoon. Anonimisering is versleuteling die onomkeerbaar is, het niet meer mogelijk om deze later weer met personen in verband te brengen. Bij pseudonimisering kunnen anonieme gegevens met de juiste sleutel inzichtelijk gemaakt worden, waardoor herleiding naar natuurlijke personen weer mogelijk is. De AVG is wel van toepassing op gepseudonimiseerde gegevens.

⁶ https://www.cip-overheid.nl/media/1136/20170507-handleiding-privacy-by-design-v3_0.pdf

ITK's geldt dat wijzigingen in de gegevens die zij aan de NVAO hebben verstrekt doorgeven. De Afdeling Nederland van de NVAO verwerkt deze wijzigingen direct in het systeem voor het primaire proces verwerkt. Via een modaliteit voor externen in het personeels- en salarissysteem (AFAS) is een beveiligde functionaliteit opgenomen waarmee externen die werkzaam zijn in opdracht van de Afdeling Nederland van de NVAO zelf hun persoonsgegevens kunnen bijhouden. Ook voor medewerkers in dienst van NVAO-NI geldt dat zij al hun persoonsgegevens zelf kunnen bijhouden in het personeels- en salarissysteem (AFAS). Secretarissen die werkzaamheden verrichten ten behoeve van het accreditatieproces wordt jaarlijks gevraagd hun gegevens ten behoeve van registratie in het register van secretarissen te controleren en aan te geven of zij hun registratie willen verlengen.

Instructies:

- Zorg dat de juistheid en actualiteit van de persoonsgegevens zoveel mogelijk gewaarborgd is door periodieke controles en/of controle op bestaande gegevens of input, bijvoorbeeld wanneer panelleden opnieuw zitting nemen in een panel.
- Zorg dat het mogelijk is om gegevens aan te passen daar waar zij onjuist, onvolledig of verouderd zijn.
- Raadpleeg desgewenst Protocol Rechten Betrokkenen.

2.4 Bewaarbeperking

De NVAO Afdeling Nederland bewaart gegevens niet langer dan noodzakelijk voor het beschreven doel of zolang als bepaald door een specifieke wet.

- Voor de accreditatieprocedures zijn de bewaartermijnen vastgelegd in de Selectielijst NVAO. Deze Selectielijst is geldig tot 2032. Deze lijst volgt voor personele aangelegenheden waar van toepassing wettelijke termijnen,
- Nadat een bewaartermijn is verstreken, geldt voor de accreditatiedossiers dat een steekproef van de dossiers zal worden overgedragen aan het Nationaal Archief. De dossiers die niet overgaan naar het Nationaal Archief zullen na ommekomst van de bewaartermijn worden vernietigd, eea overeenkomstig de selectielijst NVAO.⁷

In aanvulling op de Selectielijst en ter overbrugging naar een in de toekomst nieuw vorm te geven Selectielijst hanteert de NVAO voor zaken die niet geregeld zijn in de Selectielijst een bewaartermijnenlijst. Uitgangspunt voor deze lijst is dat voor procedures gerelateerd aan het accreditatieproces aansluiting wordt gezocht bij verwante procedures. Voor overige procedures die geen onderdeel uitmaken van de Selectielijst, waaronder verzoeken op grond van de AVG of Wet open overheid (Woo) is een bewaartermijn in de bewaartermijnenlijst opgenomen, waarbij eveneens zoveel mogelijk wordt aangesloten op de termijnen van de Selectielijst. Ter illustratie: voor de nieuwe taak Kwaliteitsafspraken is aangesloten bij het ITK-proces en geldt een bewaartermijn van 18 jaar, waarna steekproefsgewijze overdracht aan het NA zal plaatsvinden, de overige dossiers worden vernietigd. Waar dit vanuit het oogpunt van de AVG minder voor de hand ligt (principe: niet langer bewaren dan strikt noodzakelijk, indien geen doelbinding meer, dan niet langer bewaren) is een op de situatie aangepaste bewaartermijn opgenomen.

Instructies:

- Persoonsgegevens kunnen meerdere doelen dienen. Houd hiermee rekening bij het opstellen van de bewaartermijnen.
- Bewaar persoonsgegevens niet langer dan noodzakelijk voor de doelen van de verwerking.
- Stel bewaartermijnen vast. Wis gegevens wanneer deze niet langer noodzakelijk zijn voor het verwerkingsdoel.
- Raadpleeg desgewenst de Selectielijst van de NVAO.

⁷ Zie voetnoot 7

2.5 Open en transparant

De NVAO Afdeling Nederland is, als dat mogelijk is, open en transparant over de verwerking van persoonsgegevens aan de betrokkene, en de ketenpartners. Een betrokkene dient te weten wat er met zijn persoonsgegevens gebeurt. De NVAO Afdeling Nederland biedt informatie over de verwerking en de omgang met de gegevens en over de rechten van betrokkene toegankelijk en begrijpelijk aan. Dit gebeurt in een interne en een externe privacyverklaring(en) en een cookieverklaring.

Instructies:

- De NVAO verstrekt vereiste informatie voor medewerkers (incl. de medewerkers van CDHO en CMMBO) en mensen die in opdracht van de NVAO diensten verrichten (via de interne Privacyverklaring NVAO afdeling Nederland op intranet of Sharepoint. Zo nodig wordt een extra toelichting gegeven over de nieuwe of bestaande verwerking.
- De privacyverklaringen van de NVAO (intern en extern) worden periodiek door de Afdeling Nederland op actualiteit gecontroleerd.
- Raadpleeg desgewenst de personeelsregeling.

2.6 Veilig en vertrouwelijk

De NVAO afdeling Nederland zorgt dat persoonsgegevens die aan ons zijn toevertrouwd, veilig en vertrouwelijk worden verwerkt.

Instructies:

- De NVAO afdeling Nederland is verplicht (op basis van wet- en regelgeving) om passende technische en organisatorische maatregelen te treffen om persoonsgegevens een passend beschermingsniveau te bieden tegen ongeautoriseerde verwerkingen. De NVAO Afdeling Nederland heeft hiertoe een beleidskader voor informatiebeveiliging.
- De NVAO afdeling Nederland verstrekt alleen toegang tot persoonsgegevens aan die mensen die toegang tot de gegevens nodig hebben en die toestemming hebben om gegevens verder te verwerken.
- Datalekken moeten zoveel mogelijk worden voorkomen. Een datalek is een inbreuk op de beveiliging van de persoonsgegevens die leidt tot vernietiging, verlies, wijziging of ongeoorloofde verstrekking of toegang tot gegevens.
- Een datalek dat een risico voor de rechten van betrokkene inhoudt moet binnen 72 uur aan de Autoriteit Persoonsgegevens (AP) worden gemeld en soms ook aan betrokkene. Hiervoor is het Protocol beveiligingsincidenten en datalekken NVAO-Afdeling NI opgesteld. Raadpleeg bij een (vermeend) datalek de privacy officer. Voor een eerste beoordeling van het incident/datalek gebruikt de Afdeling Nederland een formulier quick scan
- Via de e-mail worden veel bestanden uitgewisseld en dus ook vaak persoonsgegevens. Het is belangrijk om een passend beschermingsniveau toe te passen bij het versturen van dergelijke gegevens. Bij het versturen van bestanden met persoonsgegevens is het passend om deze gegevens versleuteld te versturen naar de ontvanger. Op die manier wordt het risico verkleind dat er per ongeluk bestanden naar de verkeerde ontvanger worden gestuurd.

- Ter voorkoming van een datalek veroorzaakt door de optie suggesties in outlook is het advies aan de medewerkers van Afdeling Nederland deze optie uit te schakelen en zelf bewust een keuze te maken bij de selectie van een geadresseerde.
- De NVAO afdeling Nederland en in het bijzonder het privacy office van Afdeling Nederland houdt een register bij van datalekken en beveiligingsincidenten die afdeling Nederland betreffen.
- Raadpleeg eventueel het Informatie Beveiligingsbeleid NVAO-Afdeling NI

2.7 Verantwoordingsplicht

De NVAO afdeling Nederland legt verantwoording af over de zorgvuldige verwerking van persoonsgegevens.

Instructies:

- De NVAO afdeling Nederland neemt passende maatregelen om de bescherming van persoonsgegevens te waarborgen. Aan de hand van documentatie kan de NVAO afdeling Nederland aantonen dat de privacyregels worden nageleefd. Evaluatie, en monitoring van de maatregelen maakt ook onderdeel uit van de verantwoording. Deze verantwoordingsplicht (*accountability*) staat centraal in het wettelijk privacykader.
- Het privacy office van de NVAO afdeling Nederland beheert een Register van verwerkingen. In dat register staat informatie over de gegevens die worden verwerkt. De persoonsgegevens zelf staan niet in het register, wel welke categorieën persoonsgegevens er worden verwerkt.
- Wijzigingen in verwerkingen moeten door medewerkers en/of directieleden aan het privacy office worden doorgegeven.
- De directieleden van de afdeling Nederland hebben een zelfstandige verantwoordelijkheid om bij nieuwe verwerkingen (activiteiten/andere ICT systemen) de privacy officer van Afdeling Nederland en zo nodig de FG op de hoogte te stellen.
- De NVAO Afdeling Nederland vergewist zich ervan dat derde partijen behoorlijk en zorgvuldig met persoonsgegevens omgaan. Dit hoeft niet noodzakelijkerwijs te gaan over partijen waarmee een verwerkersovereenkomst mee afgesloten dient te worden. Denk hierbij aan de Arbodienst die een eigen verwerkingsverantwoordelijkheid heeft. Waar nodig wordt een verwerkingsovereenkomst gesloten; deze wordt opgenomen in het Register Verwerkingsovereenkomsten (Privacy Nexus).

2.8 Respect

De NVAO (afdeling Nederland) respecteert de rechten van de betrokkenen.

Instructies:

- De NVAO afdeling Nederland richt systemen, processen en de interne organisatie zodanig in dat op de juiste manier gehoor wordt gegeven aan verzoeken van betrokkenen omtrent persoonsgegevens.
- De NVAO afdeling Nederland hanteert een Protocol Rechten Betrokkenen, waarin de (belangrijkste) rechten van betrokkenen zijn/worden geformuleerd, zoals inzage, rectificatie, wissen, overdracht en beperking van verwerking. Ook wordt in dit protocol vermeld hoe een bepaald verzoek wordt behandeld en waar een betrokkene rekening

mee kan houden. Dit protocol heeft interne werking en is bedoeld om handvaten te bieden voor het Privacy Office.

- De NVAO afdeling Nederland kan gebruik maken van een model voor de beantwoording van inzageverzoeken of van andere modellen om aan verzoeken te voldoen.

In de diverse privacyverklaringen worden o.a. de rechten van betrokkenen ten aanzien van hun persoonsgegevens omschreven. In de diverse privacyverklaringen wordt omschreven voor wie de betreffende privacyverklaring geldt,

Alle betrokkenen (intern en extern) kunnen bij de Autoriteit Persoonsgegevens (AP) een klacht indienen over de manier waarop de NVAO met hun gegevens omgaat. De AP is verplicht deze klachten te behandelen.

3 Privacy governance

3.1 Inleiding

Doel van dit hoofdstuk over de privacy governance is inzicht te geven in de verantwoordelijkheden op het gebied van de privacybescherming binnen de NVAO afdeling Nederland. De governancestructuur helpt de NVAO afdeling Nederland om zorgvuldig met persoonsgegevens om te gaan en verantwoording af te kunnen leggen over genomen beslissingen. Een robuuste beheersorganisatie is van belang voor de implementatie en handhaving van de principes en doelstellingen uit het privacybeleid van de afdeling Nederland

Omgevingsveld

De NVAO is een zelfstandig bestuursorgaan en valt onder de politieke verantwoordelijkheid van het *Comité van Ministers*. Hoewel de NVAO een zelfstandig bestuursorgaan is, blijft het Comité van Ministers politiek verantwoordelijk voor compliance met wet- en regelgeving en dus ook de AVG.

De *Autoriteit Persoonsgegevens* (AP) is de toezichthoudende autoriteit met betrekking tot het voldoen aan de vereisten van de AVG. Wanneer betrokkenen klachten hebben over hoe de NVAO omgaat met persoonsgegevens, kunnen zij terecht bij de AP. Zo ook als betrokkenen klachten hebben over hoe Afdeling Nederland van de NVAO omgaat met persoonsgegevens. De *Nationale Ombudsman* kan eventueel ook nog een bemiddelende rol spelen tussen de NVAO en personen waarvan de NVAO gegevens verwerkt.

3.2 Privacy verantwoordelijkheden rollen en taken

Wat is de rol van de FG (Functionaris Gegevensbescherming)? ⁸

De functie van de FG (Functionaris Gegevensbescherming) binnen de NVAO afdeling Nederland is vooral gericht op het waarborgen van de privacy en bescherming van persoonsgegevens in overeenstemming met de Algemene Verordening Gegevensbescherming (AVG) en andere relevante wet- en regelgeving.

Adviesfunctie: De FG adviseert de organisatie over de naleving van de AVG. Dit omvat het geven van advies over hoe NVAO afdeling Nederland persoonsgegevens kan verwerken in overeenstemming met de wet.

Toezicht houden: De FG houdt toezicht op de naleving van de AVG binnen de organisatie. Dit kan inhouden dat de FG audits uitvoert en processen evalueert om ervoor te zorgen dat data effectief en veilig worden beheerd.

Gegevensbeschermingseffectbeoordelingen (DPIA): In bepaalde situaties, wanneer er een hoog risico is voor de rechten en vrijheden van betrokkenen, is de FG betrokken bij het uitvoeren van een gegevensbeschermingseffectbeoordeling.

Informerende en trainende: De FG heeft de taak om medewerkers van de NVAO afdeling Nederland

⁸ <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/algemene-informatie-avg/functionaris-gegevensbescherming-fg>

te informeren en op te leiden over privacy en gegevensbescherming.

Contactpunt voor toezichthouders: De FG fungeert als het contactpunt voor toezichthouders, zoals de Autoriteit Persoonsgegevens, en als aanspreekpunt voor betrokkenen wiens persoonsgegevens worden verwerkt.

Rapportage en documentatie: De FG is verantwoordelijk voor het bijhouden van documentatie met betrekking tot verwerking van persoonsgegevens en eventuele datalekken.

Relevante wetsartikelen

Aanwijzing van de FG

Artikel 37: Dit artikel beschrijft wanneer een FG moet worden aangesteld (bijvoorbeeld, als de organisatie een publieke autoriteit is of als de kernactiviteiten van de organisatie beheer van gegevens vereisen).

Taken van de FG

Artikel 39: Dit artikel beschrijft de specifieke taken van de FG, zoals het informeren en adviseren van de organisatie, toezicht houden op de naleving van de AVG, en samenwerken met de toezichthoudende autoriteit.

Onafhankelijkheid van de FG

Artikel 38: Dit artikel stelt dat de FG onafhankelijk moet kunnen optreden en niet moet worden ontslagen of gestraft voor de uitvoering van zijn taken.

De rol van de FG binnen de NVAO is essentieel voor het waarborgen van een correcte omgang met persoonsgegevens en het naleven van de AVG en andere privacywetgeving. De rol van de privacy office binnen de NVAO afdeling Nederland is vooral gericht op het waarborgen van de privacy van gegevens die de organisatie verwerkt. De NVAO afdeling Nederland is verantwoordelijk voor de accreditatie van hogeronderwijsinstellingen in Nederland en Vlaanderen, en moet daarbij voldoen aan de geldende privacywetgeving, zoals de Algemene Verordening Gegevensbescherming (AVG).

Wat is de rol van de PO (Privacy office)?

De rol van de privacy office binnen de NVAO afdeling Nederland is van cruciaal belang in het waarborgen van de privacy en de bescherming van persoonsgegevens.

Beleid en advies: Het ontwikkelen van beleid en richtlijnen omtrent privacy, en het adviseren van de organisatie over privacy-gerelateerde onderwerpen.

Gegevensbescherming: Toezien op de naleving van privacywetgeving en ervoor zorgen dat persoonsgegevens veilig worden verwerkt.

Training en bewustwording: Trainingen en workshops organiseren voor medewerkers over privacy en gegevensbescherming, om bewustwording te creëren en best practices te bevorderen.

Risicoanalyse: Het uitvoeren van risicoanalyses met betrekking tot de verwerking van persoonsgegevens en het implementeren van maatregelen om risico's te verkleinen.

Verwerkingsovereenkomsten: Beheren van contracten en overeenkomsten met derde partijen die persoonsgegevens verwerken in opdracht van de NVAO afdeling Nederland.

Klachten en incidenten: Behandelen van klachten en meldingen omtrent privacy-inbreuken of datalekken, en zorgen voor een juiste opvolging en rapportage.

Door deze rol te vervullen, draagt de privacy office bij aan een verantwoord en transparant gebruik van persoonsgegevens binnen de NVAO afdeling Nederland en helpt daarmee het vertrouwen van zowel instellingen als individuele personen in de organisatie te waarborgen.

Naast een privacy officer heeft de NVAO afdeling Nederland een CISO. De privacy officer en de CISO adviseren en ondersteunen de directie, en de medewerkers bij privacy aspecten. Door tussenkomst van de directie en op verzoek kan ook advies en ondersteuning worden gegeven aan de bestuursvoorzitter NI. Ook bepaalde beleidstaken en het organiseren van interne risicoanalyses behoren tot hun takenpakket. Primair is de privacy officer -NI het aanspreekpunt voor de uitleg van de AVG binnen de Afdeling NI van de NVAO en bij de implementatie en uitvoering van de AVG.

De NVAO afdeling Nederland heeft een privacy officer die de volgende taken verricht:

- beheert het privacybeleid en kan op verzoek van de directie, het bestuursorgaan uit eigen beweging een voorstel tot aanpassing van het beleid doen;
- zorgt voor de dagelijkse afhandeling van privacy aangelegenheden voor de NVAO;
- beheert het register van verwerkingsactiviteiten;
- stelt de jaarplanning op;
- fungeert als vraagbaak voor de directieleden van de afdeling Nederland ten aanzien van het verzamelen, registreren en leveren van persoonsgegevens. Hij raadpleegt indien nodig de Functionaris Gegevensbescherming of externe adviseurs over complexere verwerkingen en relaties met verwerkers.
- adviseert de directieleden van de afdeling Nederland bij de analyse van mogelijke risico's die samenhangen met de verwerking van persoonsgegevens.

De NVAO afdeling Nederland heeft een privacy office⁹ dat de volgende taken verricht: ondersteunt de NVAO afdeling Nederland in het naleven van de eisen uit dit privacybeleid en de privacywetgeving.

Wat is de rol van de CISO (Chief Information Security Officer)?

De rol van de Chief Information Security Officer (CISO) binnen de NVAO afdeling Nederland is

⁹ Juridische Zaken fungeert als Privacy Office op het moment van inwerkingtreding van dit beleid; eventuele wijziging wordt gecommuniceerd.

cruciaal voor het waarborgen van de informatiebeveiliging binnen de organisatie. Het vraagt om een zorgvuldige afstemming met de experts van juridische zaken, ICT, beveiliging, communicatie, de privacy en de FG. Hoewel de specifieke taken en verantwoordelijkheden kunnen variëren, omvatten de belangrijkste taken van een CISO doorgaans het volgende:

De CISO heeft onder meer als taak:

Beleid en Strategie: Ontwikkelen en implementeren van informatiebeveiligingsbeleid en -strategieën die aansluiten bij de organisatie's doelstellingen en wettelijke vereisten. Hierbij valt ook te denken aan het Opstellen en actualiseren informatiebeveiligingsbeleid en de daaruit voortvloeiende plannen;

Risicobeheer: Identificeren, analyseren en beheren van risico's met betrekking tot de informatiebeveiliging. Dit omvat het uitvoeren van risicoanalyses en het aanbevelen van passende maatregelen om deze risico's te minimaliseren.

Bewustwording en Training: Het bevorderen van bewustwording rondom informatiebeveiliging binnen de organisatie, waaronder het organiseren van trainingen en informatiesessies voor personeel.

Compliance: Zorgen voor naleving van relevante wet- en regelgeving, normen en richtlijnen op het gebied van informatiebeveiliging.

Incidentbeheer: Beheren van beveiligingsincidenten, inclusief het opstellen van procedures voor het melden en afhandelen van incidenten.

Toegangsbeheer: Toezicht houden op de toegangsrechten tot informatie en systemen, en ervoor zorgen dat deze op een veilige manier worden beheerd.

Samenwerking: Samenwerken met andere afdelingen en stakeholders om een geïntegreerde benadering van informatiebeveiliging te waarborgen.

Rapportage: Monitoren van de effectiviteit van de informatiebeveiligingsmaatregelen en rapporteren aan het management over de status en eventuele verbeterpunten.

Aanvullend

De CISO ondersteunt de NVAO afdeling Nederland en is in eerste instantie verantwoordelijk voor de informatieprivacy. De CISO ondersteunt en adviseert de NVAO afdeling Nederland bij privacyvraagstukken. De CISO helpt onder meer door het geven van (zo mogelijk) advies op maat, het opbouwen van de noodzakelijke kennis over privacy wet- en regelgeving, het toepassen hiervan en het (mede-)ontwikkelen van producten zoals informatiebeleid en privacy convenanten. Verder is de CISO verantwoordelijk voor monitoring en borgen van de eisen en architectuur voor informatiebeveiliging en het consequent toepassen van Security-by-Design en Privacy-by-Design.

Wat is de rol van de ISO?

Een ISO Internationale Organisatie voor Standaardisatie (ISO) speelt een belangrijke rol voor de NVAO afdeling Nederland door het vaststellen van standaarden en richtlijnen die de kwaliteit, veiligheid en efficiëntie van de processen en producten

van de ZBO kunnen verbeteren. Hier zijn enkele specifieke manieren waarop ISO-standaarden invloed kunnen hebben op de NVAO afdeling Nederland.

Enkele manieren waarop een ISO standaard invloed kan hebben op de NVAO afdeling Nederland zijn onder andere:

- Kwaliteitsmanagement
- Risicobeheer
- Informatiebeveiliging
- Milieu
- Gezondheid en veiligheid

Door deze standaarden te implementeren, kan de NVAO afdeling Nederland zijn operationele processen optimaliseren, de transparantie en verantwoordelijkheidsgevoel vergroten, en de tevredenheid van belanghebbenden verbeteren. Het kan ook helpen bij het voldoen aan wettelijke regelgevende vereisten.

Wat is de rol van de OR¹⁰ bij privacyvraagstukken?

De ondernemingsraad van de Afdeling Nederland (OR-NL) vertegenwoordigt het personeel van de NVAO Afdeling Nederland en beschermt hun belangen. De OR-NL heeft daarvoor verschillende rechten en bevoegdheden, zoals het recht op informatie, het adviesrecht, het instemmingsrecht en het initiatiefrecht. Met name het adviesrecht, instemmingsrecht en het initiatiefrecht spelen een rol bij de uitvoering van de AVG. Artikel 27 WOR

Het kan zijn dat er nieuwe technische maatregelen worden getroffen om te voldoen aan de AVG. Denk bijvoorbeeld aan technische maatregelen om persoonsgegevens te beveiligen of om ervoor te zorgen dat alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor het verwerkingsdoel.

Op grond van de Wet op de Ondernemingsraden (WOR) dient een besluit tot het invoeren of wijzigen van een technologische voorziening ter advies aan de ondernemingsraad te worden voorgelegd. Dus als de NVAO-NL wil over gaan tot de aanschaf van nieuwe ICT ter beveiliging van de persoonsgegevens, dan hebben de OR-NL en de COR adviesrecht.

Een besluit tot vaststelling, wijziging of intrekking van een regeling over het verwerken van, alsmede de bescherming van de bij de NVAO werkzame personen is instemming plichtig. Het moet dus gaan om een regeling die tot doel heeft persoonsgegevens te verzamelen, bewaren, gebruiken, verstrekken of beveiligen. Dit geldt onder meer voor de vaststelling van dit privacybeleid en voor het melden van een datalek waarbij persoonsgegevens zijn betrokken.

De ondernemingsraad kan tenslotte gebruikmaken van haar initiatiefrecht om voorstellen te doen voor (een aanpassing van) het privacybeleid.

Wat is de rol van de HR

Daarnaast heeft HR een rol als het gaat om de zorgvuldige omgang met persoonsgegevens. HR is het eerste aanspreekpunt bij personeelsgerelateerde vragen van medewerkers over de AVG.

3.3 Privacy overlegstructuren

Wekelijks vindt overleg plaats tussen directie en privacy-office over de voortgang van AVG-onderwerpen. Ook is het onderwerp van gesprek in periodiek overleg met de WOO-coördinator van Afdeling Nederland en directie. Vanuit de directie wordt deelgenomen aan kwartaaloverleg met de FG. De directie informeert bestuurder NL over actuele onderwerpen en de voortgang hierop. Jaarlijks vindt in het bestuur bespreking van de jaarrapportage van de FG plaats, Acties

¹⁰ <https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-uitkering/ondernemingsraad>

die uit de rapportage voortkomen worden belegd binnen de Afdeling waar de betreffende actiebetrekking op heeft.

De NVAO afdeling NL doet actief mee aan overleggen van KleinLef organisaties (AVG-werkgroep, RBB) op het gebied van privacy om de kennis omtrent privacy te delen en elkaar te helpen om beleid omtrent privacy te ontwikkelen.

3.4 Sturing, regie en toezicht

Periodiek voert de NVAO afdeling Nederland met behulp van de tool in Privacy-Nexus self-assessments uit, waaruit blijkt wat de stand van zaken is met betrekking tot privacy.

De FG ziet toe op de naleving van de relevante wetgeving, het privacybeleid en de inrichting van de interne privacy organisatie.

Interne toezichtsorganen: FG en OR

Tenslotte kent de NVAO afdeling Nederland een Functionaris Gegevensbescherming (FG) en de Ondernemingsraad van de Afdeling Nederland (OR-NL). Zij zijn vanwege hun specifieke rollen en wettelijke taken bij aspecten van de privacy van de NVAO afdeling Nederland betrokken.

Externe toezichthouders, zoals de Autoriteit Persoonsgegevens (AP) en al dan niet ingehuurde auditors kunnen de inregeling en uitvoering van de AVG controleren. Het is de eigen verantwoordelijkheid van de NVAO om intern toezicht te houden op de waarborging van privacybescherming, los van eventuele externe audits en evaluaties.

3.5 Privacy trainingen en bewustwording

Alle medewerkers krijgen bij hun aanstelling een korte introductie AVG van de PO/FG. De tekst van de eed/beloofte is in de Personeelsregeling opgenomen; hierin ligt de geheimhouding t.a.v. AVG besloten.

Daarnaast vinden reguliere bewustwordingsacties plaats, door minimaal twee keer per jaar aandacht voor een privacy onderwerp vanuit het privacy office voor Afdeling Nederland. Het privacy-office volgt regelmatig trainingen op het gebied van de AVG en houdt de voortgang hierop bij in de jaarplanning ten behoeve van directie en FG.

4 Slot

Met dit privacybeleid brengt de NVAO afdeling Nederland in kaart welke maatregelen er zijn genomen om de persoonsgegevens van medewerkers en externen, waaronder o.a. panelleden, secretarissen en studenten, te beschermen. Daarnaast geeft het beleid inzicht in de wijze waarop de verantwoordelijkheden op grond van de AVG zijn belegd binnen de Afdeling Nederland van de NVAO. Ook is per uitgangspunt vastgelegd welke instructies er zijn en welke documenten geraadpleegd kunnen worden. Hiermee wordt voldaan aan belangrijke verplichtingen op grond van de AVG, zoals het inrichten en bijhouden van een Register van verwerkingen, de wijze waarop omgegaan wordt met datalekken, het houden van een DPIA, het opstellen van een interne en externe privacyverklaring en de wijze waarop rechten van betrokkenen zijn georganiseerd.

4.1 Beheer

Het privacy office van de NVAO afdeling Nederland is verantwoordelijk voor het beheer van dit privacy beleidskader.

De instrumenten en dit beleidskader zijn levende documenten die periodiek (moeten) worden geactualiseerd. Algemene vragen over dit beleid of suggesties tot wijziging of toevoeging aan het beleid, kunnen worden gericht aan het privacy office van de NVAO (privacy@nvao.net).

4.2 Vaststelling

Dit privacybeleid is voor het eerst vastgesteld op 15 maart 2021 door het Algemeen Bestuur van de NVAO en is in verband met de verbijzondering opnieuw voorgelegd aan de directie en de ORR-NL, waarna het – na advies FG?- is vastgesteld door wie? Directie en bestuurder NL?.

4.3 Wijzigingen en evaluatie

Privacybeleid is dynamisch beleid. Nieuwe ontwikkelingen volgen elkaar op en ook de organisatie zelf zal steeds in ontwikkeling zijn. Dit betekent dat het privacybeleid ook met regelmaat bijgesteld zal moeten worden. Dit beleid wordt periodiek herzien en bijgewerkt. De volgende tabel toont de (concept)versie geschiedenis van dit privacy beleid. Evaluatie vindt in beginsel ieder jaar plaats, tenzij anders bepaald.

Datum	Opmerkingen	Versie
16-10-2019	1 ^{ste} concept beleidsdocument	0.1
27-07-2020	Concept tbv FG	0.2
2-11-2020	Concept tbv Luut	0.3
28-1-2021	Concept tbv DB	0.4
16-2-2021	Goedkeuring cpt door DB	16-2-2021
15-3-2021	Goedkeuring AB en mandatering DB en ondermandaat PO	15-3-2021
15-4-2021	Aanvulling data en technische aanpassingen (IM vervangen door CISO/privacyverklaringen hernoemd, cookieverklaring toegevoegd en protocol rechten betrokkenen hernoemd)	15-4-2021
22-4-2021	Naast CISO de IM gezet (RASCI 1 kolom voor gezamenlijke taken)	22-4-2021
7-6-2021	Regeling Rechten Betrokkenen naam gewijzigd; interne werking	7-6-2021
10-6-2021	Naam oud-voorzitter verwijderd	10-6-2021

11-9-2023		Eerste afsplitsing beleid naar afdeling Nederland, in concept	Maart 2024

Bijlage 1: Begrippen

Wat zijn persoonsgegevens?

Niet alle data of gegevens zijn per definitie persoonsgegevens. Persoonsgegevens betreft alle informatie met betrekking tot een geïdentificeerde of identificeerbare natuurlijke persoon (de "betrokkene").

De betrokkene hoeft geen direct geïdentificeerd individu te zijn, maar zodra een individu uit een groep kan worden onderscheiden, zijn de gegevens persoonsgegevens. Het is dus niet altijd nodig om de naam te weten van de persoon in kwestie om te spreken van persoonsgegevens.

Alle gegevens die betrekking hebben op een geïdentificeerde of identificeerbare persoon moeten als persoonsgegevens worden beschouwd. Enkel transactiegegevens zijn bijvoorbeeld op zichzelf geen direct identificeerbare gegevens, maar worden persoonsgegevens wanneer deze verband houden met een geïdentificeerde of identificeerbare persoon, bijvoorbeeld omdat deze is gekoppeld aan een naam, een e-mailadres of een telefoonnummer.

De AVG heeft een speciaal regime voor bijzondere categorieën persoonsgegevens. Dit betreffen persoonsgegevens waaruit de raciale of etnische afkomst, politieke opvattingen, religieuze of filosofische overtuigingen blijken, lidmaatschap van een vakvereniging, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie, gezondheids- of medische gegevens, gegevens over iemands seksleven of seksuele geaardheid. Strafrechtelijke persoonsgegevens zijn persoonsgegevens die te maken hebben met strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen. Hieronder vallen zowel veroordelingen als mogelijk gegronde verdenkingen. Dit wil zeggen dat er concrete aanwijzingen zijn dat iemand een strafbaar feit heeft gepleegd. Een voorbeeld hiervan is een opgestelde zwarte lijst van frauderende klanten bij een financiële instelling. Onder de AVG gelden speciale regels voor het verwerken van strafrechtelijke gegevens.

De verwerking, het verzamelen of gebruiken, van gevoelige persoonsgegevens, is verboden, tenzij een uitzondering op het algemene verbod van toepassing is. Het verzamelen en gebruiken van dergelijke gegevens zal daarom zoveel mogelijk worden vermeden. Vermijd ook het verzamelen en gebruik van gegevens van gevoelige groepen, zoals kinderen / minderjarigen, gehandicapten en ouderen, tenzij hiervoor duidelijk toestemming is gegeven door de bevoegde persoon.

Hieronder volgen voorbeelden van gegevens die over het algemeen als persoonsgegevens worden beschouwd:

Voornaam en / of initialen en achternaam	Financiële gegevens
E-mailadres	Betaling of transactiegegevens
Telefoonnummer	Rijbewijs
Foto	Strafrecht ketennummer
Geboortedatum / geboorteplaats	Identificatienummer werknemer

IP-adres	Werknemers informatie
Uitkomsten functioneringsgesprekken	Medische informatie
Burgerservicenummer	Biometrische gegevens
Unique Device Identifiers	MAC-adressen

Wat is een betrokkene?

De betrokkene is de persoon van wie persoonsgegevens worden verwerkt.

Wat is een verwerking?

Het 'verwerken van persoonsgegevens' of een 'verwerking van persoonsgegevens' betreft alle handelingen die men met persoonsgegevens kan verrichten. Denk hierbij aan het verzamelen, vastleggen, raadplegen, opvragen, ordenen, structureren, opslaan, bewerken of wijzigen, verstrekken en combineren. Ook het wissen of vernietigen van gegevens is een verwerking van persoonsgegevens.

Wat is een verwerkingsverantwoordelijke?

De verwerkingsverantwoordelijke is de natuurlijke persoon of rechtspersoon die (alleen of tezamen met anderen) bepaalt welke persoonsgegevens worden verzameld, waarom persoonsgegevens worden verwerkt (doel) en hoe persoonsgegevens worden verwerkt (middelen). Wanneer partijen gezamenlijk het doel en de middelen vaststellen voor de verwerking van persoonsgegevens dan spreken we van een gezamenlijke verantwoordelijkheid.

Wat is een verwerker?

Een verwerker is de natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt. Het gaat om derde partijen die voor de verwerkingsverantwoordelijke werken. Een verwerker handelt onder de verantwoordelijkheid van de verwerkingsverantwoordelijke en naar diens instructies, maar er is geen hiërarchische relatie (medewerkers zijn geen verwerkers). Daarnaast heeft de verwerker geen zeggenschap over de verwerkingen en mag de gegevens niet voor eigen doelen gebruiken.

N.B. BIJLAGE 2 IS EEN LOS DOCUMENT, HET LOSSE DOCUMENT IS LEIDEND.
BIJ VERSPREIDING VAN DIT PRIVACY BELEIDSKADER MOET DE MEEST RECENTE BIJLAGE 2 INSTRUMENTEN WORDEN TOEGEVOEGD.

Bijlage 2: Overzicht van Beleid en Instrumenten d.d. november 2024

Wet- en regelgeving

AVG Algemene Verordening Gegevensbescherming

UAVG Uitvoeringswet Algemene Verordening Gegevensbescherming

Websites

EDPS European Data Protection Supervisor, <https://edps.europa.eu/>

AP Autoriteit Persoonsgegevens, <https://autoriteitpersoonsgegevens.nl/>

Nr	Beleidsdocumenten	Vindplaats in H2 privacybeleid	Vindplaats In organisatie
1	Autorisaties (PM)		PM IB beleid
2	Informatiebeveiligingsbeleid	2.6	PM intranet
	Instrumenten voor verantwoording		
3	Cookieverklaring	2.5	website
4	Privacyverklaring Afdeling NI medewerkers	2.5 en 2.8	intranet
5	Privacyverklaring extern Afdeling NL NVAO/ CDHO/CMMBO	2.1	website
6	Protocol datalekken NVAO	2.6	intranet
7	Protocol Rechten Betrokkenen	2.3 en 2.8	Website/intranet check
8	Register datalekken en beveiligingsincidenten	2.6	Privacy nexus
9	Register van verwerkingen	2.1 en 2.7	Privacy Nexus/tabel
10	Register Verwerkingsovereenkomsten	2.7	Privacy Nexus
11	DPIA-register	2.1	Privacy Nexus
	Overige instrumenten ter ondersteuning van verantwoording		
11	Format verwerkersovereenkomst	2.7	Opvraagbaar bij PO
12	Handleiding Privacy by Design (versie 3.0 CIP)	2.2	Opvraagbaar bij PO
13	Memo Quick Scan DPIA	2.1	Opvraagbaar Po
14	Rijksmodel GEB PIA	2.1	Opvraagbaar Po
15	Selectielijst van de NVAO	2.4	website NA



--	--	--	--

Colofon

Privacy Beleidskader

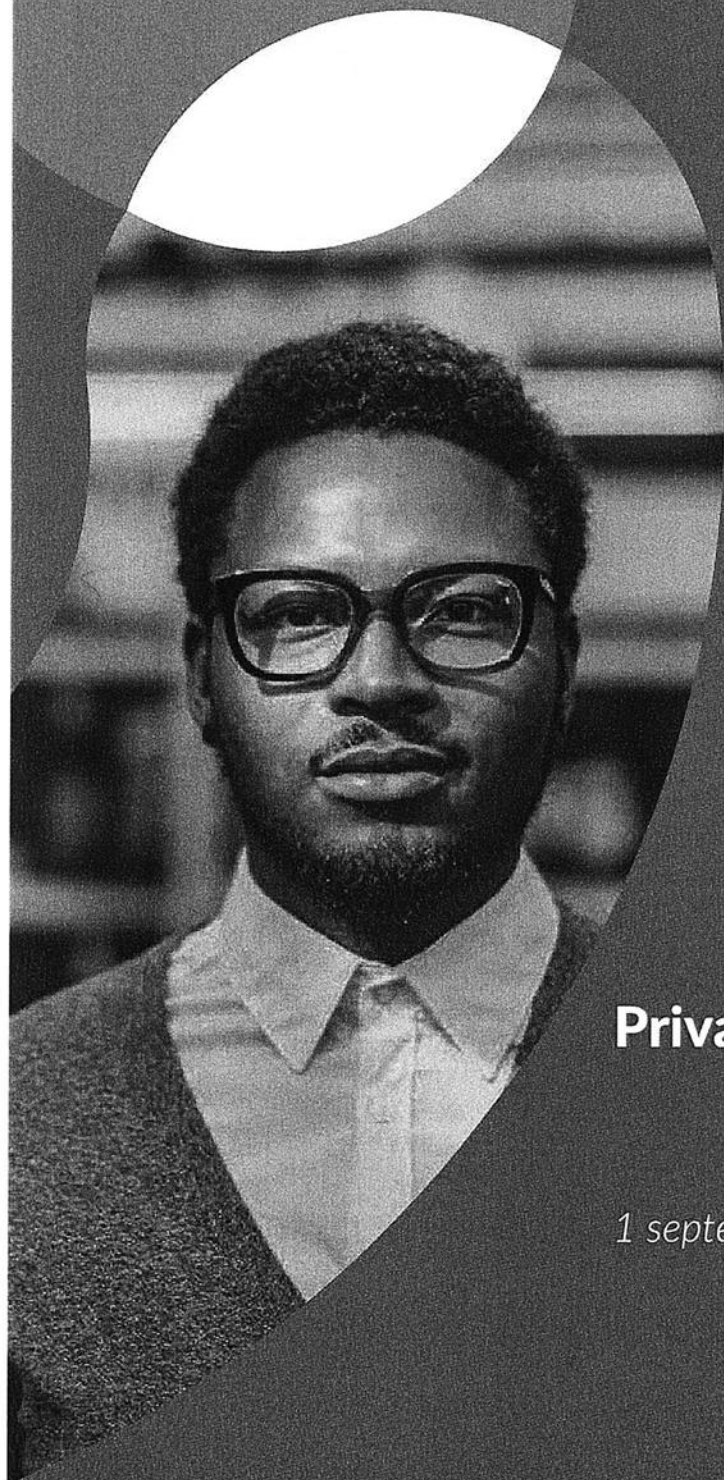


NVAO

Nederlands-Vlaamse Accreditatieorganisatie
Accreditation Organisation of the Netherlands and Flanders

Parkstraat 83 · 2514 JG Den Haag
P.O. Box 85498 · 2508 CD The Hague
The Netherlands

T +31 (0)70 312 23 00
E info@nvao.net
www.nvao.net

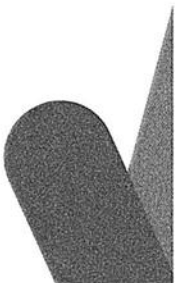


Privacyverklaring NVAO

1 september 2021

Privacyverklaring NVAO

1 september 2021



Inleiding

De NVAO werkt aan het bevorderen of verbeteren van de kwaliteit van het hoger onderwijs.

Voor het uitvoeren van de (wettelijke) taken verwerkt de NVAO persoonsgegevens. In deze privacyverklaring leest u hoe de NVAO als verwerkingsverantwoordelijke (in de zin van de Algemene verordening gegevensbescherming (AVG)) omgaat met persoonsgegevens.

De NVAO beslist welke persoonsgegevens worden verwerkt, voor welk doel en op welke manier. Ook is de NVAO ervoor verantwoordelijk dat dit in overeenstemming met de relevante privacywet- en regelgeving gebeurt.

Inhoud

1	Wat zijn persoonsgegevens?	5
2	Bijzondere persoonsgegevens	5
3	Waarom verwerkt de NVAO persoonsgegevens?	5
4	Welke persoonsgegevens verwerkt de NVAO?	5
5	Hoe gaat de NVAO met persoonsgegevens om?	6
6	Hoe worden uw persoonsgegevens beveiligd?	6
7	Wanneer en met wie worden persoonsgegevens gedeeld?	6
8	Cookies	7
9	Welke rechten heeft u als betrokkene?	7
10	Functionaris voor Gegevensbescherming	7
11	Contact	8
12	Over deze privacyverklaring	8

1 Wat zijn persoonsgegevens?

Een persoonsgegeven is informatie die direct over iemand gaat of informatie die naar deze persoon te herleiden is. Voorbeelden van persoonsgegevens zijn namen, adressen, telefoonnummers en e-mailadressen.

2 Bijzondere persoonsgegevens

Sommige persoonsgegevens zijn extra gevoelig, omdat de verwerking ervan veel impact kan hebben op iemands leven. Gegevens die iets zeggen over ras, godsdienst of gezondheid zijn voorbeelden van bijzondere persoonsgegevens. Deze persoonsgegevens zijn extra beschermd door de wet en mogen alleen worden verwerkt in door de wet genoemde situaties. BSN-nummers en persoonsgegevens van kinderen zijn geen bijzondere persoonsgegevens, maar wel persoonsgegevens die net als bijzondere persoonsgegevens extra worden beschermd door de wet.

3 Waarom verwerkt de NVAO persoonsgegevens?

De NVAO verwerkt persoonsgegevens voor verschillende doelen en wettelijke taken.

Het verwerken van persoonsgegevens kan bijvoorbeeld nodig zijn voor:

- de interne bedrijfsvoering;
- voor afdeling Nederland geldt: het verlenen van accreditaties of erkenningen Instellingstoets Kwaliteitszorg;
- voor afdeling Vlaanderen geldt: het verlenen van accreditaties, het advies verlenen over nieuwe opleidingen, het toekennen van een status op basis van een instellingsreview, het uitvoeren van systeembrede analyses.
- het instellen van of instemmen met (voorgestelde) panels, visitatiegroepen of commissies;
- het beantwoorden van vragen van burgers;
- het behandelen van klachten, of;
- het afhandelen van een verzoek op grond van de Wet openbaarheid van bestuur en AVG;
- Het behandelen van bezwaren bij besluiten en bij ontwerpen van besluiten.

4 Welke persoonsgegevens verwerkt de NVAO?

In alle gevallen worden voorletter of voornaam, achternaam, en mailadres verwerkt. Afhankelijk van het doel en de uit te voeren wettelijke taak worden functie en telefoonnummer verwerkt. Bij het indienen van een klacht wordt ook het adres (straatnaam, huisnummer, postcode en woonplaats) van betrokkene verwerkt, omdat dit wettelijk verplicht is.

Persoonsgegevens (zoals cv's) van sollicitanten worden na de sollicitatieprocedure verwijderd, tenzij betrokkene toestemming geeft deze gegevens langer te bewaren of een arbeidsrelatie wordt aangegaan.

Voor interne bedrijfsvoering worden meer persoonsgegevens (zoals cv) verwerkt, indien betrokkene (ook panellid of secretaris) werkzaamheden uitvoert voor de NVAO en in die hoedanigheid vergoeding ontvangt (bankrekeningnummer). Voor medewerkers of anderen die voor de NVAO werkzaamheden verrichten is de Privacyverklaring medewerkers van toepassing.

5 Hoe gaat de NVAO met persoonsgegevens om?

De NVAO hecht groot belang aan de bescherming van persoonsgegevens en gaat hier op een veilige en zorgvuldige manier mee om. De NVAO hanteert daarbij een aantal uitgangspunten:

- De verwerking van persoonsgegevens gebeurt in overeenstemming met de geldende wet- en regelgeving, waaronder de AVG, de Uitvoeringswet AVG en andere toepasselijke wetgeving. Te denken valt aan de Archiefwet 1995, Wet openbaarheid van bestuur, Wet op het hoger onderwijs en wetenschappelijk onderzoek voor de afdeling Nederland en de Codex Hoger Onderwijs voor de afdeling Vlaanderen.
- De verwerking van persoonsgegevens heeft een geldige rechtsgrondslag. Verwerkingen van de NVAO zijn voornamelijk gebaseerd op de uitvoering van publiekrechtelijke taken, het nakomen van wettelijke verplichtingen of de uitvoering van overeenkomsten. Het verwerken van persoonsgegevens kan bijvoorbeeld ook nodig zijn voor een gerechtvaardigd belang, zoals bij het verschaffen van toegang tot het kantoorgebouw vanwege bedrijfsvoerings- of beveiligingsaspecten.
- Persoonsgegevens worden alleen verwerkt als dat noodzakelijk is en alleen voor het specifieke doel waarvoor ze worden verzameld. Er worden niet méér persoonsgegevens verwerkt dan noodzakelijk is. Als het kan, verwerkt de NVAO minder of geen persoonsgegevens. De verwerking van persoonsgegevens is proportioneel en subsidiair.
- De NVAO is transparant over de verwerking van persoonsgegevens en informeert betrokkenen over de verwerking van hun persoonsgegevens. In enkele gevallen informeert de NVAO de betrokkenen in beginsel niet: als u de persoonsgegevens zelf heeft verstrekt aan de NVAO; als u al weet welke persoonsgegevens de NVAO van u heeft; als de omvang van de te informeren betrokkenen dusdanig groot is dat individueel informeren onevenredig veel tijd en middelen kost.
- De NVAO bewaart persoonsgegevens niet langer dan nodig is voor het doel waarvoor ze verzameld zijn, dan op grond van de Archiefwet 1995 is vereist, of op een andere wijze wettelijk is bepaald, zie ook de Codex Hoger Onderwijs. Als persoonsgegevens niet langer noodzakelijk of vereist zijn, worden deze vernietigd.

6 Hoe worden uw persoonsgegevens beveiligd?

De NVAO neemt maatregelen voor een betrouwbare, behoorlijke en zorgvuldige omgang met persoonsgegevens. Zo worden persoonsgegevens vertrouwelijk behandeld en zorgt de NVAO voor passende beveiliging van de persoonsgegevens die de NVAO onder zich heeft, in lijn met de daarvoor geldende wettelijke eisen en richtlijnen, waaronder in ieder geval de voorschriften en standaarden van de Rijksoverheid voor informatiebeveiliging. Met ontvangers en verwerkers van persoonsgegevens worden nadere afspraken gemaakt.

7 Wanneer en met wie worden persoonsgegevens gedeeld?

De uitvoering van de (wettelijke) taken kan met zich meebrengen dat de NVAO persoonsgegevens deelt (met onder andere onderwijsinstellingen). In beginsel deelt de NVAO echter geen persoonsgegevens met andere organisaties. Slechts bij hoge uitzondering en gerelateerd aan een wettelijke taak van de NVAO kunnen persoonsgegevens gedeeld worden met een ministerie of de inspectie.

Het delen van gegevens gebeurt altijd op basis van een geldige rechtsgrondslag (wet- of regelgeving, inclusief beoordelingskaders).

Ook worden afspraken gemaakt en passende maatregelen getroffen voor een betrouwbare, behoorlijke en zorgvuldige uitwisseling van de persoonsgegevens. Dat geldt ook voor de uitwisseling van persoonsgegevens met andere landen buiten de EER. Persoonsgegevens worden nooit aan derden verstrekt voor commerciële doeleinden.

8 Cookies

In de Cookieverklaring van de NVAO leest u meer over cookies bij het gebruik van de website nvaio.net.

9 Welke rechten heeft u als betrokkene?

Op grond van de AVG heeft u de volgende rechten met betrekking tot uw persoonsgegevens:

- **Recht op informatie:** de NVAO informeert u over de verwerking van uw gegevens. Daarnaast heeft u het recht om aan ons te vragen of uw persoonsgegevens worden verwerkt.
- **Inzagerecht:** u heeft het recht om inzage te krijgen in de gegevens die door de NVAO worden verwerkt. Wij zullen u een overzicht geven welke type persoonsgegevens worden verwerkt.
- **Correctierecht:** u kunt een verzoek tot wijziging van uw persoonsgegevens indienen bij de NVAO als blijkt dat deze niet juist zijn of deze inmiddels zijn veranderd.
- **Recht om vergeten te worden:** in gevallen waar u toestemming heeft gegeven om gegevens te verwerken, heeft u het recht om deze toestemming in te trekken en de NVAO te verzoeken om deze persoonsgegevens te laten verwijderen. In gevallen waar de NVAO persoonsgegevens verwerkt op grond van bijvoorbeeld een wettelijke plicht, is het niet mogelijk om deze gegevens te verwijderen.
- **Recht op bezwaar:** u heeft het recht om een bezwaar in te dienen tegen de verwerking van uw persoonsgegevens. Dit kan bijvoorbeeld als u van mening bent dat de bescherming van privacy zwaarder zou wegen dan het algemene belang van de NVAO om persoonsgegevens te verwerken.

Uw AVG-verzoek of bezwaar kunt u richten aan het privacy office van de NVAO via privacy@nvaio.net.

De NVAO heeft vanaf de ontvangst van het AVG-verzoek ten hoogste vier weken de tijd om te beoordelen of het verzoek gerechtvaardigd is en hoe de behandeling van het verzoek eruit zal zien. Heeft de NVAO meer tijd nodig om de gegevens te verzamelen, dan stuurt de NVAO binnen vier weken bericht aan verzoeker. In dit bericht staat ook vermeld dat de totale behandeling niet langer dan drie maanden in beslag zal nemen.

Het is belangrijk dat u zich, als wij daarom vragen, kunt legitimeren en dat u kunt aantonen dat de gegevens die u wilt inzien, corrigeren of verwijderen daadwerkelijk van u zijn. Het is niet toegestaan om gegevens van andere personen in te zien.

Hoe een veilige kopie gemaakt kan worden, is te vinden op [Rijksoverheid.nl](https://rijksoverheid.nl). Ook kunt u worden verzocht uw verzoek te preciseren om u zo goed mogelijk van dienst te kunnen zijn.

De NVAO maakt geen gebruik van geautomatiseerde besluitvorming (profilering) zonder menselijke tussenkomst. Dit betekent dat er altijd een medewerker betrokken is bij de besluitvorming.

10 Functionaris voor Gegevensbescherming

Bij de NVAO is een Functionaris voor Gegevensbescherming (FG) werkzaam en bij de Autoriteit persoonsgegevens gemeld. Als onafhankelijke, interne toezichthouder ziet zij erop toe dat de verwerkingen van persoonsgegevens binnen de NVAO, in overeenstemming zijn met de wet.

Heeft u een vraag over de manier waarop de NVAO omgaat met uw persoonsgegevens, dan kunt u ook contact opnemen met de FG.

U kunt uw vragen digitaal stellen aan: privacy@nvao.net

11 Contact

Voor vragen naar aanleiding van deze privacyverklaring, voor verzoeken zoals inzage in uw persoonsgegevens, of klachten, kan contact opgenomen worden met privacy@nvao.net.

Uw klacht kunt u ook indienen bij de nationale toezichthouder, de Autoriteit persoonsgegevens.

12 Over deze privacyverklaring

De Privacyverklaring NVAO is na instemming van de OR vastgesteld op 24 augustus 2021 door het gemandateerde Dagelijks Bestuur en treedt op 1 september 2021 in werking. De NVAO behoudt zich het recht voor om deze privacyverklaring op ieder gewenst moment en om welke reden dan ook te wijzigen. De meest recente versie van de privacyverklaring is beschikbaar op de website.

Colofon

Privacyverklaring NVAO

1 september 2021

Samenstelling: NVAO

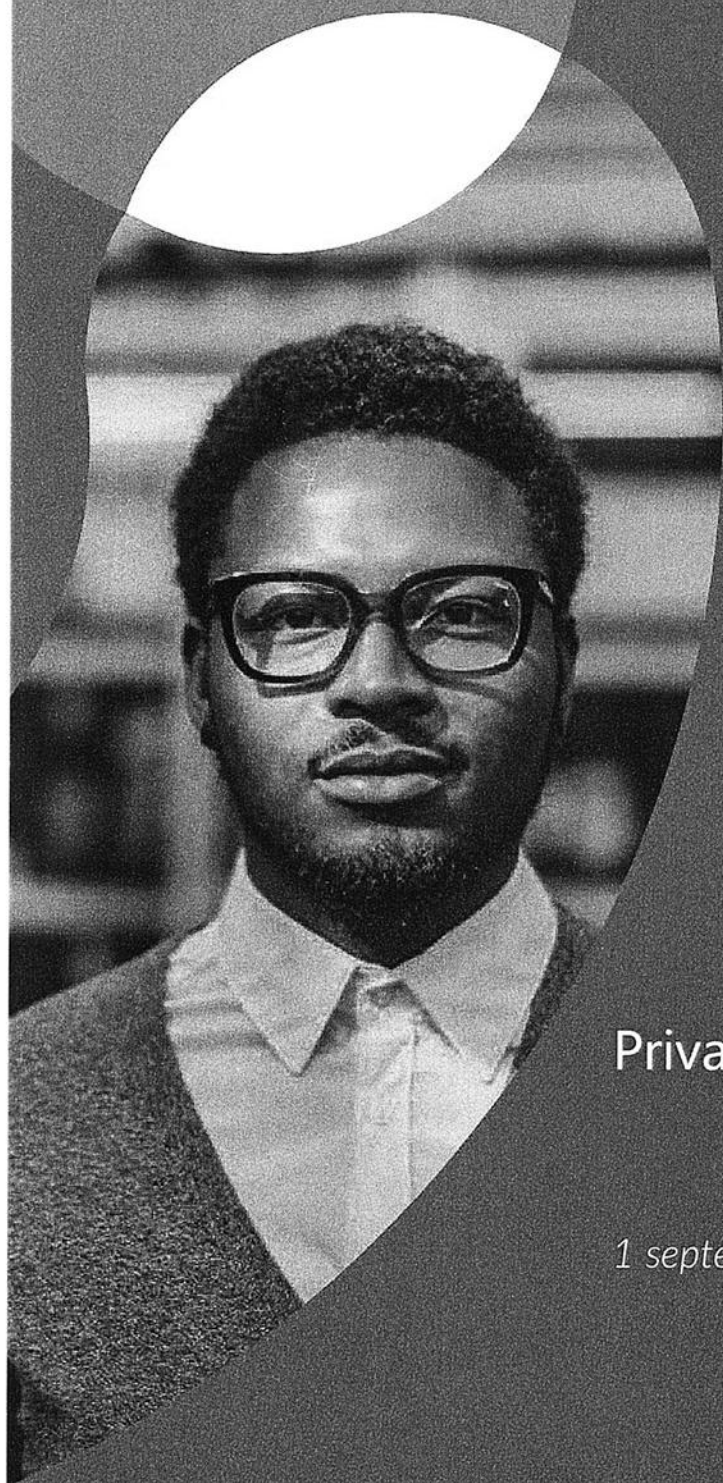


Nederlands-Vlaamse Accreditatieorganisatie
Accreditation Organisation of the Netherlands and Flanders

Parkstraat 83 · 2514 JG Den Haag
P.O. Box 85498 · 2508 CD The Hague
The Netherlands

T +31 (0)70 312 23 00
E info@nvao.net
www.nvao.net

Privacyverklaring extern NVAO NL 2025.pdf

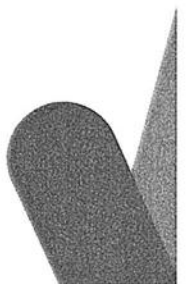


Privacyverklaring medewerkers

1 september 2021

Privacyverklaring medewerkers

1 september 2021



Inleiding

De NVAO (verder ook met 'wij' aangeduid) hecht veel waarde aan de privacy van zijn medewerkers en streeft ernaar hun persoonlijke informatie te verwerken, conform alle wettelijke bepalingen die vanuit de Algemene Verordening Gegevensbescherming (AVG) gelden.

Onder medewerkers worden allen verstaan die werkzaamheden uitvoeren t.b.v. de NVAO en een schriftelijke arbeidsovereenkomst of overeenkomst van opdracht hebben afgesloten met de NVAO. Op medewerkers van de CDHO en CMMBO is deze privacyverklaring daarmee ook van toepassing.

In deze privacyverklaring informeren wij jou als medewerker over:

- De persoonsgegevens die wij van jou verwerken;
- De doeleinden waarvoor we dat doen en wat de grondslag hiervoor is;
- Met wie wij informatie delen;
- Hoe wij omgaan met jouw persoonsgegevens;
- Hoe lang wij jouw gegevens bewaren;
- Welke privacyrechten jij hebt en hoe je deze kunt uitoefenen.

Inhoud

1	Wat zijn persoonsgegevens?	5
1.1	Bijzondere persoonsgegevens	5
1.2	Strafrechtelijke persoonsgegevens	5
2	Verwerken	5
2.1	Welke persoonsgegevens verwerken wij?	5
2.2	Waarom verwerken wij jouw persoonsgegevens?	6
3	Met wie worden jouw persoonsgegevens gedeeld?	7
4	Hoe gaan wij met jouw persoonsgegevens om?	7
5	Hoe lang worden jouw persoonsgegevens bewaard?	7
6	Welke privacy rechten heb je?	7
7	Contact.....	8
8	Slotbepalingen.....	8

1 Wat zijn persoonsgegevens?

De AVG geeft aan dat een persoonsgegeven alle informatie is over een geïdentificeerde of identificeerbare natuurlijke persoon. Persoonsgegevens gaan dus altijd direct over een persoon of zijn naar deze persoon te herleiden. Voorbeelden van persoonsgegevens zijn adressen, telefoonnummers en e-mailadressen.

1.1 Bijzondere persoonsgegevens

Sommige persoonsgegevens zijn extra gevoelig, omdat de verwerking ervan veel impact kan hebben op iemands leven. Gegevens die iets zeggen over ras, godsdienst of gezondheid, zijn voorbeelden van bijzondere persoonsgegevens. We verwerken in het kader van de aanstelling ook het Burgerservicenummer. Het BSN is geen bijzonder persoonsgegeven, maar wel een persoonsgegeven dat net als bijzondere persoonsgegevens extra wordt beschermd door de wet.

1.2 Strafrechtelijke persoonsgegevens

Strafrechtelijke gegevens zijn gegevens zoals een strafblad, strafbare feiten, verdenkingen en veiligheidsmaatregelen. Strafrechtelijke persoonsgegevens zijn ook extra beschermd door de wet.

2 Verwerken

Het verwerken van persoonsgegevens betreft alle handelingen die worden uitgevoerd met persoonsgegevens. Dit is een breed begrip: jouw privacyrechten zijn dus al gauw van toepassing. Verwerken is in ieder geval het verzamelen, vastleggen, ordenen, bewaren, wijzigen, plegen, gebruiken, doorzenden, of wissen van persoonsgegevens. Bij de hieronder genoemde verwerkingen is de NVAO als verwerkingsverantwoordelijke aan te merken, tenzij anders aangegeven..

2.1 Welke persoonsgegevens verwerken wij?

Van medewerkers kunnen wij de volgende persoonsgegevens verwerken:

- Persoonlijke identificatie-informatie (kopie ID): voor- en achternaam/-namen, adres, geboortedatum, geslacht, pasfoto, nationaliteit en geboorteplaats;
- Burgerservicenummer, identiteitskaart- of paspoortnummer;
- Contactgegevens: privé e-mailadres en telefoonnummer(s);
- Werkgerelateerde contactgegevens: werk e-mailadres en telefoonnummer;
- Contactgegevens van personen voor noodgevallen;
- Werkgerelateerde informatie, zoals aantal dienstjaren, werklocatie, werkdagen, beklede functies, referenties, verlof- en verzuimregistratie, zwangerschaps- en/of ouderschapsverlof, contractgegevens, arbeidsovereenkomst, opgebouwd pensioen, ondertekende geheimhoudingsverklaring, ondertekende ambtseed, of belofte en ondertekende Integriteitscode NVAO;
- Opleidings- en trainingsinformatie, zoals diploma's en certificaten, beroepsverleden en interne en/of externe opleidings- of trainingsdeelname;
- Prestatiegerelateerde gegevens zoals productiecijfers en plannings-, opvolgings- en functioneringsgesprekken;
- Bij beëindiging dienstverband: informatie over outplacementtraject, vaststellingsovereenkomst, (gerechtelijk) ontbindingsverzoek, ontslagvergunning en ontslagbrief;

- Informatie betreffende het gebruik van bedrijfsmiddelen van de NVAO;
- Verklaring omtrent het gedrag (VOG);
- Informatie nodig voor conformiteit en risicomanagement zoals disciplinaire dossiers;
- Informatie m.b.t. loonlijst, betalingen en voordelen, zoals salaris- en verzekeringsinformatie, pensioeninformatie, ondergeschikten, Burgerservicenummer, bankgegevens (kopie bankpas), loonbeslagen, informatie over werkgerelateerde voordelen, loonheffingsverklaring, reiskosten en de NS-Business Card;
- Persoonlijke informatie op incidentele basis (bijvoorbeeld als er sprake is van een wijziging in zijn/haar burgerlijke staat);
- Verslagen van de bedrijfsarts, het verzuimdossier, de re-integratieverslagen, en eventuele inzet van overige interventies.
- Wervingsgerelateerde informatie zoals cv, motivatie en assessmentgegevens;
- Andere informatie die je meestuurt in je CV of een bijlage.

2.2 Waarom verwerken wij jouw persoonsgegevens?

Wij verwerken persoonlijke informatie voor de volgende doeleinden:

- Personeelsplanning, -werving en -bezetting;
- Personeelsregistratie en -beheer, loonlijst, regelingen voor vergoedingen en voordelen;
- Prestatiebeheer, voortgang, inzetbaarheid, leren en ontwikkeling;
- Functieverandering, opvolgingsplanning en beëindiging dienstverband;
- Werkpiekbeheer, zoals reis- en onkostenprogramma's en interne regelingen rond gezondheid en veiligheid;
- Het beheer van operationele activiteiten;
- Het beheer van informatiesystemen;
- Interne rapportage;
- Audit(s);
- Om de NVAO, het personeel en het publiek te beschermen tegen letsel, diefstal, juridische aansprakelijkheid, fraude, misbruik of risico's voor de veiligheid van onze netwerken, berichtgeving, systemen, voorzieningen en infrastructuur;
- Juridische procedures en compliance, met inbegrip van de naleving van informatieaanvragen van overheidsinstanties, retentierechten, beslagleggingen en fiscale naleving;
- Het versturen van attenties aan het personeel als blijk van waardering en in het kader van goed werkgeverschap;
- Overige juridische en gangbare organisatie-gerelateerde doeleinden.

Wij verwerken alleen persoonsgegevens als we een wettelijke grondslag hebben. Dit gebruik van persoonlijke informatie is gebaseerd op een van de onderstaande rechtsgronden, indien van toepassing:

- De behoefte om persoonlijke informatie te verwerken in het kader van de arbeidsovereenkomst of om stappen te ondernemen om een overeenkomst met betrokkene te sluiten dan wel via een intermediair;
- De wettelijke verplichtingen van de NVAO als werkgever;
- De legitieme belangen van de NVAO, waaronder het algemeen beheer van personeelszaken, algemene bedrijfsactiviteiten, bekendmaking voor audit- en rapportagedoeleinden, interne onderzoeken, contractuele verplichtingen ten opzichte van derden, het beheer van de veiligheid van netwerken en informatiesystemen en het beschermen van de bedrijfsmiddelen van de NVAO, en;
- in bepaalde specifieke omstandigheden, met toestemming van de betrokkene.

3 Met wie worden jouw persoonsgegevens gedeeld?

In het geval van samenwerking met externe partijen, waarbij sprake is van verwerking van persoonsgegevens, maakt de NVAO afspraken over de eisen waar de gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet. De NVAO controleert deze afspraken periodiek.

Overzicht van derden met wie de NVAO persoonsgegevens deelt

Salarisadministratiesysteem, Phocus d.d. 1-1-2021	Jouw persoonsgegevens (zoals hierboven vermeld) worden beheerd in dit personeelsinformatiesysteem, ter ondersteuning van de uitvoering van onze taken zoals hierboven vermeld.
Microsoft	
Bedrijfsarts	
Arbodienst	
Evt. Re-integratiebureau	

4 Hoe gaan wij met jouw persoonsgegevens om?

De NVAO hanteert een aantal uitgangspunten bij de verwerking van persoonsgegevens en neemt maatregelen voor een betrouwbare, behoorlijke en zorgvuldige omgang met persoonsgegevens. De uitgangspunten zijn verankerd in het Privacy Beleidskader en ook in de Privacyverklaring NVAO nader uitgewerkt.

5 Hoe lang worden jouw persoonsgegevens bewaard?

Een van de uitgangspunten is dat persoonlijke informatie niet langer wordt bewaard dan nodig is om het doel waarvoor het is verzameld te bereiken. Dit betekent voor medewerkers meestal zolang er sprake is van een contractuele relatie en zolang eraan als wettelijk vereist of toegestaan is in de geldende wetgeving.

De gegevens die de NVAO van jou verwerkt worden bewaard na afloop van de arbeidsovereenkomst of overeenkomst van opdracht. Voor hoe lang is beschreven in de Selectielijst.

6 Welke privacy rechten heb je?

Op grond van de AVG heb je de volgende rechten met betrekking tot je persoonsgegevens:

- **Recht op informatie:** de NVAO informeert jou over de verwerking van jouw gegevens. Daarnaast heb je het recht om aan ons te vragen of jouw persoonsgegevens worden verwerkt.
- **Inzagerecht:** je hebt het recht om inzage te krijgen in de gegevens die door de NVAO worden verwerkt. Wij zullen je een overzicht geven welke type persoonsgegevens worden verwerkt.
- **Correctierecht:** je kan een verzoek tot wijziging van jouw persoonsgegevens indienen bij de NVAO als blijkt dat deze niet juist zijn of deze inmiddels zijn veranderd.
- **Recht om vergeten te worden:** in gevallen waar je toestemming hebt gegeven om gegevens te verwerken, heb je het recht om deze toestemming in te trekken en de NVAO te verzoeken om deze persoonsgegevens te laten verwijderen. In gevallen waar de NVAO persoonsgegevens verwerkt op grond van bijvoorbeeld een wettelijke plicht, is het niet mogelijk om deze gegevens te verwijderen.

- **Recht op bezwaar:** je hebt het recht om een bezwaar in te dienen tegen de verwerking van jouw persoonsgegevens. Dit kan bijvoorbeeld als je van mening bent dat de bescherming van privacy zwaarder zou wegen dan het algemene belang van de NVAO om persoonsgegevens te verwerken.

7 Contact

Om gebruik te maken van deze rechten kan je per e-mail een verzoek indienen.

Het verzoek kan je richten aan de privacy officer via privacy@nvao.net.

De NVAO heeft vanaf de ontvangst van het verzoek een maand de tijd om te beoordelen of het verzoek gerechtvaardigd is. Binnen maand laat de NVAO aan je weten wat er met het verzoek gaat gebeuren. Heeft de NVAO meer tijd nodig om de gegevens te verzamelen, dan ontvang je daar ook binnen een maand bericht van. Als het verzoek niet wordt opgevolgd, heb je de mogelijkheid om bezwaar te maken bij de NVAO, of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). De NVAO kan aanvullende informatie opvragen om zeker te zijn van je identiteit en de rechtmatigheid van het verzoek.

Ben je niet tevreden met onze antwoorden op jouw privacy vragen? Dan kun je een klacht indienen bij de Autoriteit Persoonsgegevens.

Bij de NVAO houdt de Functionaris voor Gegevensbescherming toezicht op de toepassing en de naleving van de AVG. Heb je na het lezen van deze privacyverklaring nog vragen over hoe wij jouw persoonsgegevens gebruiken dan kan je via e-mail contact opnemen via email: (Privacy@nvao.net) contact opnemen met de functionaris voor gegevensbescherming van de NVAO.

8 Slotbepalingen

Deze privacyverklaring is op 24 augustus 2021 na instemming van de OR vastgesteld door het gemandateerde Dagelijks Bestuur en treedt op 1 september 2021 in werking.

De verklaring wordt periodiek geëvalueerd en indien nodig herzien. Aanpassingen in deze privacyverklaring worden aangekondigd via intranet.

Colofon

Privacyverklaring medewerkers

1 september 2021

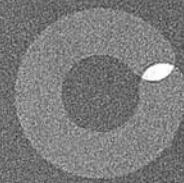
Samenstelling: NVAO



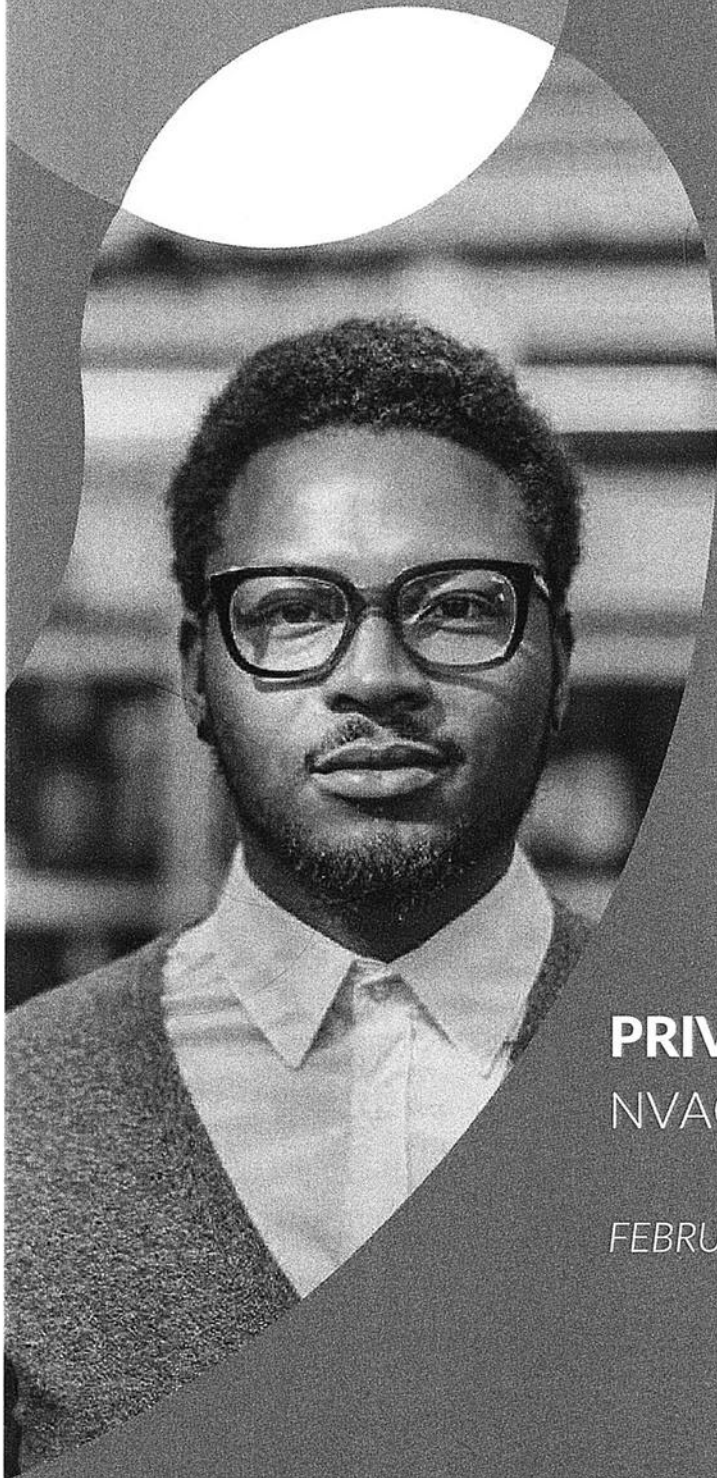
Nederlands-Vlaamse Accreditatieorganisatie
Accreditation Organisation of the Netherlands and Flanders

Parkstraat 83 · 2514 JG Den Haag
P.O. Box 85498 · 2508 CD The Hague
The Netherlands

T +31 (0)70 312 23 00
E info@nvao.net
www.nvao.net



NVAO



PRIVACYVERKLARING (INTERN)

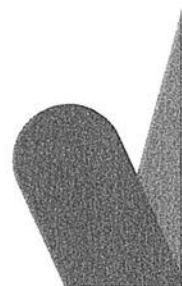
NVAO Nederland

FEBRUARI 2025

PRIVACYVERKLARING (INTERN)

NVAO NEDERLAND

FEBRUARI 2025



Inleiding

Dit is de Privacyverklaring van de Nederlands-Vlaamse Accreditatieorganisatie, afdeling Nederland (NVAO NL). De NVAO is juridisch gezien een zelfstandig bestuursorgaan (ZBO) naar Nederlands publiek recht, hetgeen betekent dat de organisatie, ongeacht of het de afdelingen betreft of het bestuur, gehouden is aan de Nederlandse regelgeving voor ZBO's. Sinds de verbijzondering is er sprake van een totale splitsing in de bedrijfsvoering binnen de afdelingen (NL en VL) en hebben de afzonderlijke afdelingen eigen voorzieningen op het gebied van ICT, financiën en HR.

Voor het primaire proces, de belangrijkste taak van de NVAO, namelijk het accrediteren van opleidingen en instellingen, is al op basis van het Verdrag bepaald dat de afzonderlijke afdelingen besluiten nemen op basis van de eigen regelgeving van Vlaanderen dan wel Nederland. Op basis van de governance-documenten die in het kader van de verbijzondering bij de NVAO zijn bekrachtigd door de Minister van Onderwijs, Cultuur en Wetenschap (OCW), is de feitelijke verwerkingsverantwoordelijkheid belegd binnen de afzonderlijke afdelingen. De afdeling Nederland van de NVAO (verder ook met 'wij' aangeduid of NVAO NL) hecht veel waarde aan de privacy van zijn medewerkers en streeft ernaar hun persoonlijke informatie te verwerken conform alle wettelijke bepalingen die vanuit de Algemene verordening gegevensbescherming (AVG) gelden.

Onder medewerkers verstaan wij in deze verklaring: iedereen die werkzaamheden uitvoert ten behoeve van NVAO NL op basis van een schriftelijke arbeidsovereenkomst dan wel op basis van een overeenkomst van opdracht. Op medewerkers van de Commissie Doelmatigheid Hoger Onderwijs (CDHO) en Commissie Macrodoelmatigheid mbo (CMMBO) is deze privacyverklaring daarmee ook van toepassing.

Hoewel bestuursleden van en voor Nederland, Algemeen Bestuur (AB) en Dagelijks Bestuur (DB), geen arbeidsovereenkomst of overeenkomst van opdracht hebben met NVAO NL, zij worden namelijk benoemd door de minister van OCW, voeren zij werkzaamheden uit ten behoeve van NVAO NL en ook zij kunnen in deze privacyverklaring meer lezen over de verwerking van hun persoonsgegevens.

Deze verklaring is ook van toepassing op panelleden en secretarissen die voor Nederlandse accreditatieprocedures betrokken zijn bij een Instellingstoets Kwaliteitszorg (ITK), Toets nieuwe opleiding (TNO) of andere panelsamenstellingen in verband met beoordelingen door NVAO NL. Deze panelleden en secretarissen hebben geen arbeidsovereenkomst met NVAO NL maar verrichten wel werkzaamheden die in opdracht van NVAO NL worden georganiseerd. Zij worden op grond van het bestuursrecht ingesteld voor deze taak en ontvangen ter uitvoering van hun werkzaamheden een overeenkomst van opdracht.

In deze privacyverklaring informeren wij jou over:

- De persoonsgegevens die wij van jou verwerken;
- De doeleinden waarvoor we dat doen en wat de grondslag hiervoor is;
- Met wie wij informatie delen;
- Hoe wij omgaan met jouw persoonsgegevens;
- Hoe lang wij jouw gegevens bewaren;
- Welke privacyrechten jij hebt en hoe je deze kunt uitoefenen.

Inhoud

1	Wat zijn persoonsgegevens?	5
1.1	Bijzondere persoonsgegevens.....	5
2	Verwerken	6
2.1	Welke persoonsgegevens verwerken wij?.....	6
2.1.1	Medewerkers met arbeidsovereenkomst.....	6
2.1.2	Medewerkers met een overeenkomst van opdracht	6
2.1.3	AB- en DB-leden Nederland.....	7
2.1.4	Medewerkers ingeleend via derden.....	7
2.1.5	Panelleden en secretarissen (TNO- en ITK-procedure en onderzoekstaak)	7
2.2	Waarom verwerken wij jouw persoonsgegevens?.....	8
3	Met wie worden jouw persoonsgegevens gedeeld?.....	10
4	Met wie worden jouw persoonsgegevens gedeeld?.....	12
5	Hoe lang worden jouw persoonsgegevens bewaard?	13
6	Welke privacyrechten heb je?	14
7	Uitoefening privacyrechten & contact gegevensbescherming.....	15
8	Slotbepaling.....	16
	Lijst van begrippen en afkortingen	17

1 Wat zijn persoonsgegevens?

De AVG geeft aan dat een persoonsgegeven alle informatie is over een geïdentificeerde of identificeerbare natuurlijke persoon. Persoonsgegevens gaan dus altijd direct over een persoon of zijn naar deze persoon te herleiden. Voorbeelden van persoonsgegevens zijn onder andere adressen, telefoonnummers en e-mailadressen.

1.1 Bijzondere persoonsgegevens

Sommige persoonsgegevens zijn extra gevoelig, omdat de verwerking ervan veel impact kan hebben op iemands leven. Gegevens die iets zeggen over ras, godsdienst of gezondheid, zijn voorbeelden van bijzondere persoonsgegevens. We verwerken in het kader van de aanstelling onder andere het Burgerservicenummer (BSN) of een ander wettelijk identificerend nummer. Het wettelijk identificerend nummer is geen bijzonder persoonsgegeven, maar wel een persoonsgegeven dat, net als bijzondere persoonsgegevens, extra wordt beschermd door de wet.

2 Verwerken

Het verwerken van persoonsgegevens betreft alle handelingen die worden uitgevoerd met persoonsgegevens. Dit is een breed begrip: jouw privacyrechten zijn dus snel van toepassing. Verwerken is in ieder geval het verzamelen, vastleggen, ordenen, bewaren, wijzigen, raadplegen, gebruiken, doorzenden of wissen van persoonsgegevens. Bij de hieronder genoemde verwerkingen is de afdeling Nederland als onderdeel van de NVAO als verwerkingsverantwoordelijke aangemerkt, tenzij anders aangegeven.

2.1 Welke persoonsgegevens verwerken wij?

Per groep personen wordt hieronder vermeld welke persoonsgegevens verwerkt kunnen worden. Het gaat om de volgende zes groepen:

- Medewerkers met een arbeidsovereenkomst;
- Medewerkers met een overeenkomst van opdracht;
- Bestuursleden AB en DB die benoemd zijn ten behoeve van Nederland;
- Medewerkers die zijn ingeleend via derden;
- Panelleden en secretarissen voor TNO en ITK en onderzoekstaak in opdracht van afdeling Nederland.

2.1.1 Medewerkers met arbeidsovereenkomst

- Persoonlijke identificatie-informatie, zoals voornamen en achternaam, geboortedatum, geslacht, burgerlijke staat, nationaliteit en geboorteplaats;
- Wettelijk identificerend nummer;
- Kopie van identificatiebewijs (ID);
- Verklaring omtrent gedrag (VOG);
- Contactgegevens werk en privé, zoals e-mailadres en telefoonnummer(s);
- Contactgegevens van personen voor noodgevallen (naam, telefoonnummer en soort relatie);
- Wervingsgerelateerde informatie, zoals curriculum vitae (CV), motivatie, referenties en assessmentgegevens;
- Werkgerelateerde informatie, zoals aantal dienstjaren, werklocatie, werkdagen, beschikbaarheid/inzetbaarheid, beklede functies binnen de NVAO, nevenfuncties buiten de NVAO, vakantie-, bijzonder- en zorgverlofregistratie, verzuimregistratie, zwangerschaps- en ouderschapsverlof, benoemingsbrief/arbeidsovereenkomst, opgebouwd pensioen, ondertekende ambtseed, of -belofte en overeenkomst bruikleen bedrijfsmiddelen;
- Opleidings- en trainingsinformatie, zoals diploma's, certificaten en interne en/of externe opleidings- of trainingsdeelname;
- Prestatiegerelateerde gegevens, zoals productiecijfers en plannings-, opvolgings- en functioneringsgesprekken;
- Financiële gegevens, zoals salaris- en verzekeringsinformatie, pensioeninformatie (evenals uitdraai ABP-overzicht), ondergeschikten, IBAN en/of BIC-code, loonbeslag(en), loonheffingsverklaring en reiskosten (woon-werkverkeer of zakelijk vervoer);
- Verslagen van de bedrijfsarts, het verzuimdossier, de re-integratieverslagen, en eventuele inzet van overige interventies;
- Bij beëindiging dienstverband: informatie over outplacementtraject, vaststellingsovereenkomst, (gerechtelijk) ontbindingsverzoek, ontslagvergunning en ontslagbrief, WW-rechten (duur & hoogte uitkering);
- Overige door de medewerker verstrekte persoonlijke informatie.

2.1.2 Medewerkers met een overeenkomst van opdracht

- Persoonlijke identificatie-informatie, zoals voornamen en achternaam/-namen, roepnaam en initialen;

- VOG;
- Contactgegevens, zoals e-mailadres en telefoonnummer (werk);
- Wervingsgerelateerde informatie, zoals CV, motivatie en referenties;
- Werkgerelateerde informatie, zoals overeenkomst van opdracht, geheimhoudingsverklaring en Integriteitsverklaring NVAO NL;
- Financiële gegevens, zoals IBAN en/of BIC-code en reiskosten (woon-werkverkeer of zakelijk vervoer);
- Overige door de medewerker overhandigde persoonlijke informatie.

2.1.3 AB- en DB-leden Nederland

- Persoonlijke identificatie-informatie, zoals voornamen en achternaam/-namen, roepnaam, initialen, adres en geboortedatum;
- Persoonlijke identificatie-informatie, zoals wettelijk identificerend nummer en burgerlijke staat;
- VOG en in gevallen kopie van ID voor het aanvragen hiervan;
- Contactgegevens, zoals e-mailadres en telefoonnummer (privé);
- Contactgegevens, zoals e-mailadres en telefoonnummer (werk);
- Wervingsgerelateerde informatie, zoals CV, motivatie en referenties;
- Werkgerelateerde informatie, zoals nevenfuncties buiten de NVAO en Integriteitsverklaring;
- Opleidings- en trainingsinformatie, zoals interne en/of externe opleidings- of trainingsdeelname;
- Financiële gegevens, zoals IBAN en/of BIC-code en reiskosten (woon-werkverkeer of zakelijk vervoer);
- Bij beëindiging dienstverband: ontslagbrief;
- Overige door de medewerker overhandigde persoonlijke informatie.

2.1.4 Medewerkers ingeleend via derden

- Persoonlijke identificatie-informatie, zoals voornamen en achternaam/-namen, roepnaam, initialen, adres, geboortedatum en pasfoto;
- Persoonlijke identificatie-informatie, zoals burgerlijke staat;
- VOG en in gevallen kopie van ID voor het aanvragen hiervan;
- Contactgegevens, zoals e-mailadres en telefoonnummer (privé);
- Contactgegevens, zoals e-mailadres en telefoonnummer (werk);
- Contactgegevens van personen voor noodgevallen (naam, telefoonnummer en soort relatie);
- Wervingsgerelateerde informatie, zoals CV, motivatie, referenties en assessmentgegevens;
- Werkgerelateerde informatie, zoals aantal dienstjaren, werklocatie, werkdagen, beschikbaarheid/inzetbaarheid, beklede functies binnen NVAO NL, nevenfuncties buiten NVAO NL, vakantie-, bijzonder- en zorgverlofregistratie, verzuimregistratie, benoemingsbrief, Integriteitsverklaring, overeenkomst bruikleen bedrijfsmiddelen, duur van de detachingsperiode, detachingsovereenkomst, inleenovereenkomst, Integriteitsverklaring NVAO NL;
- Opleidings- en trainingsinformatie, zoals interne en/of externe opleidings- of trainingsdeelname;
- Prestatiegerelateerde gegevens, zoals productiecijfers en plannings-, opvolgings- en functioneringsgesprekken;
- Financiële gegevens, zoals IBAN en/of BIC-code en reiskosten (woon-werkverkeer of zakelijk vervoer);
- Overige door de medewerker overhandigde persoonlijke informatie.

2.1.5 Panelleden en secretarissen (TNO- en ITK-procedure en onderzoekstaak)

- Persoonlijke identificatie-informatie, zoals achternaam/-namen, roepnaam, initialen, adres, geslacht en geboorteplaats, titel(s) en taalvaardigheid;
- Persoonlijke identificatie-informatie, zoals wettelijk identificerend nummer;
- Contactgegevens, zoals e-mailadres en telefoonnummer (privé);
- Contactgegevens, zoals e-mailadres en telefoonnummer (werk);
- Wervingsgerelateerde informatie, zoals CV (en motivatie);
- Werkgerelateerde informatie, zoals beschikbaarheid/inzetbaarheid, beklede functies binnen de NVAO, nevenfuncties buiten NVAO NL, beschikbaarheid/inzetbaarheid, benoemingsbrief, overeenkomst van opdracht, Onafhankelijkheidsverklaring en geheimhoudingsverklaring, besluit/bericht tot toelaten of verwijderen uit register van secretarissen en Integriteitsverklaring;
- Opleidings- en trainingsinformatie, zoals beroepsverleden en interne en/of externe opleidings- of trainingsdeelname;
- Prestatiegerelateerde gegevens, zoals productiecijfers (aantal beoordelingen of geschreven rapporten zijn bekend);
- Financiële gegevens, zoals salaris- en verzekeringsinformatie, IBAN en/of BIC-code en reiskosten (woon-werkverkeer of zakelijk vervoer);
- Overige door de medewerker overhandigde persoonlijke informatie.

2.2 Waarom verwerken wij jouw persoonsgegevens?

Doeleinden:

- Personeelsplanning, -werving en -bezetting;
- Personeelsregistratie en -beheer, loonlijst, regelingen voor vergoedingen en voordelen;
- Prestatiebeheer, voortgang, inzetbaarheid, leren en ontwikkeling;
- Functieverandering, opvolgingsplanning en beëindiging dienstverband;
- Werkplekbeheer, zoals reis- en onkostenprogramma's en interne regelingen rond gezondheid en veiligheid;
- Het beheer van operationele activiteiten;
- Het beheer van informatiesystemen;
- Interne rapportage;
- Audit(s);
- Inzet accreditaties ten behoeve van het hoger onderwijs (beoordelen van deskundigheid en onafhankelijkheid, registratie van secretarissen, publicatie rapport, archivering);
- Onderzoek in het kader van kwaliteitsbewaking en rapportagetaak.
Om de kwaliteit te waarborgen moeten gegevens verzameld en geanalyseerd worden. Als onderdeel van deze onderzoekstaak kunnen ook interviews met bijvoorbeeld focusgroepen worden afgenomen om hiermee aanvullende en verdiepende inzichten te verkrijgen. Dit helpt NVAO NL inzicht te verkrijgen over de kwaliteit van opleidingen en hierover te rapporteren aan het Ministerie van OCW;
- Om de NVAO, het personeel en het publiek te beschermen tegen letsel, diefstal, juridische aansprakelijkheid, fraude, misbruik of risico's voor de veiligheid van onze netwerken, berichtgeving, systemen, voorzieningen en infrastructuur;
- Juridische procedures en compliance, met inbegrip van de naleving van informatieaanvragen van overheidsinstanties, retentierechten, beslagleggingen en fiscale naleving;
- Het versturen van attenties aan het personeel als blijk van waardering en in het kader van goed werkgeverschap;
- Overige juridische en gangbare organisatie-gerelateerde doeleinden.

Grondslagen verwerkingen:

Wij verwerken alleen persoonsgegevens als we een wettelijke grondslag hebben. Dit gebruik van persoonlijke informatie is gebaseerd op een van de onderstaande rechtsgronden, indien van toepassing:

- Om een arbeidsovereenkomst uit te voeren, te beëindigen of om stappen te ondernemen om een overeenkomst met betrokkene te sluiten dan wel via een intermediair;
- De wettelijke verplichtingen van de NVAO als werkgever;
- Uitvoering van publieke taak, opgedragen op basis van de Wet op het hoger onderwijs en wetenschappelijk onderzoek (WHW), namelijk het instellen van een commissie van deskundigen ten behoeve van een TNO of ITK en het aanwijzen van een secretaris daarvoor. Tevens het publiceren van rapporten. Het rapport, met de hierin vermelde namen van de deskundigen die het beoordelingsproces uitvoerden, is dragend voor de besluitvorming door de NVAO over een accreditatie en de verantwoording hierbij van de deskundigheid en onafhankelijkheid van de panelleden en secretarissen. Ook het verrichten van analyses en onderzoek ter verbetering van de kwaliteitszorg maken onderdeel uit van de wettelijke taak die aan de NVAO is opgedragen;
- De legitieme belangen van de NVAO, waaronder het algemeen beheer van personeelszaken (zoals het versturen van attenties), algemene bedrijfsactiviteiten, bekendmaking voor audit- en rapportagedoeleinden, interne onderzoeken, contractuele verplichtingen ten opzichte van derden, het beheer van de veiligheid van netwerken en informatiesystemen en het beschermen van de bedrijfsmiddelen van de NVAO;
- In bepaalde specifieke omstandigheden, met toestemming van de betrokkene, zoals een eventueel smoelenboek of verjaardagskalender op intranet. Op dit moment is er geen smoelenboek op het intranet van de afdeling Nederland van de NVAO. Er worden geen foto's van medewerkers geplaatst op het internet, met uitzondering van die van de directie NL. Er is een SharePoint-omgeving met privé-adresgegevens voor medewerkers onderling, op hun eigen initiatief, als een medewerker er zelf voor kiest om hieraan deel te nemen. Voor de rechtsgrond toestemming hanteert de afdeling Nederland een AVG-toestemmingsformulier;
- Toestemming kan eveneens worden gevraagd aan leden van een eerder ingestelde commissie van deskundigen om ze nogmaals te kunnen benaderen voor een volgende accreditatie of onderzoek.

3 Met wie worden jouw persoonsgegevens gedeeld?

In het geval van samenwerking met externe partijen, waarbij sprake is van de verwerking van persoonsgegevens, maakt NVAO NL afspraken over de eisen waaraan de gegevensuitwisseling moet voldoen en heeft hierover, voor zover van toepassing, een verwerkersovereenkomst afgesloten. De afdeling Nederland van de NVAO controleert deze afspraken periodiek.

Overzicht van derden met wie de afdeling Nederland persoonsgegevens deelt

Personeelsadministratie en Salarisverwerking (AFAS/Salure)	Jouw persoonsgegevens (zoals hierboven vermeld) worden beheerd in het personeelsinformatiesysteem en salarissysteem, ter ondersteuning van de uitvoering van onze taken zoals hierboven beschreven.
Evt. Arbodienst	Jouw persoonsgegevens: NAW-gegevens, BSN/wettelijk identificerend nummer, geboortedatum, privé e-mailadres, datum van indiensttreding en uitdiensttreding, functie, arbeidsduur en werkrooster, verzuimduur en verzuimdagen.
Evt. Re-integratiebureau	Persoonsgegevens en eventueel gegevens dienstverband (functie, duur dienstverband en arbeidsduur per week).
Evt. Coachingsbureau	Persoonsgegevens en eventueel gegevens dienstverband (functie, duur dienstverband en arbeidsduur per week).
Toegang tot ICT-beheerder (Acknowledge en Business Base)	Contactgegevens, zoals e-mailadres en telefoonnummer (werk).
Belastingdienst, pensioenverzekeraar	NAW-gegevens, financiële gegevens, zoals salaris- en verzekeringsinformatie, pensioeninformatie (evenals uitdraai ABP-overzicht) ondergeschikten, IBAN en/of BIC-code, loonbeslag(en), loonheffingsverklaring, IB-47 en reiskosten (woon-werkverkeer of zakelijk vervoer).
UWV	Aangifte van werkloosheid, ziekteverzuim, medische informatie, etc.
Leveranciers (attenties voor werknemers)	Op incidentele basis worden NAW-gegevens van medewerkers gedeeld voor attenties/geschenken.

Instellingen en evaluatiebureaus	Namen van leden van de commissie van deskundigen die ten behoeve van een aanvraag om een TNO of ITK ingezet zullen worden (namen en e-mail) en de zakelijke contactgegevens (naam, e-mail en telefoonnummer) van de bij de procedure betrokken behandelend medewerker van NVAO NL.
Luchtvaartmaatschappij, boekingsite, ATPI	Faciliteren van dienstreizen. Naam, zakelijke contactgegevens, geboortedatum en BSN.
CBRE gebouwenbeheer	Voornaam en achternaam t.b.v. uitgifte pas.
Dienstverlener elektronische handtekening	Naam, functie en contactgegevens.

4 Met wie worden jouw persoonsgegevens gedeeld?

NVAO NL hanteert een aantal uitgangspunten bij de verwerking van persoonsgegevens en neemt maatregelen voor een betrouwbare, behoorlijke en zorgvuldige omgang met deze gegevens. De uitgangspunten zijn verankerd in het Privacy Beleidskader van de afdeling Nederland.

Toestemming als grondslag

Voor de grondslag toestemming is expliciete, eenduidige en vrije toestemming vereist. Omdat tussen werknemer en werkgever een gezagsverhouding bestaat, mag niet zonder meer worden aangenomen dat toestemming in volledige vrijheid wordt gegeven. NVAO NL heeft daarom in het toestemmingsformulier AVG extra waarborgen getroffen om ervoor te zorgen dat medewerkers in vrijheid toestemmen of weigeren, zonder dat dit consequenties heeft. Als de verwerking plaatsvindt op basis van verleende toestemming, heb je altijd het recht deze toestemming in te trekken. Na intrekking van de toestemming zal NVAO NL jouw persoonsgegevens niet verder verwerken. Het intrekken van jouw toestemming doet niets af aan de rechtsgeldigheid van de verwerking vóór de intrekking.

Toegang tot persoonsgegevens

Bij NVAO NL hebben, naast de leidinggevenden, alleen de medewerkers van de afdeling HR toegang tot jouw persoonsgegevens. De medewerkers zelf kunnen middels de inlog op het digitale personeelsdossier zicht en grip houden op de betreffende persoonsgegevens. Personeelsdossiers zijn alleen toegankelijk middels two-factor authenticatie.

Beveiligingsmaatregelen

NVAO NL neemt maatregelen voor een betrouwbare, behoorlijke en zorgvuldige omgang met persoonsgegevens. Zo worden persoonsgegevens vertrouwelijk behandeld en zorgt NVAO NL voor passende beveiliging van de persoonsgegevens die NVAO NL onder zich heeft, in lijn met de daarvoor geldende wettelijke eisen en richtlijnen, waaronder in ieder geval de voorschriften en standaarden van de Rijksoverheid voor informatiebeveiliging. NVAO NL hanteert een informatiebeveiligingsbeleid gebaseerd op de standaarden van de Rijksoverheid.

Met ontvangers en verwerkers van persoonsgegevens worden nadere afspraken gemaakt en waar noodzakelijk een verwerkingsovereenkomst gesloten. Bij mogelijk risicovolle verwerkingen verricht NVAO NL een DPIA en worden zo nodig maatregelen om de risico's weg te nemen of te verminderen ingezet.

5 Hoe lang worden jouw persoonsgegevens bewaard?

Een van de uitgangspunten is dat persoonlijke informatie niet langer wordt bewaard dan nodig is om het doel waarvoor deze is verzameld te bereiken. Dit betekent voor medewerkers meestal dat de informatie wordt bewaard zolang er een contractuele relatie bestaat, en daarna zolang dit wettelijk vereist of toegestaan is volgens de geldende wetgeving. Zo gelden voor de afdeling HR een aantal wettelijke bewaartermijnen. Deze termijnen zijn opgenomen in de Selectielijst NVAO.

Voor panelleden (TNO, ITK) geldt eveneens dat hun gegevens worden bewaard overeenkomstig de bepalingen in de Selectielijst NVAO.

In een aanhangsel bij de Selectielijst van de NVAO hanteert NVAO NL een bewaartermijnenoverzicht voor de verwerkingen die (nog) geen onderdeel uitmaken van de Selectielijst.

6 Welke privacyrechten heb je?

Op grond van de AVG heb je de volgende rechten met betrekking tot je persoonsgegevens:

- **Recht op informatie:** NVAO NL informeert jou over de verwerking van jouw gegevens. Daarnaast heb je het recht om aan ons te vragen of jouw persoonsgegevens worden verwerkt;
- **Inzagerecht:** Je hebt het recht om inzage te krijgen in de gegevens die door de Afdeling Nederland van de NVAO worden verwerkt. Wij zullen je een overzicht geven van welke types persoonsgegevens worden verwerkt;
- **Correctierecht:** Je kunt een verzoek tot wijziging van jouw persoonsgegevens indienen bij NVAO NL als blijkt dat deze niet juist zijn of inmiddels zijn veranderd;
- **Recht om vergeten te worden:** In gevallen waar je toestemming hebt gegeven voor het verwerken van gegevens, heb je het recht om deze toestemming in te trekken en de Afdeling Nederland van NVAO NL te verzoeken om deze persoonsgegevens te laten verwijderen. In gevallen waar NVAO NL persoonsgegevens verwerkt op grond van bijvoorbeeld een wettelijke plicht, is het niet mogelijk om deze gegevens te verwijderen;
- **Recht op bezwaar:** Je hebt het recht om bezwaar in te dienen tegen de verwerking van jouw persoonsgegevens. Dit kan bijvoorbeeld als je van mening bent dat de bescherming van privacy zwaarder zou wegen dan het algemene belang van NVAO NL om persoonsgegevens te verwerken;
- **Beperking van de verwerking:** De betrokkene kan onder bepaalde omstandigheden verzoeken om de verwerking van zijn persoonsgegevens te beperken. Dit kan bijvoorbeeld als de juistheid van de gegevens betwist wordt of de verwerking onrechtmatig is;
- **Dataportabiliteit:** Overdracht van persoonsgegevens naar andere organisaties is niet van toepassing binnen de NVAO.

7 Uitoefening privacyrechten & contact gegevensbescherming

Om gebruik te maken van deze rechten, kun je per e-mail een verzoek indienen.

Het verzoek kun je richten aan de privacy office via privacy@nvao.net.

NVAO NL heeft vanaf de ontvangst van het verzoek een maand de tijd om te beoordelen of het verzoek gerechtvaardigd is. Binnen een maand laat NVAO NL je weten wat er met het verzoek zal gebeuren. Heeft NVAO NL meer tijd nodig om de gegevens te verzamelen, dan ontvang je daar ook binnen een maand bericht van. Als het verzoek niet wordt opgevolgd, heb je de mogelijkheid om bezwaar te maken bij NVAO NL of een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP). NVAO NL kan aanvullende informatie opvragen om zeker te zijn van jouw identiteit en de rechtmatigheid van het verzoek.

Ben je niet tevreden met onze antwoorden op jouw privacyvragen? Dan kun je een klacht indienen bij de AP.

Bij de NVAO, en daarbinnen bij NVAO NL, houdt de Functionaris Gegevensbescherming (FG) toezicht op de toepassing en naleving van de AVG. Heb je na het lezen van deze privacyverklaring nog vragen over hoe wij jouw persoonsgegevens gebruiken? Dan kun je via e-mail contact opnemen met de FG van de NVAO (vacature per 1/1/25).

8 Slotbepaling

Deze privacyverklaring medewerkers is vastgesteld door de directie van NVAO NL op 6 november 2024.

De privacyverklaring medewerkers van NVAO NL kan wijzigen als nieuwe ontwikkelingen, waaronder onder andere ook signalering van knelpunten of klachten van betrokkenen, daarvoor aanleiding geven. Op intranet kun je altijd de meest actuele versie van de privacyverklaring vinden. Deze privacyverklaring is voor het laatst herzien in februari 2025.

Lijst van begrippen en afkortingen

AB	Algemeen Bestuur
AP	Autoriteit Persoonsgegevens
AVG	Algemene verordening gegevensbescherming
BSN	Burgerservicenummer
CDHO	Commissie Doelmatigheid Hoger Onderwijs
CMMBO	Commissie Macrodoelmatigheid mbo
CV	Curriculum vitae
DB	Dagelijks Bestuur
FG	Functionaris Gegevensbescherming
ID	Identiteitsbewijs
ITK	Instellingstoets Kwaliteitszorg
NL	Nederland
NVAO	Nederlands-Vlaamse Accreditatieorganisatie
OCW	Ministerie van Onderwijs, Cultuur en Wetenschap
TNO	Toets nieuwe opleiding
VL	Vlaanderen
VOG	Verklaring omtrent gedrag
WHW	Wet op het hoger onderwijs en wetenschappelijk onderzoek

Colofon

Privacyverklaring (intern)

Februari 2025

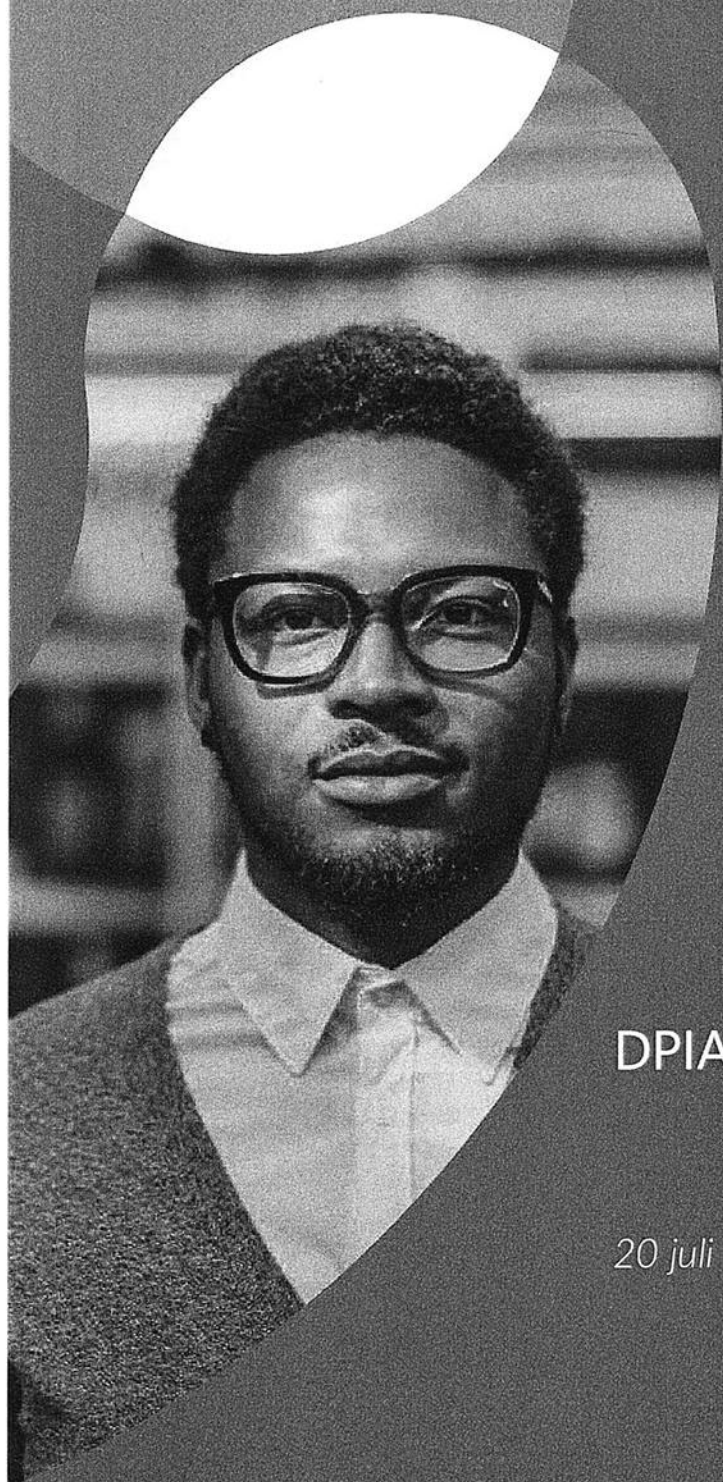
Samenstelling: NVAO Nederland



Nederlands-Vlaamse Accreditatieorganisatie
Accreditation Organisation of the Netherlands and Flanders

Parkstraat 83 2514 JG Den Haag
P.O. Box 85498 2508 CD The Hague
The Netherlands

T +31 (0)70 312 23 00
E info@nvao.net
www.nvao.net



DPIA proces NVAO

20 juli 2021

DPIA proces NVAO

20 juli 2021



1 Doel

Het doel van dit DPIA (Data Protection Impact Assessment) proces is de rollen, verantwoordelijkheden en verschillende stappen in het DPIA proces duidelijk te maken voor alle betrokkenen.

Het doel van een DPIA is om inzichtelijk te maken welke privacy risico's de verwerking met zich meebrengt voor de betrokkenen. Als een verwerking hoge risico's voor de rechten en vrijheden van betrokkenen kan inhouden is de NVAO verplicht op grond van de Algemene verordening gegevensbescherming een DPIA uit te voeren (artikel 35 AVG).

2 Rollen en verantwoordelijkheden

Medewerker	Med.	Is verantwoordelijk voor de feitelijke input vanuit het werkproces
Privacy Officer (projectleider DPIA)	PO	Begeleidt en coördineert DPIA-proces en zorgt voor AVG gerelateerde in- en output
Chief Information Security Officer	CISO	Doet check op informatiebeheer (in het bijzonder op risico's en maatregelen) en adviseert management
Dagelijks Bestuur	DB	Verwerkingsverantwoordelijke, prioritering aan de voorkant en verantwoordelijk voor vaststellen risico's
Functionaris Gegevensbescherming	FG	Advies DPIA aan verantwoordelijke (DB)
DPIA-team		Medewerker en bij voorkeur ook andere collega's uit de lijn, PO, CISO, evt. ook ketenpartners bij gegevensdeling

Mogelijke privacy-producten/output:

- Workshop DPIA – hierin neem je betrokken personen mee in wat er van hen verwacht wordt. Inventarisatie wat er nodig is om de DPIA zo efficiënt mogelijk te verrichten. Het gaat om een korte sessie van een half uur tot een uur waarin iedereen weggaat met huiswerk.
- DPIA: eventueel opdelen in verschillende sessies (grotweg)
 - Deel A: Med., CISO en PO
 - Deel B: Juridische Zaken en PO
 - Deel C: PO en CISO
- Overzicht risico's en maatregelen (per DPIA) – ten behoeve van monitoring en bijhouden van restructuur's en maatregelen zijn geaccepteerd resp. opgepakt
- Verwerkingsregister – verwerken en DPIA hierin opnemen
- Verwerkersovereenkomst of samenwerkingsafspraken
- Aanpassing van Privacyverklaring NVAO of Privacyverklaring medewerkers na afronding van het DPIA proces nodig?

Activiteit	Omschrijving	Wie	Planning
Intake	Startgesprek met Opdrachtgever (medewerker) en/of projectleider - Bepalen 'privacy producten' - Externe ondersteuning nodig?* - Samenstelling DPIA-team - Werkafspraken maken voor samenwerking project/uitvoering en privacy office - Inventarisatie benodigde informatie (o.a. pré-DPIA)	Med., PO (FG)	
Start	Startsessie (evt. op te delen) A. Workshop DPIA B. Bepalen uitgangspunten: a. Scope b. DPIA op het proces of op het systeem? C. Afstemming planning werkafspraken DPIA D. Start invullen DPIA	DPIA-team	
Uitvoering	Uitvoeren DPIA Uitvoeren (pré) DPIA op volgend (deel) ontwerp (evt. scopewijziging)	DPIA-team	
	Indien nodig: tussentijdse sessie	DPIA-team/FG	
	Opleveren concept-DPIA	DPIA-team	
Advies	Advies	FG en indien nodig CISO	
	Verwerken advies en motiveren indien advies niet wordt overgenomen	DPIA-team	
Besluitvorming	Vaststellen DPIA - Vastleggen besluitvorming mbt aanvaarding risico's en maatregelen - Bij een hoog restrisico is voorafgaande raadpleging bij de AP verplicht.	DB	
	Terugkoppeling besluit aan FG	DPIA-team	
Vervolg	Afronden overzicht risico's en beheersmaatregelen n.a.v. uitgewerkte DPIA (check na DB besluit) - Privacy Nexus	PO	
	Afstemming vervolg en evaluatie: Bv. Terugkomsessies, 2^e en volgende versies DPIA (indien van toepassing)	DPIA-team	

	- Scopewijziging tijdens implementatie - Volgende fase van een project - Ondersteuning implementatie beheersmaatregelen		
	Monitoren beheersmaatregelen Kan aanleiding zijn voor terugkomssessies	PO/FG	
Periodiek	Herijking DPIA	PO/FG op verzoek opdrachtgever	Na 3 jaar of bij verandering proces of systeem

* Als uit de pré-DPIA blijkt dat aan de verwerking hoge risico's zitten en je wil snel starten met de verwerking kan dat aanleiding zijn om externe expertise in te schakelen. Of als specifieke expertise ontbreekt mbt technische aspecten van een bepaald systeem.

3 Terminologie

DPIA: Data Protection Impact Assessment. Wordt uitgevoerd om voor nieuwe verwerkingen in een proces te onderzoeken welke data veiligheid en privacy risico's de verwerking met zich meebrengt voor de betrokkenen. Deze risico's worden gemitigeerd en/of geaccepteerd door het DB. Een DPIA wordt veelal uitgevoerd bij een nieuw proces of een grote verandering in een bestaand proces.

Pré-DPIA: Analyse die wordt gedaan om te bepalen of een DPIA nodig is of dat een kleinschalige risico analyse volstaat. Bij een pré-DPIA stel je o.a. de volgende vragen:
 Worden persoonsgegevens verwerkt, wanneer je iets wil kopen of doen?
 Welke en hoeveel persoonsgegevens worden verwerkt? Is de veiligheid daarvan geborgd?
 Kunnen persoonsgegevens worden verwijderd? Welke grondslag voor de verwerking is aanwezig? Na beantwoording van o.a. deze vragen, kan geconcludeerd worden dat bovenstaand DPIA-proces gevolgd moet worden. Het is ook mogelijk dat verwerking van persoonsgegevens een laag risico oplevert, zodat verder geen DPIA-proces hoeft te worden doorlopen.

N.B. De informatie uit een pré-DPIA (en DPIA) is dezelfde als de input die nodig is voor het Verwerkingsregister en kan dus tegelijkertijd omwille van efficiëntie.

Risico's: Risico's voor betrokkenen op informatiebeveiliging (IB) en Privacy (P) vlak. Deze komen voort uit het uitvoeren van DPIA's.

Privacy producten: Producten die naast de DPIA mogelijk moeten worden opgesteld of aangepast. Zoals bijvoorbeeld een verwerkersovereenkomst, een privacyverklaring (intern en/of extern) of afspraken over gegevensdeling.

Verwerkingsregister: De output van de DPIA kan goed worden gebruikt als input van het verwerkingsregister. Het is verplicht om een register van DPIA's (of Pré-DPIA als er geen DPIA nodig wordt gevonden) bij te houden, deze kunnen als bijlage in het verwerkingsregister worden opgenomen.



GEB: Gegevensbeschermingseffectbeoordeling (GEB) is de Nederlandse vertaling van een DPIA. Hiervoor is een Rijksmodel ontwikkeld, het Rijksmodel GEB (DPIA). De NVAO hanteert een iets aangepaste vorm van dit Rijksmodel GEB (DPIA).

4 Slotbepaling

Het Privacy Office beheert dit document. Na goedkeuring op 20 juli 2021 door het DB treedt dit document in werking.

Colofon

DPIA Proces

20 juli 2021

Samenstelling: NVAO



Nederlands-Vlaamse Accreditatieorganisatie
Accreditation Organisation of the Netherlands and Flanders

Parkstraat 83 2514 JG Den Haag
P.O. Box 85498 2508 CD The Hague
The Netherlands

T +31 (0)70 312 23 00
E info@nvao.net
www.nvao.net

Memo DPIA Quick Scan

1. Inleiding

Vraagstelling: Wanneer moet de NVAO een Data Protection Impact Assessment, afgekort DPIA, doen?

De AVG verplicht organisaties dat zij *accountable* zijn bij de verwerking van persoonsgegevens. Accountable zijn houdt kort gezegd in dat je als organisatie weet wat je aan persoonsgegevens hebt, weet wat je ermee doet, weet waar je risico's liggen, uit kan leggen hoe je met die risico's omgaat en die uitleg ook vastlegt. De organisatie kan aan het beginsel van accountability op verschillende manier inhoud en vorm geven. Eén van de AVG-instrumenten om inzicht te krijgen in de risico's die de verwerkingen van persoonsgegevens met zich brengen is de DPIA.¹ Maar hoe nuttig ook, de DPIA kost tijd en capaciteit. Het instrument moet alleen dan worden ingezet als het ook echt nodig is.

Of en wanneer een DPIA moet worden verricht, is een vraag die de verwerkingsverantwoordelijke zich mag en ook moet stellen. Bij de inwerkingtreding van de AVG werd door veel organisaties gevreesd dat alle bestaande verwerkingen (opnieuw) door de PIA-molen moesten. Dat is zeker niet het geval. Het uitgangspunt is dat een PIA moet worden gedaan bij nieuwe verwerkingen met een hoog risico. Voor bestaande verwerkingen ging de AVG ervan uit dat de PIA's al waren gedaan. En daar zit ook een deel van de oorzaak van de onduidelijkheid: dat was vaak niet het geval. Veel organisaties hebben de risico's van de bestaande verwerkingen vaak nog niet in kaart gebracht, het welbekende achterstallige onderhoud.

Deze notitie heeft als doel de NVAO een handreiking te geven om te bepalen:

- wanneer de NVAO verplicht is een DPIA te verrichten
- hoe dit in de organisatie ingebed zou kunnen worden
- wat de risico's voor de NVAO zijn als er geen DPIA is verricht.

2. Wanneer is de NVAO verplicht een DPIA te verrichten?

Een PIA is niet verplicht als de gegevensverwerking:

- Waarschijnlijk geen hoog privacyrisico oplevert.
- Sterk lijkt op een andere gegevensverwerking waarvoor al een DPIA is uitgevoerd.
- Wordt geregeld door een andere Europese of nationale wet en er bij de totstandkoming van deze wet al een DPIA is uitgevoerd. Tenzij de AP oordeelt dat er toch een PIA nodig is.
- Op een lijst staat van verwerkingen waarvoor een DPIA niet verplicht is. De AVG geeft de toezichthouders de mogelijkheid om zo'n lijst op te stellen, maar dit is niet verplicht. De AP heeft geen gebruik gemaakt van de mogelijkheid een dergelijke lijst op te stellen.

Wanneer is een DPIA wél verplicht?

Voor Nederlandse overheidsorganisaties geldt dat een DPIA moet worden uitgevoerd:

- als de verwerking op de lijst van de toezichthouder staat;²
 - bij de ontwikkeling van beleid en regelgeving die betrekking hebben op verwerkingen van persoonsgegevens of waaruit verwerkingen van persoonsgegevens voortvloeien;
 - bij voorgenomen verwerkingen van persoonsgegevens die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van betrokkenen (de mensen van wie de organisatie gegevens verwerkt). Dit is bepaald in artikel 35 AVG.
- Het bepalen van de omvang van het waarschijnlijke privacyrisico is niet eenvoudig. De werkgroep van Europese privacytoezichthouders (WP29) heeft een lijst opgesteld van 9

¹ Als we het in de AVG-context hebben over PIA wordt de DPIA (Data Protection Impact Assessment) bedoeld. In Nederland is dit de GEB (Gegevensbeschermingseffectbeoordeling) bedoeld. Voor het gemak gebruik ik hier verder de term DPIA.

² <https://autoriteitpersoonsgegevens.nl/nl/zelf-doen/data-protection-impact-assessment-dpia#voor-welke-soorten-verwerkingen-is-het-uitvoeren-van-een-dpia-verplicht-6667>

criteria om organisaties hierbij te helpen. Alle criteria samengevat moet je een DPIA doen als één of meer van de volgende verwerkingen sprake is, nl als je:

- Bijzondere of gevoelige persoonsgegevens verwerkt.
⇒ De aard van de gegevens maakt het risico hoog.
- Veel gegevens verwerkt die gevoelig kunnen zijn.
⇒ De hoeveelheid gegevens maakt het risico hoog.
- Systematische data verzamelt, koppelt, gebruikt voor besluitvorming met (mogelijk) nadelige effecten voor individuen of op een andere manier wil gaan gebruiken dan oorspronkelijk was bedacht.
⇒ Het gebruik van de gegevens maakt het risico hoog.
- Nieuwe technologie gebruikt om de verwerking mee te gaan doen. Het feit dat je een systeem dat van jezelf is, vervangt door een extern ontwikkeld cloud systeem is hier een voorbeeld van.
⇒ De verandering in de technologische verwerkingswijze maakt het risico hoog.

3. Wel of geen DPIA bij de NVAO?

De AP heeft een stroomschema ontwikkeld dat goed te gebruiken is, maar nog niet erg inhoudelijk is. Daarom heb ik een DPIA Quicksan ontwikkeld, waarbij alle punten kort zijn weergegeven. Deze Quicksan zou als uitklaplijst kunnen worden meegenomen bij nieuwe projecten/beleidsnotities e.d. waarbij persoonsgegevens (gaan) worden verwerkt.

	Criterion	Ja/nee	Wel/niet van toepassing	Toelichting
1.	Er worden persoonsgegevens verwerkt			
2.	Er is sprake van nieuwe wetgeving/nieuw beleid			
3.	Er is al een PIA op de verwerking verricht			
4.	Verwerking staat op de verplichte PIA lijst van AP: - Heimelijk onderzoek - Zwarte lijsten - Fraudebestrijding - Creditscores - Financiële situatie - Genetische persoonsgegevens - Gezondheidsgegevens - Samenwerkingsverbanden (gevoelige/bijzondere persoonsgegevens) - Cameratoezicht - Controle werknemers - Locatiegegevens - Communicatiegegevens - Internet of things - Profileren - Biometrische gegevens³ - Monitoring en beïnvloeding van gedrag			
5.	Er is mogelijk sprake van hoog risico:			
	a) Er worden bijzondere of gevoelige persoonsgegevens verwerkt			

³ UAVG: Enkel als de verwerking noodzakelijk is voor authenticatie of beveiligingsdoeleinden is de verwerking van biometrische gegevens toegestaan. NB Recente jurisprudentie: Manfield: als ze een PIA hadden gedaan en hadden proportionaliteit en subsidiariteit hadden onderzocht en beschreven, had het wellicht wel gekund.

	b) Er worden veel gegevens verwerkt die gevoelig kunnen zijn.			
	c) Er worden systematische data verzameld, gekoppeld, gebruikt voor besluitvorming met (mogelijk) nadelige effecten voor individuen of op een andere manier wil gaan gebruiken dan oorspronkelijk was bedacht.			
	d) Er wordt een nieuwe technologie gebruikt om de verwerking mee te gaan doen.			
	e) Er worden middelen (digitale handtekening, biometrische gegevens, identificatienummers, BSN) gebruikt die specifiek zijn gericht op het identificeren van personen			
	f) Blokkering van een recht, dienst of contract			
	g) De gegevens worden gedeeld met derden of openbaar gemaakt.			
	h) Is er in het verleden maatschappelijke weerstand geweest tegen vergelijkbare projecten?			

4. Borging verrichten van een DPIA bij de NVAO

Hoe kan de NVAO ervoor zorgen dat er bij voorgenomen verwerkingen of nieuw beleid of regelgeving de vraag of een DPIA al dan niet moet worden verricht wordt meegenomen? Deze vraag komt er eigenlijk op neer hoe de NVAO "privacy by design" kan gaan werken.

Als je het onderwerp privacy vanaf het begin van de ontwikkeling van nieuw beleid, een nieuw systeem of proces hebt meegenomen werk je conform het AVG principe "privacy by design".

Elke organisatie heeft zijn of haar eigen werkprocessen. Het is lastig om een algemeen sjabloon los te laten hoe je privacy by design goed meeneemt. Je zult dit in de interne processen en werkwijzen moeten meenemen. Hoe is privacy het beste in te passen in deze organisatie?

Concrete oplossingsrichtingen voor de NVAO:

- In beleidsnota, business cases, projectplannen altijd een kopie Privacy of Gegevensbescherming opnemen en hierin een verwijzing opnemen naar de checklist. Bij positieve beantwoording van vraag 1, door met de volgende vraag en dan de privacy check bij JZ neerleggen;
- Regelmatig in overleggen onderwerp vanuit het perspectief van privacyvraagstuk benaderen;
- Vraag om advies bij JZ of FG. Betrek ze tijdig bij het proces. Privacy hoeft geen stopper te zijn, het kan juist een asset zijn.

Wat moet er in ieder geval gebeuren:

- DPIA register aanleggen;
- DPIA procesbeschrijving opstellen;
- Meenemen DPIA-aanpak in Privacy Beleid en Governance.

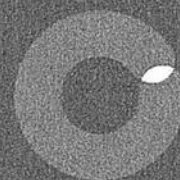
5. Risico's voor NVAO als er geen DPIA is gedaan

Als er geen DPIA is uitgevoerd en dat evident wel had gemoeten, kan de Autoriteit persoonsgegevens de organisatie een bestuurlijke boete opleggen.⁴ Uiteraard kan de organisatie ervoor kiezen om geen DPIA te verrichten. Die beslissing moet op grond van het beginsel van accountability dan wel een

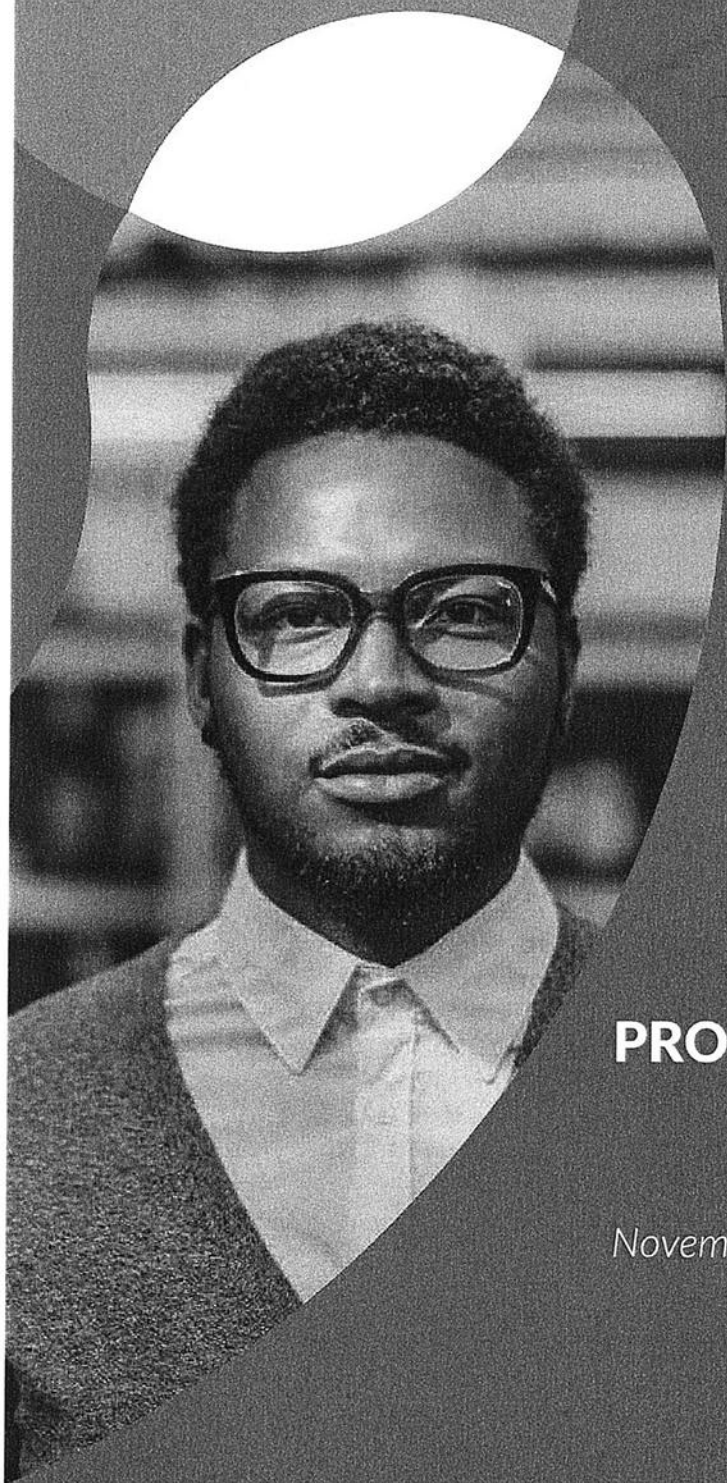
⁴ Boetebeleidsregels Autoriteit Persoonsgegevens 2019, Stort. 2019, 14586.

beredeneerde keuze zijn van de verwerkingsverantwoordelijke. Het is een beslissing die op managementniveau genomen moet worden, inclusief reserveringen voor boetes.

Het is altijd vervelend om de boetekwestie op te werpen, beter is te kijken naar de voordelen die een DPIA een organisatie kan brengen. Het kan een organisatie heel bewust maken van de risico's van bepaalde verwerkingen, het kan tijd en geld besparen omdat privacy geen stopper wordt. Als een DPIA op tijd is gedaan kunnen bepaalde ICT-aspecten meteen worden meegenomen bij de inrichting van de systemen in plaats van achteraf. Juist die bijsturen en changes zijn zeer bewerkelijk en kostbaar.



NVAO

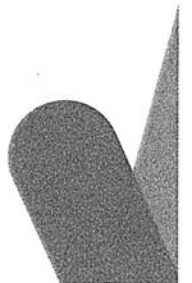


PROTOCOL DATALEKKEN

November 2019

Protocol datalekken

November 2019



Inleiding

In een organisatie waarin veel persoonsgegevens worden verwerkt vinden datalekken plaats. Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij een organisatie zonder dat dit de bedoeling is van deze organisatie. Een deel van de datalekken moet bij de Autoriteit Persoonsgegevens (AP) worden gemeld en in bepaalde gevallen moet ook de betrokkene worden geïnformeerd. Alle datalekken moeten worden geregistreerd.

De AVG bepaalt dat datalekken direct, binnen 72 uur, gemeld moeten worden aan de Autoriteit Persoonsgegevens ('AP'), tenzij het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Daarnaast moet het datalek ook aan de betrokkenen gemeld worden indien het waarschijnlijk een groot risico voor de rechten en vrijheden van de betrokkenen met zich meebrengt.

Aan de beantwoording van bovenstaande vraag moet een zorgvuldige (belangen)afweging voorafgaan. Hierbij is bijvoorbeeld de aard en de omvang van de persoonsgegevens die gelect zijn van belang. Als er bijzondere persoonsgegevens, zoals gegevens over gezondheid, gelect zijn, dan is de melding meestal noodzakelijk.

Dit protocol datalekken is bedoeld als hulpmiddel voor de beantwoording van de vraag of er sprake is van een datalek en of dit gemeld moet worden.

Inhoud

1	Wat is een datalek?.....	5
2	Contactpersoon aanwijzen.....	5
3	Informeren medewerkers.....	5
4	Uitvoeren van het stappenplan Datalekken.....	5
4.1	Stappenplan datalekken.....	6

1 Wat is een datalek?

Er is sprake van een datalek als er een inbreuk in verband met persoonsgegevens heeft plaatsgevonden. Alleen een dreiging of een tekortkoming in de beveiliging is niet voldoende; er moeten daadwerkelijk persoonsgegevens gelekt zijn.

Onder een datalek verstaat de AP persoonsgegevens die gelekt of vernietigd zijn als gevolg van een beveiligingsincident. Bij het lek zijn persoonsgegevens blootgesteld aan verlies of onrechtmatige verwerking. Bij verlies zijn de persoonsgegevens er niet meer. Onder onrechtmatige verwerking vallen bijvoorbeeld onbevoegde kennisneming, wijziging, aantasting of de verstrekking daarvan.

Voorbeelden van inbreuken in verband met persoonsgegevens kunnen zijn:

- kwijtraken van een USB -stick
- diefstal van een laptop
- inbraak door een hacker
- persoonsgegevens per ongeluk gepubliceerd
- hacking, malware of fishing
- persoonsgegevens aan verkeerde persoon verstuurd
- calamiteiten zoals brand in een datacentrum

2 Contactpersoon aanwijzen

De organisatie moet een eigen contactpersoon aanwijzen aan wie eventuele datalekken gemeld moeten worden. Dit kan bijvoorbeeld een directeur, bestuurslid of de Functionaris Gegevensbescherming zijn. Voor de NVAO is dit JZ als privacy officers, JZ maakt een eerste inschatting en overlegt met FG. Het vermoeden (op basis van formulier Quick Scan) van een datalek wordt ook voorgelegd aan de directeur Nederland/Vlaanderen, zo nodig ook aan ICT/Communicatie. In deze tekst wordt steeds gesproken over Contactpersoon.

3 Informeren medewerkers

Medewerkers binnen de organisatie moeten zich er van bewust te zijn dat als er sprake is van een (eventueel) datalek, zij dit mogelijke datalek direct (diezelfde dag nog) moeten melden bij de Contactpersoon (JZ), zodat deze tijdig kan onderzoeken (aan de hand van formulier quick scan melden datalekken) of sprake is van een datalek en zo ja het datalek kan melden bij de Autoriteit Persoonsgegevens. Medewerkers moeten ook bekend zijn met het in dit protocol opgenomen stappenplan.

4 Uitvoeren van het stappenplan Datalekken

De binnen de organisatie aangewezen Contactpersoon draagt zorg voor de invoering en naleving van het hieronder opgenomen stappenplan Datalekken. Dit protocol is opgezet als stappenplan, met opeenvolgende stappen die doorlopen dienen te worden. In de praktijk zal het evenwel ook voorkomen dat - afhankelijk van de aard van het incident - sommige stappen elkaar zeer snel opvolgen of deels samenvallen. Ter illustratie: stappen 2-3-4-5 volgen elkaar snel op of vallen samen als na een melding de eerste analyse uitwijst dat zeer waarschijnlijk sprake is van een datalek, eea is kort afgestemd met FG en directie en eerste inschatting risico's is gemaakt, en conclusie is melden.

4.1 Stappenplan datalekken

	Processtappen	Activiteit	Actoren	Wanneer
0	Er wordt een (mogelijk) datalek ontdekt	Meld intern via de mail (privacy@nvao.net) een melding van (mogelijke) datalek. Informeert de verantwoordelijke Contactpersoon en geef bij de melding aan om wat voor soort incident het gaat (bv onjuiste adressering, verlies documenten, etc).	Medewerker die het ontdekt	
1	Beoordeel mogelijk datalek, eventueel adviesFG	Medewerker vult formulier quick scan melden datalekken in. Onderzoek beveiligingsincident aan de hand van formulier quick scan melden datalekken.	Quick scanformulier wordt ingevuld door medewerker en vervolgens beoordeeld door Contactpersoon	Z.s.m.
2		Voorlopige uitkomsten: • Er is een datalek: Inbreuk in de zin van de AVG, beveiligingsincident wordt geclassificeerd als datalek. Er is geen inbreuk op de AVG. • Er is een meldplichtig datalek: Melden AP is niet verplicht, niet waarschijnlijk dat inbreuk een risico inhoudt voor rechten en vrijheden van natuurlijke personen. Melden aan AP binnen 72 uur nadat de organisatie met redelijke zekerheid heeft vastgesteld dat sprake is van een datalek. Onderzoek of er persoonsgegevens verloren zijn gegaan of onrechtmatig gebruikt kunnen worden. Beoordeel wie of welke afdelingen binnen de organisatie hierbij betrokken zijn. Beoordeel of er andere organisaties of een verwerker*betrokken is bij het incident. Zo ja dan dient deze bij het proces betrokken te worden.	In samenspraak met FG en directeur NL/VL en IT	
3	Bestrijdt het datalek	Stop het datalek als het nog kan. Neem andere maatregelen om het datalek en de daaruit voortvloeiende schade te beperken. Leg de acties van de genomen maatregelen vast in het dossier (formulier van contactpersoon	Contactpersoon, medewerker, IT en directeur NL/VL Medewerker heeft formulier ingevuld (zie stap 2), JZ controleert, afstemmen met FG	Z.s.m.

4	Vaststellen impact datalek	Onderzoek het datalek en de gevolgen daarvan. Onderzoek de aard van de gegevens die gelekt zijn. Bijv. gezondheidsgegevens, wachtwoorden, gegevens over financiële situatie of die kunnen leiden tot stigmatisering/misbruik. Onderzoek de omvang van de gelekte gegevens. Beoordeel welke impact het lek kan hebben op de betrokken personen. Stel vast wat de nadelige gevolgen kunnen zijn.	Contactpersoon in overleg met FG	
5	Vaststellen meld- en herstelaanpak	Bepaal aanpak/ informeren AP (https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken) Bepaal aanpak/informeren betrokkenen Bepaal acties voor nazorg betrokkenen Bepaal acties voor belang van de organisatie Bepaal acties voor verbetering	Afstemming door contactpersoon met FG en directeur NL/VL over aanpak en afweging melding AP Aanpak/informeren betrokkenen na afstemming hierover door FG en directeur. Belang organisatie en acties verbeteren beveiliging door contactpersoon i.o.m. FG, directeur NL/VL, zo nodig IT en Communicatie	Melding AP binnen 72 uur nadat met redelijke zekerheid is vastgesteld dat sprake is van een datalek
6	Registreer datalek	Register datalekken	Contactpersoon	Na beoordeling datalek en naarmate inbreuk zich ontwikkelt
7	Melden betrokkenen***	Melding via bijvoorbeeld brief Meedelen wat er is gebeurd, welke persoonsgegevens getroffen zijn en wat de mogelijke gevolgen van het datalek kunnen zijn. Informeren over de maatregelen die de organisatie neemt en die de betrokkene zelf kan nemen om schade te voorkomen.	Contactpersoon in samenspraak met FG, directeur NI/VL, i.o.m. Communicatie Brief uit namens bestuur. Contactpersoon en FG Communicatie	Z.s.m. na melding AP

8	Informeren anderen	Informeer Bestuur Informeer politieke leiding/departement (bij grote impact) Informeer overigen na melding AP	Contactpersoon dtv Directeur NL/VL Directeur NL/VL en/ of bestuurder, afhankelijk van impact	Z.s.m. na melding en evt. al eerder na vaststelling datalek
9	Nadere analyse en evaluatie melding		Contactpersoon, Directeur NL/VL, IT, Communicatie	Na melding AP en betrokkenen
10	Uitvoeren vervolgacties, verbeter-of herstelwerkzaamheden	Herstel het datalek Verbeter de beveiliging Lever nazorg aan de betrokkenen	IT, in overleg met contactpersoon en FG Contactpersoon	
11	Optimaliseer het beveiligings- en het datalek-proces	<i>lessons learned</i> Registreer, evalueer en verbeter de beveiliging en het proces inzake melding datalekken	Contactpersoon, FG, Directeur NL/VL, Bestuur, Communicatie	
12	Sluiting melding		Contactpersoon	Na afronding herstelwerkzaamheden

** Verwerker*

Het kan gebeuren dat het datalek optreedt bij de verwerker. De organisatie is en blijft (als verwerkingsverantwoordelijke) altijd verantwoordelijk voor het datalek bij de verwerker. In dat geval moet dus hetzelfde stappenplan worden afgewerkt. De verwerker zal bij de stappen betrokken moeten worden. In de de verwerkersovereenkomst wordt afgedwongen (opgenomen in standaard verwerkersovereenkomst van de NVAO) dat de verwerker eventuele datalekken onverwijld meldt bij de organisatie en de organisatie helpt bij het beoordelen of er gemeld moet worden en de afwikkeling van het datalek. Belangrijk is dat de verwerker niet buiten de organisatie om een datalek meldt bij de Autoriteit Persoonsgegevens. De verwerker moet verder alle redelijke instructies van de organisatie opvolgen.

*** Melden AP*

Melding aan de Autoriteit persoonsgegevens kan alleen achterwege blijven indien het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Of hiervan sprake is hangt mede af van de aard, omvang en gevoeligheid van de geleepte persoonsgegevens en het gemak waarmee personen kunnen worden geïdentificeerd, de ernst van de gevolgen voor de personen en eventueel bijzondere kenmerken. Indien bijvoorbeeld uitsluitend de adresgegevens zijn geleept van een kleine groep betrokkenen, dan is het onwaarschijnlijk dat er sprake is van een hoog risico. Dat is wellicht anders indien de adresgegevens in combinatie met andere gegevens zijn geleept. Bij de afweging van het risico voor de rechten en vrijheden van de betrokken zal altijd de Functionaris Gegevensbescherming betrokken moeten worden.

**** Melden betrokkenen*

Wanneer het datalek waarschijnlijk meebrengt dat sprake is van een groot risico voor de rechten en vrijheden van de betrokkenen, moet het datalek ook aan de betrokkenen worden gemeld. Het risico zal bijvoorbeeld moeten worden beoordeeld aan de hand van de aard en de hoeveelheid van de geleepte gegevens. Als er persoonsgegevens van gevoelige aard geleept zijn, zal het lek in ieder geval gemeld moeten worden aan de betrokkenen. Bij de afweging van het risico voor de rechten en vrijheden van de betrokkenen zal altijd de Functionaris Gegevensbescherming betrokken moeten worden.

Colofon

Protocol datalekken

November 2019

Samenstelling: NVAO

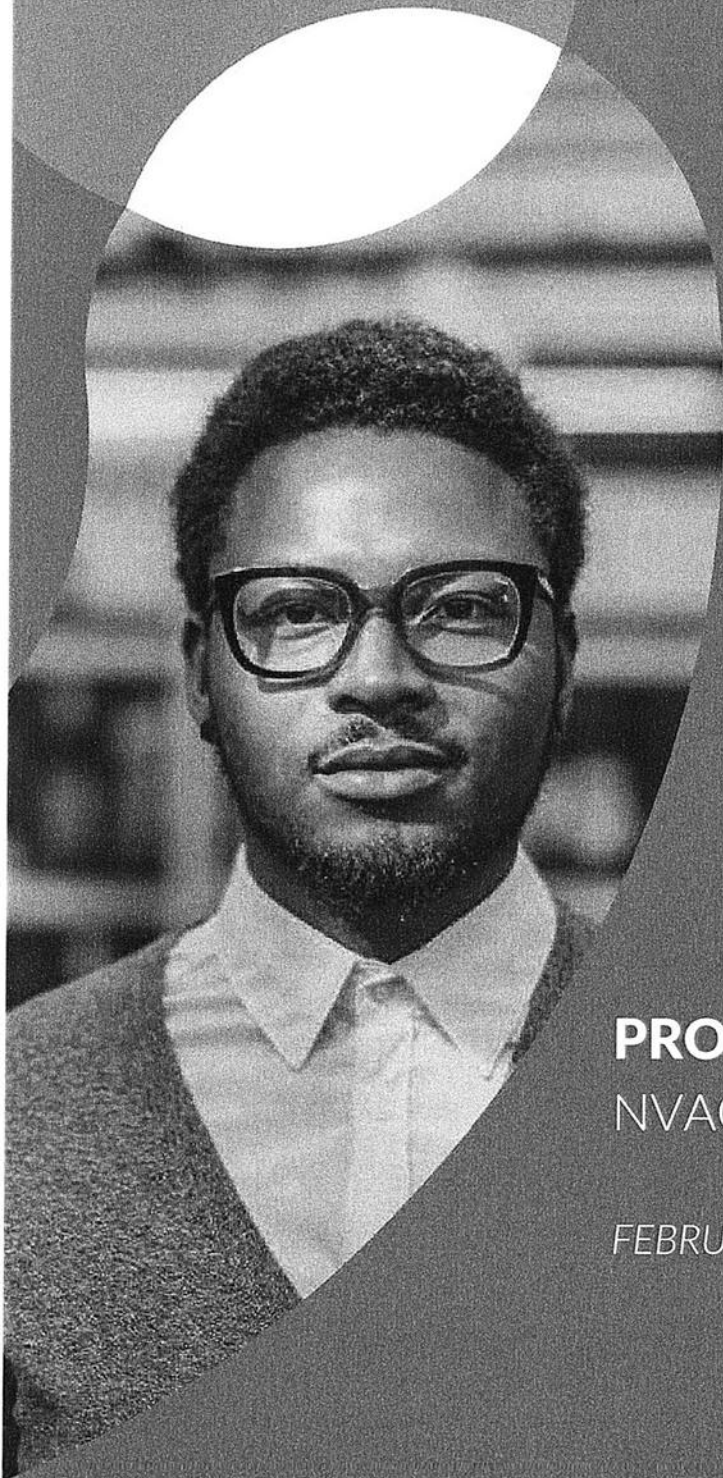


Nederlands-Vlaamse Accreditatieorganisatie
Accreditation Organisation of the Netherlands and Flanders

Parkstraat 83 2514 JG Den Haag
P.O. Box 85498 2508 CD The Hague
The Netherlands

T +31 (0)70 312 23 00
E info@nvao.net
www.nvao.net

10



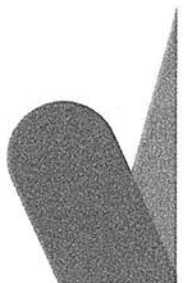
PROTOCOL DATALEKKEN
NVAO NEDERLAND

FEBRUARI 2025

PROTOCOL DATALEKKEN

NVAO NEDERLAND

FEBRUARI 2025



Inleiding

In dit protocol is beschreven wat een beveiligingsincident of datalek is, hoe je dit kunt herkennen en hoe we hierbij handelen binnen de Nederlands-Vlaamse Accreditatieorganisatie, afdeling Nederland (NVAO NL). Gekozen is om te werken vanuit één stappenplan en een gezamenlijke aanpak voor zowel beveiligingsincidenten als datalekken vanwege de nauwe samenhang tussen deze twee situaties.

Op 1 januari 2016 is de meldplicht datalekken in werking getreden via de Wet bescherming persoonsgegevens (Wbp). NVAO NL is als verwerker van persoonsgegevens verplicht om datalekken te melden bij de Autoriteit Persoonsgegevens (AP). Per 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) van toepassing. Dat betekent dat in de hele Europese Unie (EU) dezelfde privacywetgeving geldt. De Wbp geldt vanaf dat moment niet meer. De AVG geeft aan dat een persoonsgegeven elk gegeven is over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Dat het om een natuurlijke persoon moet gaan, houdt in dat gegevens van organisaties geen persoonsgegevens zijn. Er zijn vele soorten persoonsgegevens. Voor de hand liggende gegevens zijn iemands naam, adres en woonplaats, etc.

Van een datalek is sprake in geval van een inbreuk op de beveiliging die leidt tot verlies van persoonsgegevens of tot de mogelijkheid dat er als gevolg van de inbreuk op de beveiliging persoonsgegevens onrechtmatig worden verwerkt.

Met deze procedure geeft de NVAO uitvoering aan het vastgestelde privacybeleid van afdeling Nederland.

Inhoud

1	Wat is een datalek?	5
2	Wat is een beveiligingsincident?	6
3	Een voorbeeld van een datalek dat tevens een beveiligingsincident kan zijn.....	7
4	Rollen en verantwoordelijkheden	8
4.1	IT en ISO	8
4.2	Directie.....	8
4.3	Communicatie.....	8
4.4	HR	8
5	Stappenplan beveiligingsincident / datalek.....	9
5.1	Uitvoeren van het stappenplan beveiligingsincidenten/datalekken.....	9
6	Slotbepaling	13
	Lijst van begrippen en afkortingen.....	14

1 Wat is een datalek?

Volgens de AP, de Nederlandse privacytoezichthouder, is een datalek "een inbreuk op de beveiliging van persoonsgegevens." Dit houdt in dat er sprake is van een situatie waarbij persoonsgegevens onbedoeld of onrechtmatig zijn vernietigd, verloren, gewijzigd of toegankelijk zijn gemaakt. Ook het onrechtmatig verwerken van persoonsgegevens valt hieronder.

Een datalek volgens de AP kan dus betrekking hebben op:

- **Onbeveiligde databases:** Een organisatie slaat klantgegevens op in een onveilige database, waardoor deze toegankelijk is voor onbevoegden;
- **Phishing-aanvallen:** Werknemers klikken op een phishing-link en geven inloggegevens vrij, waardoor hackers toegang krijgen tot gevoelige bedrijfsinformatie;
- **Verlies van apparaten:** Een laptop of smartphone met klantinformatie wordt gestolen of verloren, waardoor de gegevens in verkeerde handen kunnen vallen;
- **Publicatie van documenten:** Per ongeluk gevoelige documenten worden online gepubliceerd of op een openbaar platform gedeeld;
- **E-mailfouten:** Vertrouwelijke informatie wordt per ongeluk naar de verkeerde ontvanger gemaïld.

2 Wat is een beveiligingsincident?

Een beveiligingsincident is een gebeurtenis die de beveiliging van informatie of systemen in gevaar kan brengen. Dit kan bijvoorbeeld gaan om ongeautoriseerde toegang tot gegevens, malware-infecties, datalekken of fysieke inbraken. Het doel van het identificeren en rapporteren van dergelijke incidenten is om de impact te minimaliseren en te zorgen voor een snelle reactie om verdere schade te voorkomen. Binnen NVAO wordt gebruikgemaakt van protocollen en procedures om deze incidenten te beheren en te onderzoeken.

We spreken van een beveiligingsincident als bij een fout of lek geen persoonsgegevens betrokken zijn. Als bijvoorbeeld een laptop zoekraakt, maar de toegang ertoe door beveiliging niet mogelijk is, spreken we van een beveiligingsincident. Bij een datalek gaat het om mogelijke, niet toegestane toegang van derden tot persoonsgegevens. Datalekken worden meestal veroorzaakt door menselijk handelen.

Phishing: Pogingen om gebruikers te misleiden om persoonlijke informatie te delen via nep-e-mails of websites.

Malware-infectie: Verspreiding van kwaadaardige software die systemen kan beschadigen of gegevens kan stelen.

Inbraak: Fysieke toegang tot een gebouw of serverruimte zonder toestemming, met als doel gegevens te stelen of systemen te saboteren.

Denial-of-Service (DoS) aanval: Een aanval die een systeem of netwerk overweldigt met verkeer, waardoor het niet meer bereikbaar is voor legitieme gebruikers.

Ongeautoriseerde software-installatie: Het installeren van niet-goedgekeurde applicaties op bedrijfsapparatuur, wat kan leiden tot beveiligingsrisico's.

Deze incidenten kunnen ernstige gevolgen hebben voor de integriteit, vertrouwelijkheid en beschikbaarheid van informatie.

3 Een voorbeeld van een datalek dat tevens een beveiligingsincident kan zijn.

Een bekend voorbeeld van een datalek dat ook als een beveiligingsincident wordt beschouwd, is de datalek bij Equifax in 2017. Tijdens dit incident werden persoonlijke gegevens van ongeveer 147 miljoen mensen blootgesteld, waaronder namen, geboortedata, sociale zekerheidsnummers en rijbewijsnummers.

Het beveiligingsincident werd veroorzaakt door een kwetsbaarheid in de software die Equifax gebruikte, en het bedrijf had de update om deze kwetsbaarheid te verhelpen niet op tijd geïmplementeerd. Het datalek had aanzienlijke gevolgen voor de getroffen individuen en leidde tot rechtszaken, boetes en versterking van regelgeving rondom data- en informatiebeveiliging. Dit is een duidelijk geval waarin een datalek het resultaat was van een beveiligingsincident.

4 Rollen en verantwoordelijkheden

4.1 IT en ISO

Een Information Security Officer (ISO) ontwikkelt en implementeert informatiebeveiligingsbeleid, voert risicoanalyses uit, en verzorgt trainingen. Hij begeleidt Security Awareness-projecten en houdt toezicht op de naleving van beveiligingsmaatregelen. Daarnaast adviseert hij de directie over informatiebeveiligingskwesties.

4.2 Directie

Eventuele incidenten en datalekken worden voorgelegd aan de directie en, indien nodig, door hun tussenkomst voorgelegd aan het bestuur.

4.3 Communicatie

Interne- en externe communicatie.

4.4 HR

HR is betrokken bij de borging van het beleid rondom datalekken door direct bij indiensttreding afspraken te maken met het Privacy Office (PO), zodat awareness over de belangrijkste zaken rondom privacy en het voorkomen van datalekken direct vanaf de start bij de NVAO wordt meegegeven.

5 Stappenplan beveiligingsincident / datalek

Het informeren van medewerkers over datalekken/beveiligingsincidenten is een belangrijk onderdeel van een goed gegevensbeschermingsbeleid. Dit zorgt ervoor dat iedereen in de organisatie weet hoe te handelen bij een datalek/beveiligingsincident, wat de risico's zijn, en wat de procedures zijn voor het melden van een dergelijk incident.

Medewerkers binnen de organisatie moeten zich ervan bewust zijn dat, wanneer er sprake is van een (mogelijk) datalek/beveiligingsincident, zij dit zo snel mogelijk melden bij de PO en ISO. Om de PO en ISO in staat te stellen een beoordeling hierop uit te voeren, werkt de NVAO met een Quickscan-formulier. Dit formulier helpt de PO en ISO bij het antwoord op de vraag of er sprake is van alleen een beveiligingsincident, dan wel dat er persoonsgegevens bij betrokken zijn. Er is in dat geval (mede) sprake van een datalek.

Wanneer er sprake is van een datalek, wordt door de PO, in afstemming met de Functionaris Gegevensbescherming (FG) en directie, vastgesteld of een meldplichtig datalek aan de orde is. Wanneer dit het geval is, wordt er binnen 72 uur een melding gemaakt bij de AP. In paragraaf 5.1 is een volledig stappenplan opgenomen met een beschrijving van hoe te handelen bij een datalek.

5.1 Uitvoeren van het stappenplan beveiligingsincidenten/datalekken

Processtappen	Activiteit	Actoren	Wanneer
0	Er wordt een (mogelijk) beveiligingsincident of datalek ontdekt.	1a. Maak intern via de mail (privacy@nvao.net) een melding van (mogelijke) datalek + maak een melding bij IT (ICT). Geef bij de melding aan om wat voor soort incident het gaat (bijv. onjuiste adressering, verlies documenten, laptop, etc.). 1b. Stop het beveiligingsincident en/of datalek als het nog kan. 1c. Neem andere maatregelen om het beveiligingsincident en/of datalek en de daaruit voortvloeiende schade te beperken. 2. Zorg dat je bereikbaar blijft.	Betrokken medewerker. PO, ISO en directie, zo nodig in afstemming met FG. z.s.m.
1	Formulier Quickscan invullen.	De medewerker vult het Quickscan-formulier in en stuurt dit naar de ISO en PO.	Betrokken medewerker. z.s.m.
2	Quickscan-analyse	1. De ISO en PO analyseren het Quickscan-formulier en stellen vast of er sprake is van een incident/datalek. 2. Eerste registratie in Privacy Nexus.	ISO/PO, zo nodig in afstemming met de FG. z.s.m.
		Voorlopige inschatting 1. Er is geen sprake van een beveiligingsincident/datalek. 2a. Er is sprake van een beveiligingsincident, maar er zijn	

3	Vaststelling beveiligingsincident/ datalek	geen persoonsgegevens bij betrokken. 2b. Er is sprake van een beveiligingsincident, maar er zijn wel persoonsgegevens bij betrokken (datalek). Vervolgacties bij alleen een beveiligingsincident door IT, conform IB-beleid en beheersmaatregelen. Vervolgstappen bij een datalek: Vervolg het stappenplan met stap 4.	PO/JZ, eventueel in afstemming met ISO en FG.	Binnen 24 uur na het ter kennis brengen van het incident bij ISO/PO.
4	Vaststellen van de impact van het beveiligingsincident/ datalek.	1. Onderzoek het beveiligingsincident/datalek en de gevolgen daarvan. 2. Onderzoek de aard van de gegevens die gelekt zijn, bijv. persoonsgegevens of wachtwoorden. 3. Onderzoek de omvang van de geleepte gegevens. 4. Beoordeel welke impact het lek kan hebben op de betrokken personen. 5. Stel vast wat de nadelige gevolgen kunnen zijn. 6. Bepaal of er derden (bijvoorbeeld een verwerker) bij betrokken zijn, en zo ja, betrek deze er dan ook bij.	PO in overleg met de FG.	
5	Vaststellen meld- en herstelaanpak.	1. Bepaal aanpak/informeren AP en/of datalek: wel of niet melden bij de AP. 2. Bepaal aanpak/informeren betrokkenen. 3. Bepaal acties voor nazorg betrokkenen. 4. Bepaal acties voor het belang van de organisatie. 5. Bepaal acties voor verbetering.	Afstemming door PO met FG en directie over aanpak en afweging melding bij de AP. Aanpak/informeren betrokkenen na afstemming (PO/directie/FG). DTV directie: Informeren bestuur. Belang organisatie en acties verbeteren beveiliging door PO in overleg met FG, directie, zo nodig IT en communicatie.	Melding bij de AP binnen 72 uur nadat met redelijke zekerheid is vastgesteld dat er sprake is van een datalek.

6	Registreer beveiligingsincident/ datalek.	Vervolg registratie Privacy Nexus.	PO/ISO.	Na beoordeling beveiligingsincident/ datalek en naarmate inbreuk zich ontwikkelt.
7	Melden betrokkenen***.	1. Melding via bijvoorbeeld brief/ e-mail <i>*Indien hiervoor gekozen wordt, valt dit samen met stap 8 aangezien het bestuur hiervan op de hoogte moet zijn en de Bestuurder NL zal ondertekenen.</i> 2. Meedelen wat er is gebeurd, welke persoonsgegevens getroffen zijn en wat de mogelijke gevolgen van het datalek kunnen zijn. 3. Informeren over de maatregelen die de organisatie neemt en die de betrokkene zelf kan nemen om schade te voorkomen.	PO in samenspraak met FG, directie in overleg met communicatie. Indien van toepassing: Brief uit door directie of namens bestuur. Dit laatste door de directie. Contactpersoon en FG. Communicatie.	z.s.m. na melding AP.
8	Informeren relevante derden.	1. Informeer bestuur. 2. Informeer politieke leiding/departement (bij grote impact). 3. Informeer eventuele overige betrokkenen.	PO/ISO/JZ, eventueel in afstemming met directie en/of bestuurder, afhankelijk van de impact.	
9	Nadere analyse en evaluatie van de melding.		PO, directie, ISO, communicatie.	Na melding AP en betrokkenen.
10	Uitvoeren vervolgacties, verbeter- of herstelwerkzaamheden.	1. Herstel het datalek. Verbeter de beveiliging. 2. Lever nazorg aan de betrokkenen. <i>Lessons learned</i>	IT, in overleg met PO en FG. PO/directie/ Communicatie.	Z.s.m. na afronding analyse en evaluatie (stap 9).
11	Optimaliseer het beveiligings- en datalekproces.	Registreer, evalueer en verbeter de beveiliging en het proces inzake melding van datalekken. Monitoring van opvolging van vastgestelde verbeterpunten.	PO, ISO, FG, directie, eventueel in afstemming met directie, bestuur en communicatie.	Z.s.m. na afronding van de verbeter- of herstelwerkzaamheden (stap 10).
12	Sluiting melding.	Afronding registratie.	PO/ISO.	Na afronding herstelwerkzaamheden.

*Verwerker

Het kan gebeuren dat het datalek optreedt bij de verwerker. De organisatie is en blijft (als verwerkingsverantwoordelijke) altijd verantwoordelijk voor het datalek bij de verwerker. In dat geval moet hetzelfde stappenplan worden afgewerkt. De verwerker zal bij de stappen betrokken moeten worden.

In de verwerkersovereenkomst wordt afgedwongen (opgenomen in de standaard verwerkersovereenkomst van de NVAO-NL) dat de verwerker eventuele datalekken onverwijld

meldt bij de organisatie en de organisatie helpt bij het beoordelen of er gemeld moet worden en bij de afwikkeling van het datalek. Belangrijk is dat de verwerker niet buiten de organisatie om een datalek meldt bij de AP. De verwerker moet verder alle redelijke instructies van de organisatie opvolgen.

****Melden AP**

Melding aan de AP kan alleen achterwege blijven indien het onwaarschijnlijk is dat het datalek leidt tot een hoog risico voor de rechten en vrijheden van de betrokkenen. Of hiervan sprake is, hangt mede af van de aard, omvang en gevoeligheid van de gelecte persoonsgegevens en het gemak waarmee personen kunnen worden geïdentificeerd, de ernst van de gevolgen voor de personen en eventueel bijzondere kenmerken. Indien bijvoorbeeld uitsluitend de adresgegevens zijn gelect van een kleine groep betrokkenen, dan is het onwaarschijnlijk dat er sprake is van een hoog risico. Dat is wellicht anders indien de adresgegevens in combinatie met andere gegevens zijn gelect. Bij de afweging van het risico voor de rechten en vrijheden van de betrokkenen zal altijd de Functionaris Gegevensbescherming betrokken moeten worden.

*****Melden betrokkenen**

Wanneer het datalek waarschijnlijk meebrengt dat er sprake is van een groot risico voor de rechten en vrijheden van de betrokkenen, moet het datalek ook aan de betrokkenen worden gemeld. Het risico zal bijvoorbeeld moeten worden beoordeeld aan de hand van de aard en de hoeveelheid van de gelecte gegevens. Als er persoonsgegevens van gevoelige aard zijn gelect, zal het lek in ieder geval gemeld moeten worden aan de betrokkenen. Bij de afweging van het risico voor de rechten en vrijheden van de betrokkenen zal altijd de Functionaris Gegevensbescherming betrokken moeten worden.

6 Slotbepaling

Dit *Protocol Datalekken* is vastgesteld door de directie NVAO NL op 6 november 2024.

Het *Protocol Datalekken* kan wijzigen als er nieuwe ontwikkelingen, waaronder onder andere ook signalering van knelpunten of klachten van betrokkenen, daarvoor aanleiding geven. Op Intranet kun je altijd de meest actuele versie van het *Protocol Datalekken* vinden. Dit protocol is voor het laatst herzien in februari 2025.

Lijst van begrippen en afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene verordening gegevensbescherming
DoS	Denial-of-Service
EU	Europese Unie
FG	Functionaris Gegevensbescherming
ISO	Information Security Officer
PO	Privacy Office
NL	Nederland
NVAO	Nederlands-Vlaamse Accreditatieorganisatie
Wbp	Wet bescherming persoonsgegevens

Lijst van begrippen en afkortingen

AHOVOKS	Agentschap voor Hoger Onderwijs, Volwassenenonderwijs, Kwalificaties en Studietoelagen
CDHO	Commissie Doelmatigheid Hoger Onderwijs
CMMBO	Commissie Doelmatigheid MBO
CROHO	Centraal Register Opleidingen Hoger Onderwijs
ECA	European Consortium for Accreditation in higher education

Colofon

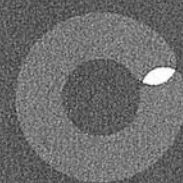
Protocol Datalekken
Februari 2025
Samenstelling: NVAO Nederland



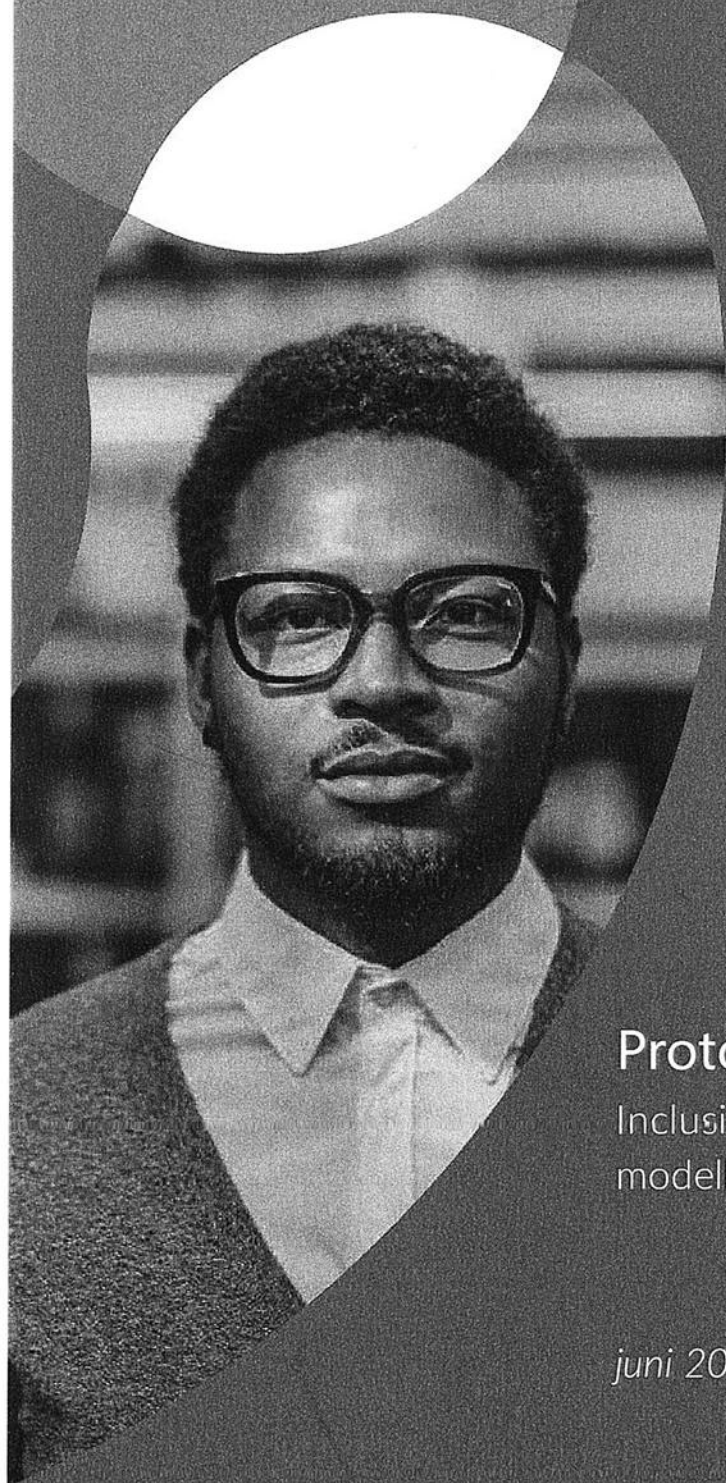
Nederlands-Vlaamse Accreditatieorganisatie
Accreditation Organisation of the Netherlands and Flanders

Parkstraat 83 2514 JS Den Haag
P.O. Box 85498 2508 CD The Hague
The Netherlands

T +31 (0)70 312 23 00
E info@nvao.net
www.nvao.net



NVAO



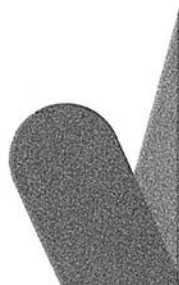
Protocol Rechten Betrokkenen

Inclusief: de toelichting en eventuele
modelbrieven

juni 2021

Protocol Rechten Betrokkenen
Inclusief: de toelichting en
eventuele modelbrieven

juni 2021



Artikel 1 Begripsbepaling en reikwijdte

De Algemene Verordening Gegevensbescherming (AVG) is van toepassing op de verwerking van persoonsgegevens van een natuurlijke persoon (betrokkene) door de NVAO.

Artikel 2 AVG-verzoek indienen (welke, wie, wijze waarop, kosten)

- 2.1 Een betrokkene, of diens wettelijk vertegenwoordiger of gemachtigde, kan een AVG verzoek indienen om inzage, correctie, overdracht, wissen en beperking van persoonsgegevens die worden verwerkt door de NVAO (verwerkingsverantwoordelijke). Als een wettelijk vertegenwoordiger of gemachtigde namens de betrokkene het verzoek indient, moet die persoon wel aantonen dat hij of zij daartoe bevoegd is.
- 2.2 Een verzoek kan worden ingediend via privacy@nvao.net. De NVAO kan extra informatie opvragen om zeker te zijn van de identiteit van betrokkene.
- 2.3 Een AVG-verzoek kan schriftelijk of digitaal, moet een datum bevatten én ondertekend zijn én bevat ten minste:
 - a. dat het een beroep betreft op de AVG;
 - b. de volledige naam, voorletters en indien per post wordt gecommuniceerd, het adres van de betrokkene;
 - c. de geboortedatum van betrokkene;
 - d. een kopie van een geldig legitimatiebewijs van betrokkene, waarbij het BSN onleesbaar is gemaakt; en
 - e. het e-mailadres van betrokkene.
- 2.4 Aan een verzoek zijn geen kosten verbonden, tenzij verzoeken buitensporig zijn of veelvuldig worden herhaald en redelijkerwijs vergoeding gevraagd kan worden door de NVAO.

Artikel 3 Ontvangstbevestiging en termijnen

- 3.1 Na ontvangst van een AVG-verzoek verstuurt de NVAO in beginsel binnen tien werkdagen een ontvangstbevestiging. Een ontvangstbevestiging bevat de naam van een contactpersoon van de NVAO, een beschrijving van de procedure, de te verwachten behandelingsduur en eventueel de mededeling dat het verzoek (nog) niet aan de vereisten voldoet.
- 3.2 De NVAO heeft vanaf de ontvangst van het AVG-verzoek ten hoogste vier weken de tijd om te beoordelen of het verzoek gerechtvaardigd is en hoe de behandeling van het verzoek eruit zal zien. Heeft de NVAO meer tijd nodig om de gegevens te verzamelen, dan stuurt de NVAO binnen vier weken bericht aan verzoeker. In dit bericht staat ook vermeld dat de totale behandeling niet langer dan drie maanden in beslag zal nemen.

Artikel 4 De NVAO, verwerkingsverantwoordelijke?

- 4.1 De NVAO toetst of een verzoek ziet op verwerkingen waarvoor de NVAO is aan te merken als verwerkingsverantwoordelijke.
- 4.2 Indien de NVAO geen verwerkingsverantwoordelijke is, dan zendt de NVAO dit (deel van het) verzoek door aan de organisatie die van dat (deel van het) verzoek verwerkingsverantwoordelijke is. Verzoeker ontvangt daarvan bericht.

De NVAO maakt onderscheid in de uitvoering van de inwilliging van een verzoek om:

- a. inzage in;
- b. correctie (rectificatie) van;
- c. overdracht van;
- d. wissen van; en
- e. beperking van de verwerking van;
- f. persoonsgegevens.

5.1. Indien het AVG-verzoek tot inzage wordt ingewilligd, stelt de NVAO de volgende gegevens ter beschikking:

- een volledig overzicht van de verwerkte persoonsgegevens;
- een omschrijving van:
 - het doel of de doeleinden van de verwerking;
 - de categorieën van gegevens waarop de verwerking betrekking heeft;
 - de ontvangers of categorieën ontvangers;
 - de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of de criteria om die termijn te bepalen;
 - de mededeling dat betrokkene het recht heeft om de NVAO te verzoeken de gegevens te rectificeren of wissen of dat de verwerking van hem betreffende gegevens wordt beperkt, en het recht tegen die verwerking bezwaar te maken;
- de beschikbare informatie over de herkomst van de gegevens;
- indien van toepassing, het bestaan van geautomatiseerde besluitvorming, waaronder profilering, en, tenminste in het geval van profilering, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor betrokkene.

5.2 Een verzoek tot correctie kan worden ingewilligd, indien de opgenomen gegevens:

- feitelijk onjuist; of
- voor het doel of doeleinden van de verwerking onvolledig of niet ter zake dienend; of
- in strijd met een wettelijk voorschrift;

zijn verwerkt.

5.3 Een verzoek tot overdracht kan worden ingewilligd indien dit technisch mogelijk is en in de volgende gevallen:

- de verwerking gebeurt op basis van toestemming;
- de verwerking gebeurt op basis van uitvoering van een overeenkomst waarbij de betrokkene partij is;
- de verwerking gebeurt op basis van geautomatiseerde procedés.

5.4 Een verzoek tot wissen wordt ingewilligd, indien:

- de persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of verwerkt;
- de betrokkene de toestemming intrekt en er geen andere rechtsgrond voor de verwerking is;
- de betrokkene bezwaar kan maken tegen de verwerking;
- de persoonsgegevens onrechtmatig zijn verwerkt.

5.5 Een verzoek tot beperking van de persoonsgegevens wordt onder andere ingewilligd, indien;

- de juistheid van de persoonsgegevens wordt betwist door de betrokkene;
- de verwerking onrechtmatig is;
- de NVAO de persoonsgegevens niet meer nodig heeft voor de verwerkingsdoeleinden;
- de betrokkene bezwaar heeft gemaakt tegen de verwerking, mede hangende een onderzoek wiens belangen zwaarder wegen.

Artikel 6 Kennisgevingsplicht

Nadat aan een AVG-verzoek is voldaan, brengt de NVAO indien relevant en mogelijk andere ontvangers op de hoogte.

Artikel 7 Overige rechten

Een schriftelijke beslissing op een AVG-verzoek (o.g.v. artt. 15 tot en met 22 AVG) is een besluit van de NVAO, waartegen bezwaar kan worden ingediend. De wijze waarop een dergelijk bezwaar wordt ingediend, staat vermeld op de website van de NVAO. Ook kan een klacht ingediend worden bij de Autoriteit Persoonsgegevens.

Artikel 8 Slotbepalingen

- 8.1 Dit Protocol is een nadere uitwerking van het Privacy Beleidskader en de daaruit vloeiende privacyverklaringen.
- 8.2 Dit Protocol wordt beheerd door het Privacy Office en is op <datum> door het Dagelijks Bestuur vastgesteld en treedt op diezelfde dag in werking. Wijzigingen in deze regeling kunnen door het Privacy Office worden vastgesteld.
- 8.3 Dit Protocol en de toelichting daarop beogen het Privacy Office meer handvaten te bieden voor het behandelen van AVG-verzoeken.

Toelichting op dit protocol

Wettelijk kader	Artikelen	Overweging
Algemene Verordening Gegevensbescherming, Ook wel: VERORDENING (EU) 2016/679 VAN HET EUROPEES PARLEMENT EN DE RAAD van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming)	i.h.bijz.: 4, 12 en 15 t/m 22, 89 lid 1	14
Uitvoeringsbesluit AVG (UAVG)	34	
Handvest van de grondrechten van de Europese Unie	8 lid 1	
Verdrag betr. de werking van de Europese Unie (VWEU)	16 lid 1	

Artikel 1 Begripsbepaling en reikwijdte

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) van toepassing. Dat betekent dat sinds die datum dezelfde privacywetgeving geldt in de hele Europese Unie. De belangrijkste regels voor de omgang met persoonsgegevens in Nederland zijn vastgelegd in de AVG.

N.B. De bescherming van natuurlijke personen bij de verwerking van persoonsgegevens is een grondrecht.

N.B. Onder 'persoonsgegevens' wordt verstaan (zie artikel 4 AVG): alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ('betrokkene'); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identicator zoals een naam, een identificatienummer, locatiegegevens, een online identicator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon. Het is mogelijk dat jurisprudentie op termijn een andere uitleg geeft aan het begrip persoonsgegevens. In dat geval zal jurisprudentie gevolgd worden en de regeling op die manier geïnterpreteerd kunnen worden.

Indien het onduidelijk is wie betrokkene is, wordt zoveel mogelijk aangesloten bij de bedoeling van de AVG en eventuele juridische uitspraken hieromtrent.

Artikel 2 Verzoeken indienen (welke, wie, wijze waarop, kosten)

- 2.1 Naast een betrokkene zelf kan een wettelijk vertegenwoordiger of gemachtigde een verzoek indienen. Of iemand wettelijk vertegenwoordiger is of gemachtigde dient wel uit een schriftelijk bewijsstuk te blijken. Een betrokkene kan bijvoorbeeld een minderjarige zijn of iemand die zich laat bijstaan door een raadsman. In dat geval kan een raadsman of ouder verzoeker zijn namens de betrokkene.

Welke verzoeken kunnen worden ingediend, zijn in dit lid opgesomd. Deze zijn verder uitgewerkt in artikel 5.1 t/m 5.5.

- 2.2 De wijze waarop een verzoek kan worden ingediend, staat vermeld op de website, inclusief het mailadres van de Functionaris Gegevensbescherming. De functionaris moet – hoe paradoxaal ook – juist om de persoonsgegevens te kunnen beschermen van betrokkene, kunnen toetsen of betrokkene wel is wie hij zegt dat hij is. In dat verband is het van belang dat de rechtmatigheid van een verzoek kan worden getoetst door de functionaris.

- 2.3 Een verzoek dient compleet te worden ingediend. Aan alle eisen dient te worden voldaan.
- 2.4 Aan een verzoek zijn in beginsel geen kosten verbonden, tenzij veelvuldig en buitensporig door iemand een (zelfde) verzoek wordt gedaan en redelijkerwijs niet van de NVAO kan worden verwacht telkens een dergelijk verzoek kosteloos in behandeling te nemen. De beginselen redelijkheid en billijkheid worden hierop van toepassing verklaard.

Artikel 3 Verzoeken bevestigen en al dan niet in behandeling nemen (termijnen)

- 3.1 De NVAO spant zich in om zo snel mogelijk een ontvangstbevestiging te sturen en uiterlijk binnen tien werkdagen, waarbij de NVAO naast de ontvangstbevestiging van het verzoek ook informatie geeft over wie de behandelaar is, de procedure, de behandeltermijn en eventueel betrokkene in de gelegenheid stelt om een verzoek compleet te maken, indien nog niet aan alle in 2.3 van deze regeling genoemde eisen is voldaan.
- 3.2 Indien het – om wat voor een reden dan ook – de NVAO niet lukt om binnen tien werkdagen te reageren, wordt aangesloten bij de wettelijke termijn, zie artikel 12 AVG met dien verstande dat een maand niet altijd evenveel dagen heeft en daarom een termijn van vier weken is aangehouden. De verlenging naar 3 maanden is ook wettelijk bepaald

Artikel 4 Verzoeken in behandeling nemen (als verwerkingsverantwoordelijke)

- 4.1 De NVAO is alleen gehouden verzoeken in behandeling te nemen in de gevallen dat zij als verwerkingsverantwoordelijke is aan te merken.
- 4.2 Het is mogelijk dat enkele verzoeken meerdere aspecten omvatten, waarbij de NVAO verwerkingsverantwoordelijke is ten aanzien van sommige aspecten en ten aanzien van andere aspecten een andere rechtspersoon verwerkingsverantwoordelijke is.

Artikel 5 Procedure (uitvoering verzoeken)

- 5.1 Zie artikel 15 AVG

De NVAO controleert of derden op de hoogte moeten worden gebracht om tegen dit AVG-verzoek bezwaar te maken.

Indien een derde bezwaar kan maken tegen de inwilliging van inzage van persoonsgegevens aan betrokkene, omdat zijn eigen persoonsgegevens hiermee verwerkt worden of anderszins, stelt de NVAO deze derde op de hoogte en biedt de NVAO aan deze derde de gelegenheid zijn zienswijze naar voren te brengen, tenzij dit onmogelijk blijkt of onevenredige inspanning kost.

- 5.2 Zie artikel 16 AVG
- 5.3 Zie artikel 20 AVG
- 5.4 Zie artikel 17 AVG en artikel 89 lid 1 AVG

Wanneer de NVAO de persoonsgegevens openbaar heeft gemaakt, neemt hij - rekening houdend met de beschikbare technologie en de uitvoeringskosten - redelijke (technische) maatregelen, om eventuele andere verwerkingsverantwoordelijken die de persoonsgegevens verwerken, ervan op de hoogte te stellen dat de betrokkene heeft verzocht om iedere koppeling naar, of kopie of reproductie van die persoonsgegevens te wissen.

Artikel 5.4 van deze regeling is niet van toepassing voor zover verwerking nodig is:

- voor het uitoefenen van recht op vrijheid van meningsuiting en informatie;
- voor het nakomen van een in het unierechtelijk of lid-statelijk recht neergelegde wettelijke verwerkingsverplichting die op de NVAO rust, of voor het vervullen van een taak van algemeen belang of het uitoefenen van het openbaar gezag dat aan de NVAO is verleend;
- om redenen van algemeen belang op het gebied van de volksgezondheid;
- met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden;
- voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

5.5 Zie artikel 18 AVG

De NVAO mag slechts die beperkte persoonsgegevens verwerken met toestemming van de betrokkene óf voor de instelling, uitoefening of onderbouwing van een rechtsvordering óf ter bescherming van de rechten van een andere natuurlijke persoon of rechtspersoon óf om gewichtige redenen van algemeen belang voor de Unie of voor een lidstaat.

Artikel 6 Kennisgevingsplicht

Zie artikel 19 AVG

- 6.1 De NVAO brengt iedere ontvanger aan wie de persoonsgegevens van verzoeker zijn verstrekt in kennis van de correctie of het wissen van de persoonsgegevens of de beperking van de verwerking, tenzij dit onmogelijk blijkt of onevenredig veel inspanning vergt.
- 6.2 Indien verzoeker dit wenst, verstrekt de NVAO informatie over ontvangers die diens persoonsgegevens hebben ontvangen.

Artikel 7 Overige rechten

Artikel 34 UAVG: Een schriftelijke beslissing op een verzoek als bedoeld in de artikelen 15 tot en met 22 van de verordening wordt genomen binnen de in artikel 12, derde lid, van de verordening genoemde termijnen en geldt, voor zover deze is genomen door een bestuursorgaan, als een besluit in de zin van de Algemene wet bestuursrecht.

Artikel 8 Slotbepalingen

- 8.1 Het bureau van de NVAO is gevestigd in Den Haag; de NVAO heeft haar statutaire zetel in Den Haag, Nederland. Op een AVG-verzoek jegens de NVAO, is daarmee de AVG van toepassing.
- 8.2 Het Dagelijks Bestuur heeft het Protocol Rechten Betrokkenen voor het eerst vastgesteld op <datum> 2021.
- 8.3 Het Algemeen Bestuur heeft in haar vergadering van 15 maart 2021 ingestemd met het Privacy Beleidskader en het Dagelijks Bestuur gemandateerd onderliggende documenten over privacy aangelegenheden op te stellen en goed te keuren. Dit mandaat moet nog in de mandaatregeling worden opgenomen.
- 8.4 Het Protocol Rechten Betrokkenen wordt na vaststelling of wijziging gepubliceerd op wiki ten behoeve van intern gebruik van het Privacy Office.

Eventuele modellen toevoegen van AVG-verzoeken

Aanhef

Onderwerp: verzoek om inzage

Uw verzoek

Bij e-mail van XXXX heeft u, op grond van de Algemene verordening gegevensbescherming, verzocht om inzage in uw persoonsgegevens die de NVAO verwerkt. U heeft aangegeven dat u zich beroept op uw rechten van inzage, dataportabiliteit en informatie op grond van de Algemene verordening gegevensbescherming (Hierna: AVG). U heeft aangegeven dat u in het verleden als XXXstudent-panellid betrokken bent geweest bij de NVAO. U heeft verzocht om een kopie van alle data die op u betrekking hebben, de rechtsgrond van de betreffende verwerkingen en de vraag of de betreffende data met anderen zijn gedeeld en zo ja, op basis van welke rechtsgrond.

Verloop van de procedure

De ontvangst van uw verzoek is bij brief bevestigd op XXXX, met kenmerk XXXX. Met dezelfde brief is de behandelingstermijn verlengd tot XXXX.

In de bijlage bij deze brief vindt u een volledig overzicht aan van (de verwerking van) uw persoonsgegevens binnen de NVAO.

Dit betreft de informatie waar u op grond van de Algemene verordening gegevensbescherming recht op heeft. Het gaat om de volgende informatie:

- de doeleinden van de verwerkingen;
- de categorieën van persoonsgegevens en om welke persoonsgegevens het gaat
- de (categorieën) ontvangers aan wie de persoonsgegevens worden verstrekt
- de bewaartermijn van de persoonsgegevens
- de gegevensbron van de persoonsgegevens,
- of sprake is van geautomatiseerde besluitvorming of profilering en indien dat het geval is nuttige informatie over de onderliggende logica, het belang van de verwerking en de verwachte gevolgen van de verwerking voor u;
- de getroffen waarborgen bij internationale doorgifte;
-

Verwerking persoonsgegevens en privacyverklaring

Wellicht ten overvloede wil ik u nog melden dat de NVAO zorgvuldig omgaat met uw persoonsgegevens en deze vertrouwelijk behandelt. Zo worden uw persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld (zie ook de Privacyverklaring op de website van de NVAO, XXXXlink

Namens het bestuur van de NVAO,

NAAM & ONDERTEKENING

Niet eens?

Heeft u vragen over deze brief of bent u het niet eens met het besluit? Neemt u dan telefonisch contact met ons op via (070) 312 23 00. We nemen dan samen met u het besluit door.

Bezwaar

Komen we er niet uit dan kunt u binnen zes weken na de dag waarop dit besluit is verzonden een bezwaarschrift indienen, per post, t.a.v.:

Privacy Office NVAO, Postbus 85498, 2508 CD Den Haag.

Door uw bezwaar op tijd in te dienen voorkomt u, dat wij uw bezwaarschrift niet meer kunnen behandelen.

Als u bezwaar maakt, vergeet dan niet de volgende gegevens te vermelden: het kenmerk van de beslissing waartegen u bezwaar indient; de datum van verzending van uw bezwaarschrift; uw naam; geboortedatum; adres; telefoonnummer en de reden waarom u het niet eens bent met de beslissing. U kunt ook bewijsstukken meesturen.

Colofon

Protocol Rechten Betrokkenen

juni 2021

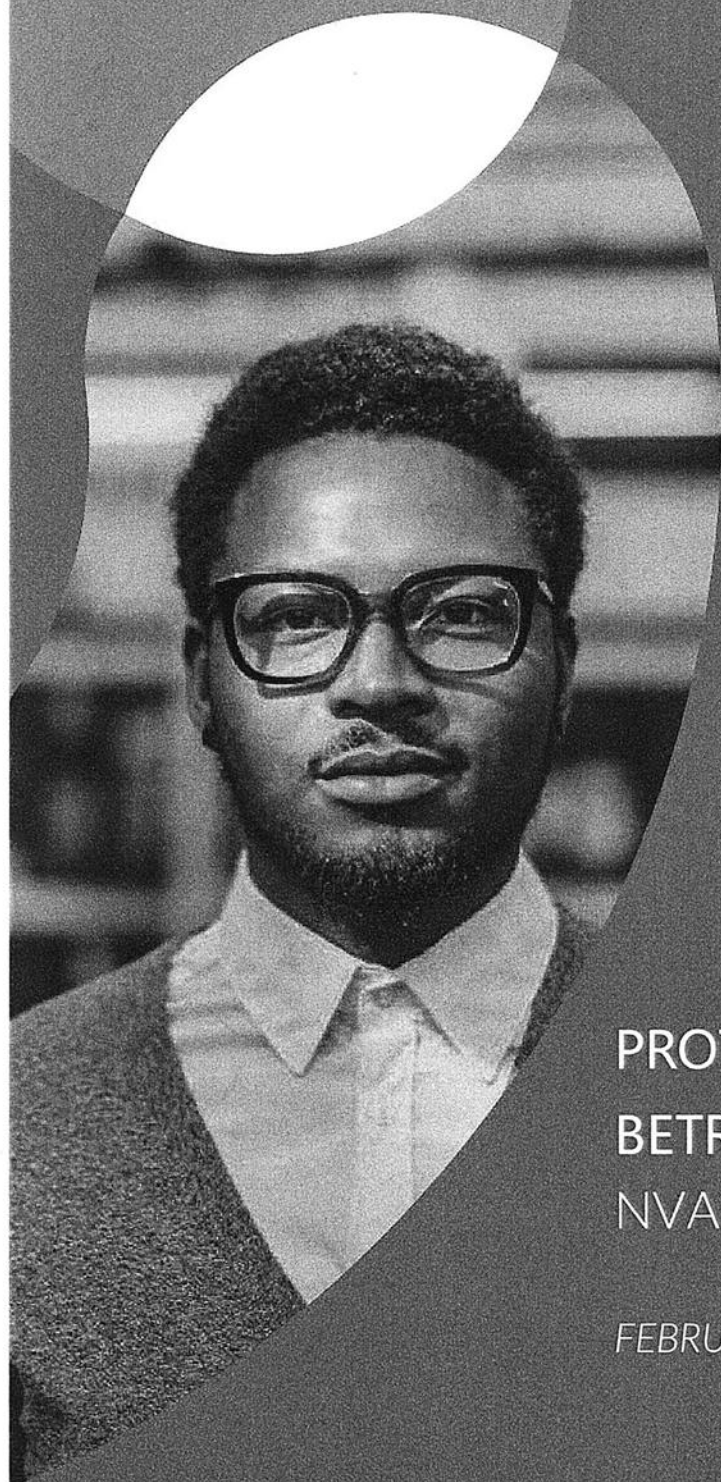
Samenstelling: NVAO



Nederlands-Vlaamse Accreditatieorganisatie
Accreditation Organisation of the Netherlands and Flanders

Parkstraat 83 · 2514 JG Den Haag
P.O. Box 85498 · 2508 CD The Hague
The Netherlands

T +31 (0)70 312 23 00
E info@nvao.net
www.nvao.net

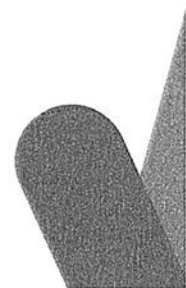


PROTOCOL RECHTEN
BETROKKENEN
NVAO NEDERLAND

FEBRUARI 2025

PROTOCOL RECHTEN
BETROKKENEN
NVAO NEDERLAND

FEBRUARI 2025



Inleiding

Dit protocol geeft een overzicht van de rechten van betrokkenen binnen de activiteiten van de Nederlands-Vlaamse Accreditatieorganisatie, afdeling Nederland (NVAO NL). Het doel is om transparantie te waarborgen en de belangen van betrokkenen te beschermen, terwijl we tevens voldoen aan de geldende wet- en regelgeving, waaronder de Algemene verordening gegevensbescherming (AVG). Dit betreft een interne werkbeschrijving voor de behandeling van verzoeken betreffende de rechten van betrokkenen.

Inhoud

1	Overzicht relevante bepalingen rechten betrokkenen	5
1.1	Informatie en transparantierechten	5
1.2	Recht op inzage.....	5
1.3	Recht op rectificatie	5
1.4	Recht op verwijdering	5
1.5	Recht op beperking van de verwerking	5
1.6	Recht van bezwaar	5
2	Werkwijze indiening en behandeling verzoeken	6
3	Klachten en geschillen	7
4	Slotbepaling.....	8
	Lijst van begrippen en afkortingen	12

1 Overzicht relevante bepalingen rechten betrokkenen

1.1 Informatie en transparantierechten

Betrokkenen hebben het recht om geïnformeerd te worden over:

- De wijze waarop hun persoonsgegevens worden verzameld, gebruikt en opgeslagen;
- Het doel van de gegevensverwerking;
- De betrokkenheid van NVAO NL in de gegevensverwerking;
- De contactgegevens van de Functionaris Gegevensbescherming (FG).

1.2 Recht op inzage

Betrokkenen hebben het recht om een verzoek in te dienen voor inzage in de persoonsgegevens die door NVAO NL worden verwerkt.

1.3 Recht op rectificatie

Betrokkenen hebben het recht om onjuiste of onvolledige persoonsgegevens te laten corrigeren.

1.4 Recht op verwijdering

Betrokkenen hebben, onder specifieke omstandigheden, het recht om hun persoonsgegevens te laten verwijderen. Dit is onder meer het geval wanneer:

- De persoonsgegevens niet langer noodzakelijk zijn voor de doeleinden waarvoor deze zijn verzameld;
- De betrokkene zijn of haar toestemming intrekt en er geen andere rechtsgrondslag voor de verwerking aanwezig is.

1.5 Recht op beperking van de verwerking

Betrokkenen hebben het recht om de persoonsgegevens die zij aan NVAO NL hebben verstrekt, te ontvangen in een gestructureerd, gangbaar en leesbaar formaat. Tevens hebben zij het recht om deze gegevens over te dragen aan een andere verwerker.

1.6 Recht van bezwaar

Het recht op bezwaar tegen de verwerking van persoonsgegevens is een belangrijk onderdeel van de AVG. Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van hun persoonsgegevens door een organisatie, onder bepaalde voorwaarden.

Rechtsgrond: Betrokkene heeft het recht om bezwaar te maken tegen de verwerking van hun persoonsgegevens wanneer deze verwerking is gebaseerd op de uitvoering van een taak van algemeen belang of de uitoefening van openbaar gezag¹, of wanneer de verwerking plaatsvindt op basis van gerechtvaardigde belangen².

Voorwaarden: Om een geldig bezwaar in te dienen, moet de betrokkene duidelijk maken waarom hij of zij bezwaar maakt tegen de verwerking van persoonsgegevens. Dit kan bijvoorbeeld zijn omdat er persoonlijke redenen zijn die verband houden met zijn of haar specifieke situatie.

Effect van bezwaar: Als een bezwaar is ingediend en het is gegrond, moet NVAO NL de verwerking van de persoonsgegevens stopzetten, tenzij zij dwingende gerechtvaardigde redenen kan aantonen die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene.

Informatieplicht: NVAO NL is verplicht om de betrokkene te informeren over hun recht op bezwaar, bijvoorbeeld in privacyverklaringen of bij het verzamelen van persoonsgegevens.

¹ Artikel 6, lid 1, onder e

² Artikel 6, lid 6, onder f

2 Werkwijze indiening en behandeling verzoeken

Bij een verzoek moet duidelijk aangegeven worden welke persoonsgegevens de betrokkene wenst in te zien, te corrigeren, te verwijderen of waartegen bezwaar gemaakt wordt.

- **Indiening:** Verzoeken kunnen ingediend worden via het volgende e-mailadres: privacy@NVAO.net;
- **Legitimatie:** Het is belangrijk dat een verzoeker zich kan legitimeren en dat aangetoond wordt dat de gegevens daadwerkelijk van verzoeker zijn. Het is niet toegestaan om gegevens van andere personen in te zien;
- **Veilige kopie t.b.v. legitimatie:** Verzoekers kunnen gebruik maken van de website Rijksoverheid.nl voor legitimatie. Als een verzoek niet duidelijk is, kan verzoeker gevraagd worden om het verzoek te preciseren, zodat we verzoeker zo goed mogelijk van dienst kunnen zijn;
- **Bevestiging:** NVAO NL bevestigt de ontvangst van het verzoek binnen vijf werkdagen;
- **Behandeling:** Het verzoek wordt binnen één maand na ontvangst behandeld. Deze termijn kan één keer met maximaal twee maanden verlengd worden, maar dit moet dan wel schriftelijk aan de aanvrager worden meegedeeld, met uitleg over de reden voor de verlenging. Verwezen wordt naar de procesbeschrijving *Borging rechten van betrokkenen* (bijlage 1);
- **Communicatie:** Betrokkene wordt schriftelijk geïnformeerd over de uitkomst van hun verzoek.

3 Klachten en geschillen

Betrokkene heeft het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP) als zij van mening zijn dat hun rechten niet worden gerespecteerd.

4 Slotbepaling

Dit protocol is vastgesteld op 6 november 2024. Dit protocol over de rechten van betrokkenen van NVAO NL kan worden aangepast als nieuwe ontwikkelingen – waaronder bijvoorbeeld signaleringen van knelpunten of klachten van betrokkenen – daar aanleiding toe geven. Op intranet kun je altijd de meest actuele versie van dit protocol vinden. Dit protocol over de rechten van betrokkenen is voor het laatst herzien in februari 2025.

Bijlage 1: Procesbeschrijving borging rechten van betrokkenen

Wat	Wie verzendt/doet	Wie ontvangt?	Wanneer?
AVG verzoek	Betrokkene	Medewerker en/of PO. Een medewerker stuurt een verzoek direct door naar PO	Datum X
Registratie verzoek	Privacy Office (PO)	Privacy Nexus	Z.s.m. na datum X
Vaststellen type verzoek	PO	Betrokkene	Z.s.m. na ontvangstverzoek
Inschatting termijn afdoening	PO stemt af en maakt inschatting of verlengde termijn afdoening nodig is	-	Z.s.m. na datum X
Ontvangstbevestigingsbrief/ mail met zo nodig verzoek om ID-bewijs (voorbeeld 1)	Vanuit PO, ondertekening door directie	Betrokkene	Datum X + max. tien werkdagen
Interne navraag op basis van het verzoek	PO	HR, financiën, beleidsafdeling en directie	Z.s.m. na ontvangst verzoek
Inhoudelijke behandeling, inclusief verzamelen eventuele gegevens	PO	Concept naar directie en eventueel FG	Z.s.m. na ontvangst verzoek
Interne mails naar collega's in geval van verzoek verwijdering (voorbeeld 2)	PO	Diverse afdelingen	Z.s.m. na datum X
Bevestiging van collega's dat persoonsgegevens zijn verwijderd	Collega's NVAO NL	PO	Eén maand na datum X
Herinnering (indien nodig)	PO	Collega's	Zes weken na datum X
Besluit (voorbeeld 3) en versturen	Vanuit PO, ondertekening door directie/bestuurder	Betrokkene	Uiterlijk drie maanden na datum X
Afronden registratie	PO	Privacy Nexus	Z.s.m. na verzending besluit

Voorbeeld 1:

Raadpleeg ook de modelbrief bij Privacy > Documenten > Archief > 110 Rechten van betrokkene, bedoeld voor verschillende AVG-verzoeken.

Voorbeeld 2:

Beste collega's,

Onlangs hebben wij een verzoek ontvangen van een ex-medewerker XXX, (werkzaam van tot) waarin hij/zij officieel vraagt om zijn/haar persoonsgegevens die conform de wettelijke vervalt termijn vernietigd mogen worden, ook daadwerkelijk te verwijderen. Vanaf heden zal in alle communicatie verwezen worden naar 'Rechtspersoon XXX'.

In het verleden kan het zijn dat jullie met betrokkene hebben samengewerkt en/of over en met haar hebben gecommuniceerd. Om aan zijn/haar verzoek te kunnen voldoen vragen wij het volgende.

Controleer jullie mailbox en verwijder zijn/haar naam en eventueel andere persoonsgegevens zoals:

- CV & sollicitatiebrief;
- Referenties;
- Arbeidsovereenkomst/Akte van aanstelling;
- Privé adres & telefoonnummer;
- E-mails en brieven m.b.t. arbeidsvoorwaarden;
- Correspondentie m.b.t. benoemingen, promotie/demotie en ontslag;
- Correspondentie en verslagen m.b.t. functionering en beoordeling.

Controleer hiervoor o.a.

- De e-mail (inbox, folders, verzonden items, deleted items, archief);
- Digitale folders & mappen, denk hierbij ook aan de deleted items en downloads;
- Hardcopy documenten.

In het kader van de Algemene Verordening Gegevensbescherming dienen wij dit binnen een vastgestelde termijn af te ronden. Uiterlijk over **1 maand** moet ik een terugkoppeling ontvangen waarin wordt bevestigd dat de gevraagde gegevens zijn verwijderd.

Laatste stap

Na afhandeling van deze e-mail zowel deze e-mail als de aan mij verzonden reply met eventuele verdere informatie verwijderen uit de verzonden items en deleted items.

Bij voorbaat dank voor de medewerking.

Met vriendelijke groet,

Voorbeeld 3: Besluit op AVG verzoek (verwijderen gegevens)

Geachte

Op XXXX heeft u bij NVAO NL een verzoek ingediend om verwijdering van uw persoonsgegevens waar geen wettelijke bezwaartermijn meer voor geldt. De ontvangst van dit verzoek is door NVAO NL op XXXX bevestigd. Ter bevestiging van uw identiteit heeft NVAO NL desgevraagd een kopie van een geldig legitimatiebewijs ontvangen. De kopie is inmiddels uit onze administratie verwijderd.

Uw verzoek valt onder de reikwijdte van de Algemene verordening gegevensbescherming. Voor de NVAO is het Archiefwet 1995 van toepassing en leidend alsmede de 'Selectielijst voor de Nederlands - Vlaamse Accreditatieorganisatie (NVAO) zoals is vastgesteld in de Staatcourant 7827 op 23 april 2012.

Naar aanleiding van het verzoek hebben wij alle medewerkers gevraagd communicatie en/of documenten waarin uw persoonsgegevens voorkomen én die niet met het primaire proces te maken hebben te verwijderen. Op dit verzoek is van alle medewerkers een bevestiging van (voltooide) uitvoering ontvangen. Voor gegevens die onderdeel uitmaken van het primaire proces geldt een langere bewaartermijn (18 jaar).

Binnen HR is zowel het papieren als het digitale personeelsdossier doorgenomen. Alle documenten, e-mails en bestanden die conform de Selectielijst in aanmerking komen voor vernietiging zijn vernietigd. Voor financiële handelingen geldt dat hier nog een wettelijke bewaartermijn (7 jaar) op van toepassing is die nog niet is verstreken. Bij ommekomst hiervan zullen uiteraard ook deze gegevens worden verwijderd.

Uw verzoek tot verwijdering van persoonsgegevens evenals de procedurele vastlegging hiervan zal 5 jaar bewaard blijven bij de NVAO.

Wellicht ten overvloede wil ik u nog melden dat NVAO NL zorgvuldig omgaat met uw persoonsgegevens en deze vertrouwelijk behandelt. Zo worden uw persoonsgegevens alleen verwerkt door personen met geheimhoudingsplicht en voor het doel waarvoor deze gegevens zijn verzameld (zie ook de Privacyverklaring op de website van de NVAO > link)

Met vriendelijke groet,

(Ondertekening directie)

Directeur Nederland NVAO

Niet eens?

Heeft u vragen over deze brief of bent u het niet eens met het besluit? Neemt u dan telefonisch contact met ons op via (070 312 2300, u kunt vragen naar de contactpersoon van deze brief dan wel privacy office) of per e-mail via privacy@nvao.net. We nemen dan samen met u het besluit door.

Bezwaar

Komen we er niet uit dan kunt u binnen zes weken na de dag waarop dit besluit is verzonden een bezwaarschrift indienen.

Door uw bezwaar op tijd in te dienen voorkomt u, dat wij uw bezwaarschrift niet meer kunnen behandelen. Als u bezwaar maakt, vergeet dan niet de volgende gegevens te vermelden: het kenmerk van de beslissing waartegen u bezwaar indient; de datum van verzending van uw bezwaarschrift; uw naam; geboortedatum; adres; telefoonnummer en de reden waarom u het niet eens bent met de beslissing. U kunt ook bewijsstukken meesturen.

Lijst van begrippen en afkortingen

AP	Autoriteit Persoonsgegevens
AVG	Algemene verordening gegevensbescherming
FG	Functionaris Gegevensbescherming
NL	Nederland
NVAO	Nederlands-Vlaamse Accreditatieorganisatie
PO	Privacy Office

Colofon

Protocol rechten betrokkenen
Februari 2025
Samenstelling: NVAO Nederland



Nederlands-Vlaamse Accreditatieorganisatie
Accreditation Organisation of the Netherlands and Flanders

Parkstraat 83 · 2514 JG Den Haag
P.O. Box 85498 · 2508 CD The Hague
The Netherlands

T +31 (0)70 312 23 00
E info@nvao.net
www.nvao.net

Handleiding privacy by design, model Rijksoverheid

<https://www.rijksoverheid.nl/documenten/rapporten/2023/06/01/handleiding-privacy-by-design-versie-1-0>

Handleiding bewaren email, Rijksoverheid

<https://www.informatiehuishouding.nl/documenten/vragen-en-antwoorden/wat-houdt-de-handreiking-bewaren-van-e-mail-in>

Register van Verwerkingsactiviteiten NVAO-NL

Gegevens verwerkingsverantwoordelijke:

NVAO-NL
Parkstraat 83
Postcode
Den Haag
Telefoonnummer

Contactgegevens
Privacy Officer: Privacy@nvaio.net
FG: vacature

Primaire proces: accreditaties NL

Verwerking	Verwerkings verantwoord elijke	Doel verwerking	Grondslag	Afdeling	Categorieën van betrokkenen	Categorieën persoons gegevens*	Categorieën ontvangers	Doorgifte/ Verwerken Binnen/Buiten EU	Bewaartermijn
1. Samenstellen panelleden en secretarissen TNO/ITK/verificatie	NVAO-NL	Beoordelen deskundigheid en onafhankelijkheid tbt deelname panel	Uitvoering publieke taak	Relatiebeheer P&A Beleid en onderzoek	Panelleden Secretarissen TNO/ITK	NAW VOG Contactgegevens Motivatie CV Referenties Integriteitsverklaring IBAN Geheimhoudingswerk laring Onafhankelijkverkla ring	Panelleden Secretarissen contactpersonen IHO	Binnen EU/EER	Selectielijst 18 j V met steekproef naar NA
2. Instemmen voorgedragen panelleden en secretarissen ABO	NVAO-NL	Toets deskundigheid en onafhankelijkheid tbt deelname panel	Uitvoering publieke taak	Relatiebeheer P&A Beleid en onderzoek	Panelleden Secretarissen ABO	Naam Contactgegevens Motivatie CV Referenties Integriteitsverklaring Onafhankelijkverkla ring	Panelleden Secretarissen Contactpersonen IHO	Binnen EU/EER	Selectielijst 18 j V met steekproef naar NA
3. Verzoek registratie tbt deelname panelleden aan nieuwe accreditaties TNO/ITK/ verificatie	NVAO-NL	Toets deskundigheid en onafhankelijkheid tbt deelname panel	Toestemming	Relatiebeheer P&A	Panelleden Secretarissen TNO/ITK	Contactgegevens Vaardigheden	nvt	Binnen EU/EER	1 jaar bij verzoek controle op vervoldgeefname en juistheid gegevens indien geen verlenging vermijding gegevens
4. Contact tbt accreditaties	NVAO-NL	Bieden van ondersteuning, verstrekken van informatie over accreditatieproces	Uitvoering publieke taak	Relatiebeheer P&A Beleid en onderzoek	Contactpersonen IHO	Contactgegevens	nvt	Binnen EU/EER	1 jaar met actualisatie

5. Publicatie rapporten	NVAO NL	Informeren studenten over kwaliteit van opleiding	Uitvoering publieke taak	P & A Communicatie	Panelleden Secretarissen TNO/ITK/ABO	Naam en functie	Bezoekers website	Binnen EU/EER	Selectielijst 18 j V met steekproef naar NA
6. Registratie secretarissen	NVAO NL	Borging kwaliteit secretarissen	Uitvoering publieke taak	Beleid en onderzoek/ JZ	Secretarissen accreditaties	Naam, rapporten op naam	nvt	Binnen EU/EER	1 jaar bij verzoek controle op vervolgoedname en juistheid gegevens indien geen verlenging vernietiging gegevens
7. Analyse en onderzoek gegevens oiv de accreditatieprocedure	NVAO NL	Rapporteren MINOCW kwaliteit opleidingen	Uitvoering publieke taak	Beleid en onderzoek	Panelleden Secretarissen TNO/ITK/ABO	Naam en functie	Ministerie van OCW	Binnen EU/EER	Gegevens onderzoek zelf Gepseudonimiseerd: gedurende 10 jaar. Indien onderzoek niet wordt afgeond: gepseudonimiseerd 5 jaar.
Interviews tbv analyse en onderzoek			Toestemming						Bij toestemming voor de duur van de toestemming en niet langer dan bovengenoemde termijnen.
8. Registratie tbv uitwisseling en kennisbeoordeling bij accreditaties	NVAO NL	Faciliteren deelname aan Meet&Greet, online of fysieke informatiebijeenkomst, verzenden nieuwsbrief, training secretarissen en panelleden	Toestemming	Communicatie en beleid	Deelnemers aan bijeenkomsten voor kennisdeling	Contactgegevens	nvt	Binnen EU/EER	Thematische analyse (eindproduct van onderzoek) geanonimiseerd, V 18 of selectielijst en steekproef naar NA. Maximaal
9. Opstellen, ondertekenen en verzenden (uploaden in LEO) VTB/ besluit	NVAO NL	Bekendmaken (voornemen) besluit aan aanvrager	Uitvoeren publieke taak	P & A	Aanvrager Ondertekenaar van het besluit	Contactgegevens	Instelling IHO, dienstverlener gecertificeerde en gekwalificeerde ondertekening	Binnen EU/EER	Selectielijst 18 j V met steekproef naar NA
10. Behandelen bezwaar	NVAO NL	Behandelen van bezwaar, contact met indiener, eventuele gemachtigde, contactpersoon voor externe bezwarencommissie	Uitvoeren publieke taak Wettelijke verplichting	JZ	Indiener bezwaar, medewerkers	Contactgegevens alle categorieën van persoonsgegevens (in onderliggende dossiers)	Gemachtigde Externe bezwarencommissie	Binnen EU/EER	Selectielijst: bewaren i/vm overdracht NA
11. Beredingsprocedure	NVAO NL	Beroepsprocedure voor belanghebbenden	Wettelijke verplichting	JZ	Appellant, eventueel gemachtigde	Naam, contactgegevens, functie	RNS Gemachtigden	Binnen EU/EER	Selectielijst: bewaren i/vm overdracht NA
12. Handelingen voortvloeiend uit de Archiefwet (bewaren/overdracht/vernietigen)	NVAO NL	Het voldoen aan de bewaarplicht/ Vernietigingsplicht	Wettelijke verplichting	Archief	Panelleden secretarissen medewerkers en bestuurders NVAO derden	Namen en functie	NA	Binnen EU/EER	Selectielijst: Athankelijk van type dossier (accréditatie/ verantwoordings bestuur)
13. WOO verzoeken	NVAO NL	Behandelen WOO verzoeken	Wettelijke verplichting	JZ/ Communicatie/ directie	Verzoeker	Naam en contactgegevens	Verzoeker	Binnen EU/EER	Selectielijst V na 10 jaar

14. Behandeling datalekken	NVAO NL	Melden datalekken bij AP, Contact onderhouden met indener datalekmeldingen en interne organisatie	Wettelijke verplichting	PO / Directie/IT	Contactpersonen IHO en medewerkers derde organisaties, Medewerkers NVAO NL, Verzoekers/melder s/klager s/derden Belanghebbenden	Contactgegevens, alle categorieën van persoonsgegevens (in onderliggende dossiers)	Bezoekers website indien besluit tot openbaarmaking	Binnen/Buiten EU	5 jaar voor statistische doeleinden
15. Verzoek rechten van betrokkenen AVG	NVAO NL	Afhandelen van ingediend verzoek	Wettelijke verplichting	IJZ/HR/IT/ Beleid/ Commun- catie/Directie	Verzoekers/melder s/klager s/derden Belanghebbenden	Contactgegevens, alle categorieën van persoonsgegevens (in onderliggende dossiers)	Verzoekers	Binnen EU/EER	Indien afwijzing in geval van geen gegevens: na ommekomst bezwaartermijn In geval van verzoeken m.b.t. verwijdering, persoonsgegevens afhankelijk inhoud verzoek bewaartermijn Selectielijst
16. Behandelen klachten intern/extern	NVAO NL	Afhandelen klacht	Wettelijke verplichting	IJZ/HR/directie	Klager	Naam, Contactgegevens	Klachtbehandelaar Overige betrokkenen bij de klacht	Binnen EU/EER	Overige verzoeken: redelijke termijn van maximaal 2 jaar Verliefden na 5 jaar
17. Back-ups	NVAO NL	Waarborgen van continuïteit en herstel bij incidenten of storingen	Gerechtsvaardigd belang	Alle betrokkenen waarvan persoonsgegevens in systemen worden verwerkt	Alle gegevens die in een back-up terecht komen	IT beheer of indien wij dat hebben de leverancier die de back-up dienst aanbiedt	Binnen EU/EER	n.b.	
18. Sharepoint	NVAO NL	Opslaan, delen, bewerken	Uitvoering publieke taak	Medewerker, panelleden, instellingen	Naam, contactgegevens, functie en alle andere persoonsgegevens	Interne medewerker, panelleden, secretarissen	Binnen EU-EER	Selectielijst	
Taken op gebied van HR-en financiën									
Verwerking	Verwerkings verantwoordelijke	Doel verwerking	Grondslag	Afdeling	Categorieën van betrokkenen	Categorieën persoons Gegevens*	Categorieën ontvangers	Doorgifte/ Verwerkingen Binnen/Buiten EU	Bewaartermijn
1. Werving en selectie	NVAO NL	Werven en selecteren van nieuw personeel.	Uitvoering overeenkomst/ toestemming voor in portefeuille houden	HR	Interne/ externe medewerkers	Naam, adres, woonplaats, BSN, functie, CV, kopie diploma's.	nvt	Binnen/Buiten EU	Bij afwijzen sollicitanten: V 1 maand na afwijzing, V 1 jaar indien persoonsgegevens met toestemming van de betrokkene na beëindiging van de sollicitatieprocedure worden bewaard.

2. Personeels- en financiële administratie	NVAO NL	Uitvoering geven aan (arbeids)overeenkomst/ verplichtingen op grond van de wet (BW) Administratieplicht fiscale wetgeving	Uitvoering overeenkomst/ wettelijke verplichting	HR/financiën	Huidige en oud-medewerkers (vanwege bewaarplicht)	Naam, (zakelijke email) adres, woonplaats, BSN, bankgegevens, gegevens met betrekking tot arbeids-overeenkomst, functie, CV, kopie identificatiedocument, kopie diploma's, loonbelasting-verklaring, formulier salarisbetaling, pensioeninformatie, verlof, VOG, geheimhoudings-verklaring, Eed/beloofte, toelagen, gratificaties, declaraties, inhoudingen, loonbeslag, gegevens omtrent functioneren in de vorm van gespreksverslagen, nevenfuncties, opleiding/training Ontslagbrief VSO	UWV/ pensioenverzekeraar/ Belastingdienst/ AFAS/ Banken, leveranciers i.v.m. attenties medewerkers Beheerder gebouw (toegangspas) Leverancier gekwalificeerde digitale handtekening	Binnen EU/EER	Personeelsgegevens Selectielijst V 10 jaar na einde dienstverband Fiscale gegevens Selectielijst V7 Overige gegevens niet gebonden aan wettelijke bewaartermijn: maximaal 2 jaar
3. Verzuimregistratie	NVAO NL	Uitvoering aan Arbowergving	Wettelijke verplichting	HR	Medewerkers, werkgever, Arbodienst, UWV	NAW-gegevens, ge-boorte datum, BSN- nummer, e-mailadres, tele-foonnummer, IBAN	ARBO, coachings-bureau, UWV,	Binnen EU/EER	Personeelsgegevens Selectielijst V 10 jaar na einde dienstverband
4. Inhuur extern personeel	NVAO-NL	Opdrachten tlv het primair proces, p- en financiële administratie, IT	Uitvoering overeenkomst	Bedrijfsvoering	Medewerkers van dienstverleners	NAW VOG Contactgegevens Motivatie CV Referenties Integratieverklaring IBAN Geheimhoudings-verklaring	nvt	Binnen EU/EER	4 weken na beëindiging sollicitatieprocedure zonder toestemming, i.k.v de AVG. - 1 jaar na beëindiging sollicitatieprocedure met toestemming van de sollicitant, i.k.v AVG. Indien ingehuurd salarisadministratie: 7 jaar na afloop contract, Kopie ID V 10 jaar na einde contract ogv Selectielijst VOG, integriteitsverklaring en de geheimhoudingsverklaring: 2 jaar, i.k.v de AVG

5. Contractbeheer	NVAO NL	Afsluiten van overeenkomsten met leveranciers	Uitvoering overeenkomst	Bedrijfsvoering/financien	Leveranciers	Zakelijke contactgegevens	nvt	Binnen EU/EER	Selectielijst V 7 jaar i.v.m. verantwoording financiële administratieplicht
6. Uitbetalen van AB bestuursleden	NVAO NL	Vergoeding van bestuurswerkzaamheden AB	Wettelijke verplichting	Bedrijfsvoering/financien	Bestuursleden	NAV, contactgegevens, financiële gegevens, identiteitsgegevens,	nvt	Binnen EU/EER	Selectielijst V 7 jaar i.v.m. verantwoording Financiële administratieplicht
7. Uitbetalen panelleden/secretarissen	NVAO NL	Vergoeding voor inzet panelwerkzaamheden	Uitvoering publieke taak/ OVO	Bedrijfsvoering/financien	Panelleden Secretarissen TNO/TK	NAV Contactgegevens IBAN	Belastingdienst AFAS	Binnen EU/EER	V 7 jaar na uitbetaling
8. Scholing personeel	NVAO NL	Registratie deelname opleiding/ cursus	Uitvoering AO	HR	Medewerkers	Naam, functie, gevolgde training, certificaten evaluaties	HR, leidinggeversden, opleidingsinstituten	Binnen EU/EER	Tot 2 jaar na einde dienstverband certificaten conform selectielijst 10 jaar
Bezoekersbeheer Extern bezoek	NVAO NL	Veiligheid en toegangscontrole	Gerechvaardigd belang: beveiliging	Facilitair/bedrijfsvoering	Bezoekers, gasten en leveranciers	Naam organisatie, tijdstip bezoek, kentekens	Receptie	Binnen EU/EER	Max 1 jaar tenzij incident.

*Categorieën persoonsgegevens: de NVAO-NL verwerkt geen bijzondere persoonsgegevens. Dit gegeven is dan ook niet opgenomen als optie in dit register

Uitvoeringsregels april 2024

<https://www.nvao.net/nl/nieuws/2025/9/geactualiseerde-uitvoeringsregels-accreditatiestelsel-hoger-onderwijs-nederland>

Uitvoeringsregels september 2024

<https://www.nvao.net/nl/nieuws/2024/8/actualisering-uitvoeringsregels-accreditatiestelsel-hoger-onderwijs-nederland>

Verwerkersovereenkomst [NAAM BEDRIJF]

Datum: [INVOEREN DATUM]

Contractpartijen:

1. Verwerkingsverantwoordelijke te weten, de Nederlands Vlaamse
Accreditatieorganisatie, gevestigd te Den Haag, vertegenwoordigd door ... NVAO.

hierna te noemen: '**Verwerkingsverantwoordelijke**',

en

2. Verwerker te weten [STATUTAIRE NAAM], statutair gevestigd te [PLAATS],
vertegenwoordigd door [NAAM EN/OF NAAM BESTUURDER]

hierna te noemen: '**Verwerker**',

gezamenlijk aan te duiden als: '**Partijen**';

Overwegende dat:

Partijen hebben op [DATUM] een Overeenkomst met betrekking tot
[OMSCHRIJVING] gesloten. Ter uitvoering van deze Overeenkomst worden
Persoonsgegevens verwerkt.

Verwerkingsverantwoordelijke hecht grote waarde aan het beschermen van deze
Persoonsgegevens. Om die reden leggen Partijen in deze Verwerkersovereenkomst en
de daarbij behorende bijlagen, te weten:

1. overzicht met verwerkingen van Persoonsgegevens en verwerkingsdoelen
2. overzicht met beveiligingsmaatregelen
3. proces rondom het melden van Datalekken en de te verstrekken informatie met
betrekking tot het Datalek vast wat Verwerker wel en niet mag doen met de
Persoonsgegevens.

1. Definities

De hierna en hiervoor gebruikte begrippen volgen uit de Algemene Verordening
Gegevensbescherming en hebben de volgende betekenis:

- 1.1 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare
natuurlijke persoon ('**de Betrokkene**'); als identificeerbaar wordt beschouwd een
natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name
aan de hand van een identificator zoals een naam, een identificatienummer,
locatiegegevens, een online identificator of van een of meer elementen die
kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische,
economische, culturele of sociale identiteit van die natuurlijke persoon.
- 1.2 Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot
Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd
via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen,
structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken,

verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

- 1.3 Verwerkingsverantwoordelijke: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van Persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lidstatelijke recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen ('**Verwerkingsverantwoordelijke**').
- 1.4 Verwerker: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke Persoonsgegevens verwerkt ('**Verwerker**').
- 1.5 Betrokkene: geïdentificeerde of identificeerbaar natuurlijk persoon op wie de verwerkte Persoonsgegevens betrekking hebben.
- 1.6 Verwerkersovereenkomst: deze Overeenkomst inclusief de bijlagen ('**Verwerkersovereenkomst**').
- 1.7 Overeenkomst: de hoofdovereenkomst waar deze Verwerkersovereenkomst uit voortvloeit.
- 1.8 Inbreuk in verband met Persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens ('**Datalek**').
- 1.9 Toezichthoudende autoriteit: een onafhankelijke overheidsinstantie verantwoordelijk voor het toezicht op de naleving van de wet in verband met de verwerking van Persoonsgegevens. In Nederland is dit de Autoriteit Persoonsgegevens.

2. Totstandkoming, duur en beëindiging van deze Verwerkersovereenkomst

- 2.1 Deze Verwerkersovereenkomst treedt in werking op de datum waarop Partijen deze ondertekenen.
- 2.2 Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst en zal gelden voor zolang de Overeenkomst duurt.
- 2.3 Indien de Overeenkomst eindigt, eindigt deze Verwerkersovereenkomst automatisch; de Verwerkersovereenkomst kan niet apart worden opgezegd.
- 2.4 Na beëindiging van deze Verwerkersovereenkomst zullen de lopende verplichtingen voor Verwerker, zoals het melden van Datalekken waarbij Persoonsgegevens van Verwerkingsverantwoordelijke betrokken zijn en de plicht tot geheimhouding blijven voortduren.

3. Verwerken Persoonsgegevens

- 3.1 Verwerker verwerkt alleen Persoonsgegevens in opdracht van Verwerkingsverantwoordelijke en Verwerker heeft geen zeggenschap over de Persoonsgegevens. Verwerker volgt instructies van Verwerkingsverantwoordelijke ten aanzien van de verwerking en mag de Persoonsgegevens niet op een andere manier verwerken, tenzij

Verwerkingsverantwoordelijke Verwerker daar van tevoren toestemming of opdracht voor geeft.

- 3.2 In Bijlage 1 wordt opgenomen welke Persoonsgegevens Verwerker precies zal verwerken en voor welke verwerkingsdoeleinden.
- 3.3 Verwerker houdt zich aan de wet en verwerkt de gegevens op een behoorlijke, zorgvuldige en transparante wijze.
- 3.4 Verwerker mag zonder voorafgaande schriftelijke toestemming van Verwerkingsverantwoordelijke geen andere personen of organisaties inschakelen bij het verwerken van de Persoonsgegevens.
- 3.5 Wanneer Verwerker met toestemming van Verwerkingsverantwoordelijke andere organisaties inschakelt, moeten zij minimaal voldoen aan de eisen die zijn opgenomen in deze Verwerkersovereenkomst.
- 3.6 Wanneer Verwerkingsverantwoordelijke een verzoek van een Betrokkene ontvangt ten aanzien van het uitoefenen van zijn of haar rechten, dan werkt Verwerker daar binnen een termijn van 14 dagen aan mee. Deze rechten bestaan uit een verzoek om inzage, verbetering, aanvulling, verwijdering of afscherming, bezwaar maken tegen de verwerking van de Persoonsgegevens en een verzoek tot overdraagbaarheid van de eigen Persoonsgegevens.
- 3.7 Rekening houdend met de aard van de verwerking en de ter beschikking staande informatie, verstrekt de Verwerker de Verwerkingsverantwoordelijke de benodigde informatie in het kader van het kunnen uitvoeren van een Privacy Impact Assessment door de Verwerkingsverantwoordelijke.

4. Beveiligen Persoonsgegevens

- 4.1 Verwerker zorgt ervoor dat de Persoonsgegevens voldoende worden beveiligd. Om verlies en onrechtmatige verwerkingen te voorkomen neemt Verwerker passende technische en organisatorische maatregelen.
- 4.2 Deze maatregelen zijn afgestemd op het risico van de Verwerking. Een overzicht van deze maatregelen en het beleid daaromtrent wordt opgenomen in Bijlage 2.
- 4.3 Ter controle van de genomen beveiligingsmaatregelen zal Verwerker aan Verwerkingsverantwoordelijke ieder jaar een rapportage sturen waarin de genomen maatregelen staan en de eventuele aandachts- en/of verbeterpunten. Hiervoor brengt Verwerker geen kosten in rekening aan Verwerkingsverantwoordelijke.
- 4.4 Verwerkingsverantwoordelijke mag een audit laten uitvoeren om te bepalen of het verwerken van de Persoonsgegevens aan de wet en de afspraken uit deze Verwerkersovereenkomst voldoet. Verwerker verleent hierbij zijn medewerking, waaronder het toegang verlenen tot gebouwen en databases en het ter beschikking stellen van alle relevante informatie.
- 4.5 De kosten voor de uitvoering van deze audit zullen voor rekening van Verwerker komen wanneer blijkt dat Verwerker zich niet aan de verplichtingen in deze Verwerkersovereenkomst houdt.
- 4.6 De controle op de algehele verwerking van Persoonsgegevens door Verwerker kan, naast de auditmogelijkheid, ook geschieden via zelfevaluatie door Verwerker. Verwerker zal hierbij aan Verwerkingsverantwoordelijke een rapport verstrekken waarin Verwerker aantoont dat hij voldoet aan de wet en de afspraken uit deze

Verwerkersovereenkomst. Deze rapportage dient te worden ondertekend door een directielid binnen de organisatie van Verwerker.

- 4.7 Wanneer Partijen vinden dat een wijziging in de te nemen beveiligingsmaatregelen noodzakelijk is, treden Partijen in overleg over de wijziging daarvan. De kosten gemoeid met het wijzigen van de beveiligingsmaatregelen komen voor rekening van degene die de kosten maakt.

5. Exporteren Persoonsgegevens

- 5.1 Verwerker mag geen Persoonsgegevens laten verwerken door andere personen of organisaties buiten de Europese Economische Ruimte (EER), zonder daarvoor voorafgaande schriftelijke toestemming te hebben verkregen van Verwerkingsverantwoordelijke.

6. Geheimhouding

- 6.1 Verwerker zal de verstrekte Persoonsgegevens geheim houden, tenzij dit op basis van een wettelijke verplichting niet kan.
- 6.2 Verwerker zorgt dat zijn/haar personeel en ingeschakelde hulppersonen zich aan deze geheimhouding houden, door een geheimhoudingsplicht in de (arbeids)-contracten op te nemen.

7. Datalekken

- 7.1 In geval van een ontdekking van een mogelijk Datalek zal Verwerker Verwerkingsverantwoordelijke hierover informeren binnen een termijn van 24 uur overeenkomstig het proces volgend uit Bijlage 3, zodat Verwerkingsverantwoordelijke indien nodig een melding van het Datalek bij de Toezichthouder kan doen.
- 7.2 Verwerker zal Verwerkingsverantwoordelijke op de hoogte houden van nieuwe ontwikkelingen rondom het Datalek, ook zal Verwerker de getroffen maatregelen om het Datalek te beperken en te beëindigen en een soortgelijk incident in de toekomst te kunnen voorkomen, overleggen aan Verwerkingsverantwoordelijke.
- 7.3 Verwerker mag geen melding van een Datalek aan de Toezichthouder doen, wanneer bij het Datalek Persoonsgegevens van Verwerkingsverantwoordelijke betrokken zijn. Ook mag Verwerker de Betrokkenen niet informeren over het Datalek. Deze verantwoordelijkheid ligt bij Verwerkingsverantwoordelijke.
- 7.4 Eventuele kosten die gemaakt worden om het Datalek op te lossen en in de toekomst te kunnen voorkomen, komen voor rekening van degene die de kosten maakt.

8. Aansprakelijkheid

- 8.1 Als Verwerker de verplichtingen uit deze Verwerkersovereenkomst niet nakomt, kan Verwerkingsverantwoordelijke Verwerker daarvoor aansprakelijk stellen.
- 8.2 Verwerker is aansprakelijk voor alle schade die Verwerkingsverantwoordelijke lijdt door het niet nakomen van de wet en de bepalingen uit deze Verwerkersovereenkomst, voor zover dit is ontstaan door de werkzaamheden van Verwerker.

- 8.3 Indien Verwerker de verplichtingen in deze Verwerkersovereenkomst overtreedt, is Verwerker aan Verwerkingsverantwoordelijke een direct opeisbare boete verschuldigd van [BEDRAG] voor iedere overtreding en [BEDRAG] voor iedere dag dat Verwerker de overtreding begaat. Daarnaast behoudt Verwerkingsverantwoordelijke het recht om schadevergoeding te vorderen. (optioneel)
- 8.4 Verwerker is aansprakelijk voor de aan Verwerkingsverantwoordelijke opgelegde bestuurlijke boete door de Toezichthouder als de schade het gevolg is van het onrechtmatig of nalatig handelen van Verwerker.
- 8.5 Verwerkingsverantwoordelijke is niet aansprakelijk voor aanspraken van Betrokkene of andere personen en organisaties waar Verwerker de samenwerking mee is aangegaan of waarvan Verwerker Persoonsgegevens verwerkt, als dit het gevolg is van het onrechtmatig of nalatig handelen van Verwerker.

9. Teruggave Persoonsgegevens en bewaartermijn

- 9.1 Na het beëindigen van deze Verwerkersovereenkomst geeft Verwerker de Persoonsgegevens terug aan Verwerkingsverantwoordelijke.
- 9.2 De overgebleven Persoonsgegevens zal Verwerker vernietigen na verstrijken van de wettelijke bewaartermijn en/of op verzoek van Verwerkingsverantwoordelijke. Hierbij valt bijvoorbeeld te denken aan Persoonsgegevens die om belastingtechnische redenen bewaard moeten blijven.
- 9.3 Verwerker zal na de teruggave en/of vernietiging van de Persoonsgegevens schriftelijk aan Verwerkingsverantwoordelijke verklaren niet langer in het bezit te zijn van de Persoonsgegevens.

10. Toepasselijk recht en geschillenbeslechting

- 10.1 De Verwerkersovereenkomst en de uitvoering daarvan worden beheerst door het Nederlands recht.
- 10.2 Eventuele geschillen die tussen Partijen ontstaan, verband houdende met deze Verwerkersovereenkomst, worden voorgelegd aan de bevoegde rechter voor het arrondissement waarin de Verwerkingsverantwoordelijke gevestigd is.

11. Slotbepalingen

- 11.1 Deze Verwerkersovereenkomst is onderdeel van de Overeenkomst. Alle rechten en verplichtingen uit de Overeenkomst zijn daarom ook van toepassing op de Verwerkersovereenkomst.
- 11.2 Bij eventuele tegenstrijdigheden tussen de bepalingen in de Verwerkersovereenkomst en de Overeenkomst, gelden de bepalingen uit deze Verwerkersovereenkomst ten aanzien van de verwerking van Persoonsgegevens.
- 11.3 Afwijkingen van deze Verwerkersovereenkomst zijn slechts geldig wanneer Partijen dit samen schriftelijk afspreken.

Aldus door Partijen overeengekomen en ondertekend:

Verwerkingsverantwoordelijke:

Ondertekend voor en namens [STATUTAIRE NAAM]

Naam:

Functie:

Datum en plaats:

Handtekening:

Verwerker:

Ondertekend voor en namens [STATUTAIRE NAAM]

Naam:

Functie:

Datum en plaats:

Handtekening:

Bijlage 1: Overzicht met verwerkingen van Persoonsgegevens en verwerkingsdoelen

Het onderstaande schema zal ingevuld moeten worden elke keer dat een Verwerkersovereenkomst wordt gesloten. Het geeft een volledig overzicht van de Persoonsgegevens die verwerkt zullen worden. Dit maakt het makkelijker om aan te kunnen tonen waar, door wie en voor welk doel de Persoonsgegevens worden verwerkt.

Beschrijving verwerkingsactiviteiten door Verwerker:	
Verwerkingsdoelen:	
Verwerkingsverantwoordelijke:	
Verwerker:	
Sub-Verwerkers:	
Verwerkte Persoonsgegevens:	
Locatie verwerkingen:	
Bewaartermijn:	

Bijlage 2: Overzicht met beveiligingsmaatregelen

Overzicht van de beveiligingsnormen die de Verwerkingsverantwoordelijke aan de Verwerker oplegt.

Om vast te stellen wat passende beveiligingsmaatregelen zijn, moet een afweging worden gemaakt op basis van de risico's van de verwerking aan de hand van onder meer de volgende punten:

- Het soort Persoonsgegevens dat verwerkt wordt (normaal, bijzonder of gevoelig) en eventueel de daarbij behorende (risico)classificatie die de organisatie zelf aan de gegevens heeft gegeven. *Gaat het bijvoorbeeld om een naam of een e-mailadres, wat minder gevoelige Persoonsgegevens zijn, of gaat het om het verwerken van een BSN.*
- De hoeveelheid betrokkenen van wie gegevens worden verwerkt. *Hoe meer betrokkenen er zijn, hoe meer eisen er worden gesteld aan de beveiliging van de gegevens.*
- Het doel waarvoor gegevens worden verwerkt.
- De duur en de wijze waarop gegevens bewaard moeten worden.

Er kan vervolgens onderscheid gemaakt worden tussen organisatorische beveiligingseisen, zoals het voorkomen van diefstal van een laptop met daarop Persoonsgegevens uit de auto, en technische beveiligingseisen, zoals een uitgebreide IT-omgeving die beveiligd wordt tegen virussen en waar encryptie van de gegevens wordt toegepast. Van een grote organisatie wordt meer verwacht ten aanzien van de te nemen beveiligingseisen.

De onderstaande maatregelen zijn suggesties voor beveiligingsmaatregelen en de aanwezigheid hiervan kan een indicatie zijn van een gepast beveiligingsniveau.

Technische beveiligingsmaatregelen

- ☐ Up-to-date virusscanner op elke laptop, pc en tablet
- ☐ Beveiligde USB-sticks
- ☐ Accurate beveiliging medewerkerstelefoon
- ☐ Bitlocker toegangsmechanisme
- ☐ Unieke inlogcode en wachtwoord (regelmatig aanpassen)
- ☐ Versleutelde e-mail
- ☐ Geen onbeveiligde externe harde schijven
- ☐ Geen onbeveiligde back-ups maken
- ☐ Geen documenten op privé-laptop opslaan

Organisatorische beveiligingsmaatregelen

- ☐ Clean desk policy
- ☐ Laptop niet onbemand achterlaten
- ☐ Laptop nooit achterlaten in de auto
- ☐ Privacy screens medewerkers
- ☐ Oude documenten op juiste manier vernietigen
- ☐ Zorgvuldig gebruik van USB-sticks

Bijlage 3: Proces rondom het melden van Datalekken en de te verstrekken informatie

Wat is een beveiligingsincident en wanneer moet dit gemeld worden?

Een datalek is een beveiligingsincident waarbij Persoonsgegevens, die de Verwerker namens de Verwerkingsverantwoordelijke beheert, mogelijk verloren zijn gegaan of onbedoeld toegankelijk waren voor derden. Het gaat om gegevens die te koppelen zijn aan deze personen, zoals, maar niet beperkt tot, namen, adressen, telefoonnummers, e-mailadressen, login-gegevens, cookies, IP-adressen of identificerende gegevens van computers of telefoons.

Hieronder vind je een aantal voorbeelden van beveiligingsincidenten die moeten worden gemeld bij de Autoriteit Persoonsgegevens.

- De website met login-gegevens is gehackt of is toegankelijk voor derden.
- Verlies van een laptop of USB-stick met Persoonsgegevens.
- Salarisstroken van medewerkers zijn per ongeluk naar verkeerde personen gestuurd.
- Brieven of e-mails worden naar een verkeerd adres gestuurd.
- Een aanval van een hacker op het ICT-systeem.
- Een verloren of gestolen telefoon waar Persoonsgegevens op aanwezig zijn.

Wat te doen bij twijfel?

Als je op basis van bovenstaande niet zeker weet of er sprake is van een beveiligingsincident, stel je jezelf in ieder geval alvast de volgende vragen als hulpmiddel:

- Is er een technisch of fysiek beveiligingsprobleem?
- Gaat het probleem over de beveiliging van Persoonsgegevens? Ook IP-adressen, telefoonnummers of identificerende gegevens, bijvoorbeeld van hardware, kunnen hieronder vallen.
- Gaat het om gevoelige gegevens zoals ras, gezondheidsgegevens, informatie over iemands financiële situatie, zoals salaris of gegevens waar (identiteit)fraude mee kan worden gepleegd, zoals een Burgerservicenummer?
- Zijn er grote hoeveelheden Persoonsgegevens onbedoeld toegankelijk geworden voor derden?
- Gaat het om gegevens van kwetsbare groepen zoals kinderen?
- Worden de Persoonsgegevens beheerd door een leverancier?

Ook wanneer je twijfelt, neem het zekere voor het onzekere en neem altijd contact op met de [invoeren naam contactpersoon of afdeling].

Waar meld je het beveiligingsincident?

Als je een beveiligingsincident hebt ontdekt, neem je direct contact op met de [invoeren naam contactpersoon of afdeling]:

Telefoon: [invoeren telefoonnummer]

Of

E-mail: [invoeren e-mailadres]

Geef in je e-mail beantwoording op de onderstaande vragen

Wij willen graag dat je de onderstaande vragen voor ons beantwoord. Deze vragen zijn gelijk aan de informatie die aan de Autoriteit Persoonsgegevens moet worden verstrekt.

De [invoeren naam contactpersoon of afdeling] kan je helpen met de beantwoording hiervan. Gaarne de vragen zo volledig mogelijk en schriftelijk beantwoorden.

1. Geef een samenvatting van het beveiligingslek/beveiligingsincident/datalek: wat is er gebeurd? Vermeld hier ook de naam van het betrokken systeem.
2. Welke typen Persoonsgegevens zijn betrokken bij het beveiligingsincident? Zoals, maar niet beperkt tot, naam, adres, e-mailadres, IP-nummer, Burgerservicenummer, pasfoto en ieder ander tot een persoon te herleiden gegeven.
3. Van hoeveel personen zijn de Persoonsgegevens betrokken bij het beveiligingsincident?
Geef a.u.b. een minimum en maximum aantal personen.
4. Omschrijving groep personen om wiens gegevens het gaat.
Geef aan of het gaat om medewerkersgegevens, gegevens van internetgebruikers. Bijzondere aandacht verdienen gegevens van een kwetsbare groepen personen, zoals kinderen.
5. Zijn de contactgegevens van de betrokken personen bekend?
Het kan zijn dat betrokkenen geïnformeerd moeten worden over het datalek, kunnen we deze personen in dat geval bereiken?
6. Wat is de oorzaak (root cause) van het beveiligingsincident?
Heeft u een idee hoe het beveiligingsincident heeft kunnen ontstaan?
7. Op welke datum of in welke periode heeft het beveiligingsincident plaats kunnen vinden?
Geef dit a.u.b. zo specifiek mogelijk aan.

Toestemmingsformulier voor Gegevensverwerking NVAO

(afdeling Nederland)

Informatie over gegevensverwerking

NVAO NL hecht veel waarde aan uw privacy en behandelt uw persoonsgegevens met de grootst mogelijke zorg. Wij verwerken uw gegevens uitsluitend in overeenstemming met de geldende wet- en regelgeving en ons privacybeleid.

Doel van de gegevensverwerking

Wij verwerken uw persoonsgegevens voor de volgende doeleinden:

- VB Het uitvoeren van accrediteringsprocedures.
- VB Het onderhouden van communicatie met betrokkenen.
- VB Het verbeteren van onze diensten en processen.

Soorten persoonsgegevens die wij verwerken

Wij kunnen de volgende gegevens van u verwerken:

- Naam :
- E-mailadres :
- Telefoonnummer :
- Organisatie :
- Functie :
- Overige relevante informatie die u aan ons verstrekt :

Duur van gegevensopslag

Uw persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor ze zijn verzameld, met inachtneming van de wettelijke bewaartermijnen.

Beveiliging van uw gegevens

Wij nemen passende technische en organisatorische maatregelen om uw persoonsgegevens te beschermen tegen verlies of onrechtmatige verwerking. Dit omvat onder andere encryptie van gegevens en het beperken van toegang tot uw informatie.

Uw rechten

U heeft recht op toegang tot uw persoonsgegevens, rectificatie, verwijdering, beperking van de verwerking en overdracht van uw gegevens. Tevens heeft u het recht om bezwaar te maken tegen de verwerking van uw persoonsgegevens. Wij moedigen u aan om deze rechten uit te oefenen indien nodig.

Toestemming

Door dit formulier in te vullen en te ondertekenen, geeft u toestemming voor de verwerking van uw persoonsgegevens door de Nederlands-Vlaamse Accreditatieorganisatie (NVAO NL) voor de bovengenoemde doeleinden. U kunt uw toestemming altijd intrekken door contact met ons op te nemen. Het intrekken van toestemming heeft geen terugwerkende kracht; alle verwerkingen die al hebben plaatsgevonden blijven rechtmatig.

Contactinformatie

Als u vragen heeft over dit formulier of over hoe wij omgaan met uw persoonsgegevens, kunt u contact met ons opnemen via:

Nederlands-Vlaamse Accreditatieorganisatie (Afdeling NL)

E-mailadres: privacy@nvao.net

Wij streven ernaar om uw privacy te respecteren en te waarborgen en bedanken u voor uw vertrouwen.

Handtekening Naam : _____

Handtekening : _____

Datum : _____

20

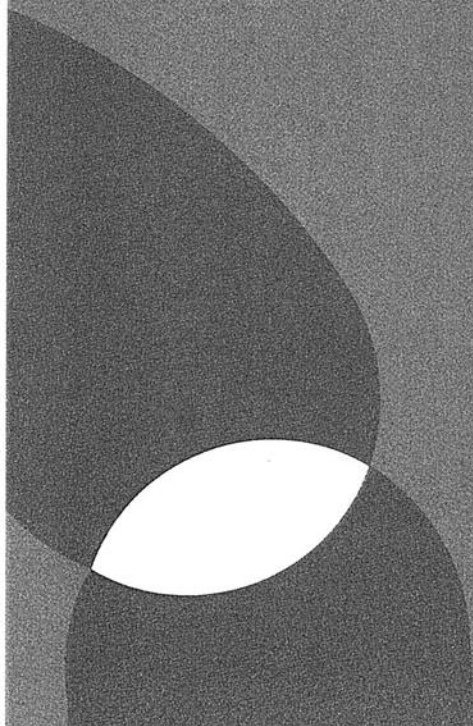


NVAO • NEDERLAND

PERSONEELSREGELING

NVAO NL, CDHO EN CMMBO

JANUARI 2025

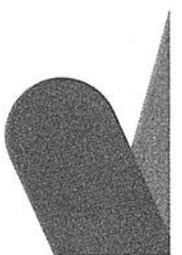


NVAO • NEDERLAND

PERSONEELSREGELING

NVAO NL, CDHO EN CMMBO

JANUARI 2025



[REDACTED]

2.2 AVG

De AVG is een privacywet die sinds 25 mei 2018 van kracht is in de hele Europese Unie (EU). Met de invoering van de AVG is de bescherming van persoonsgegevens in alle EU-landen op dezelfde manier geregeld.

Binnen de NVAO is de *Handreiking Veilige omgang Persoonsgegevens* van toepassing op alle medewerkers, evenals op gedetacheerden en ingeleend personeel. De volledige regeling is te vinden op het Intranet.

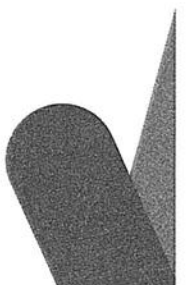


Handreiking Veilige omgang persoonsgegevens

1 september 2021

Handreiking Veilige omgang persoonsgegevens

1 september 2021



Inleiding

De Algemene Verordening Gegevensbescherming stelt dat persoonsgegevens veilig en zorgvuldig moeten worden verwerkt. Iedere medewerker van de NVAO, CDHO en CMMBO (verder samen te noemen "de NVAO") heeft hier voortdurend mee te maken. Bij binnenkomst van het pand, het inloggen in je computer, communiceren met collega's en externen, het gebruik maken van de (digitale) middelen die door de NVAO worden aangeboden, het weggooien van papier, en ga zo maar door.

Deze handreiking geeft weer op welke manier de NVAO verwacht hoe zijn medewerkers - en externen die in opdracht van de NVAO werkzaamheden verrichten - met middelen omgaan, die persoonsgegevens kunnen bevatten en waarmee persoonsgegevens kunnen worden verwerkt. N.B. Deze handreiking is van toepassing op medewerkers van de CDHO of CMMBO conform de hostingsovereenkomsten met de NVAO. Externen die in opdracht van de CDHO of CMMBO werkzaamheden verrichten vallen onder de regelingen van OCW.

Verder is deze handreiking specifiek bedoeld als aanvulling op het Huisreglement (bijlage 1 van de Personeelsregeling) en de Integriteitscode die aansluit bij de Gedragscode Integriteit Rijk, waarin de nodige bepalingen staan, over o.a. bedrijfsmiddelen, usb-gebruik, virusbeveiliging, bezoek, goed werkgever- en werknemerschap, gebruik van publieke middelen enzovoort.

De diverse onderwerpen die van belang zijn voor een veilige omgang met persoonsgegevens staan hieronder op alfabetische volgorde.

Met persoonsgegevens worden dezelfde gegevens bedoeld zoals in het Privacy beleidskader omschreven en in de diverse privacyverklaringen genoemd.

Inhoud

1	Anonimiseren	6
2	Archief	6
3	Bedrijfsmiddelen	6
4	Bezoek	6
5	Contact	6
6	Datalek	6
7	Dataminimalisatie	6
8	Disclaimer	7
9	Eed/belofte	7
10	Encryptie	7
11	E-mail, beveiliging?	7
12	E-mail, bewaren	8
13	E-mail, controleer het adres van de ontvanger	8
14	E-mails, opschonen	8
15	E-mail, verdachte berichten	8
16	E-mail, verkeerd verzonden	8
17	Gedragsregels	8
18	Geheimhoudingsverklaring	9
19	Gebruik van e-mail en internet	9
20	IT-systeem van de NVAO	9
21	Media	9
22	OneDrive	9
23	Openbaar Vervoer	9
24	Papier met persoonsgegevens of vertrouwelijke informatie	9
25	Pseudonimiseren	10
26	Registratie of monitoren	10
27	Schermb beveiliging of screensaver	10
28	Sleutels	10
29	Social media	10
30	Teams	10
31	Thuiswerken of onderweg naar huis	11
32	USB-stick	11
33	Verdachte omstandigheden	11
34	Verlies of diefstal	11
35	Videoconferencing	11

36	Virus	11
37	Wachtwoorden, toegangscode.....	11
38	Whatsapp	12
39	Zorgvuldigheid, goed werkgever- en werknemerschap.....	12
40	Slotbepaling.....	12

1 Anonimiseren

Het is niet altijd noodzakelijk om directe persoonsgegevens te delen met derden. Anonimiseren is een extra beveiligingsmaatregel, zie E-mail, beveiliging?

2 Archief

De fysieke archieven zijn alleen toegankelijk voor de medewerkers die daarvoor zijn geautoriseerd. Wie geautoriseerd zijn voor de diverse fysieke archieven is te vinden in de bijlage van deze handreiking. Wie geautoriseerd zijn voor diverse digitale archieven is te vinden in het Autorisatiebeleid.

3 Bedrijfsmiddelen

Medewerkers krijgen bedrijfsmiddelen (denk aan bijvoorbeeld een telefoon) ter beschikking gesteld. Dit wordt geregistreerd en er wordt getekend voor ontvangst. Zodra de medewerker de NVAO weer verlaat, levert deze de bedrijfsmiddelen in (voor afloop van de arbeidsovereenkomst/detachering/etc) bij HR. Zie bij Zorgvuldigheid.

4 Bezoek

Bezoekers die binnenkomen mogen niet zonder meer doorlopen, maar dienen te worden opgehaald door degene die het bezoek heeft uitgenodigd. De contactpersoon is gedurende het bezoek tot en met het vertrek verantwoordelijk voor de begeleiding van de bezoeker.

5 Contact

Neem bij twijfel of vragen over privacy aangelegenheden contact op met JZ via privacy@nvao.net.

6 Datalek

Bij een datalek gaat het om toegang tot, vernietiging, wijziging of het vrijkomen van persoonsgegevens zonder dat dit de bedoeling is van de medewerker. Krijg je te maken met een datalek of vermoed je een datalek, neem dan contact op met privacy@nvao.net. Zie ook het Protocol Datalekken NVAO.

7 Dataminimalisatie

Het is goed om na te gaan of alle persoonsgegevens wel daadwerkelijk verstuurd moeten worden. Zo min mogelijk persoonsgegevens versturen is een extra beveiligingsmaatregel, zie E-mail, beveiliging?

8 Disclaimer

Een disclaimer onderaan een e-mail sluit de aansprakelijkheid uit. Een verzoek om verkeerd verzonden berichten te verwijderen (zie *E-mail, verkeerd verzonden*) sluit geen aansprakelijkheid uit, maar is voor de veilige omgang van persoonsgegevens van belang en kan aan een disclaimer worden gekoppeld.

9 Eed/belofte

Zie *Geheimhoudingsverklaring* en de *Personeelsregeling* voor de gehele tekst van de eed/belofte.

10 Encryptie

Encryptie is een methode waarbij gegevens zodanig worden versleuteld dat ze niet meer in de oorspronkelijke vorm beschikbaar zijn en niet kunnen worden gelezen. Encryptie is dus een extra beveiligingsmaatregel om persoonsgegevens te versturen, zie *E-mail, beveiliging*?

11 E-mail, beveiliging?

Bij het verwerken (lees: e-mailen) van persoonsgegevens moet je je gezond verstand gebruiken en zorgvuldig afwegen of het versturen van persoonsgegevens op veilige wijze kan gebeuren via de e-mail of dat extra beveiliging nodig is.

Wanneer je kiest voor e-mail, zijn er een aantal zaken, waarmee je rekening moet houden:

- de gevoeligheid van de persoonsgegevens die je gaat versturen;
- de hoeveelheid persoonsgegevens (en van hoeveel betrokkenen) die je gaat versturen;
- naar hoeveel ontvangers je deze persoonsgegevens gaat sturen; en
- andere omstandigheden die relevant zouden kunnen zijn.

Wanneer je beoordeelt dat er op basis van bovenstaande omstandigheden een verhoogd risico is op het onrechtmatig verwerken van persoonsgegevens (bijvoorbeeld doordat de gegevens naar een verkeerde ontvanger kunnen worden gestuurd) dan is het verstandig om extra beveiligingsmaatregelen te nemen om de persoonsgegevens verder te beschermen

Extra beveiligingsmaatregelen kunnen zijn:

1. Dataminimalisatie

Bij het versturen van persoonsgegevens over de e-mail is het goed om na te gaan of alle persoonsgegevens wel daadwerkelijk noodzakelijk zijn om te versturen (via de e-mail) om het gewenste doel te bereiken. Kan de ontvanger ook zonder (een deel) van de persoonsgegevens zijn of haar doel bereiken?

2. Pseudonimiseren/ Anonimiseren

Het is niet altijd noodzakelijk om directe persoonsgegevens te delen met derden. Wanneer de ontvanger hetzelfde doel kan bereiken door met gepseudonimiseerde of geanonimiseerde gegevens te werken dan is het zeer gewenst (en in de meeste gevallen zelfs verplicht) om dit in die vorm te delen met de ontvanger.

3. Encryptie

Wanneer er een bestand met persoonsgegevens van meerdere betrokkenen (bijv. een Excellijst met namen) naar een derde partij wordt verstuurd, is het gebruiken van encryptie verplicht. De meest simpele vorm hiervan is het te versturen bestand te voorzien van een wachtwoord. Dit wachtwoord verzend je via een sms of een andere e-mail aan de ontvanger (nadat je de juistheid van het adres nogmaals hebt gecheckt).

4. Gegevens delen via een beveiligd portaal

Indien de gegevens die je via de e-mail wilt versturen ook voor de ontvanger via een web-

portaal, zoals Office365 (TEAMS/SharePoint) beschikbaar zijn, dan verwijst je naar het web-portaal om de gegevens in te zien.

5. Een ander middel gebruiken

Wanneer de conclusie is dat het een te hoog risico met zich meebrengt om de persoonsgegevens via een e-mail te versturen, is het verstandig om een ander medium te kiezen. Per post of koerier zijn opties, maar niet in alle gevallen veiliger.

Wanneer bijvoorbeeld een mail met een cv naar een derde moet worden verstuurd, is het noodzakelijk hiervoor aanvullende maatregelen te treffen. Beveiliging van e-mails en e-mailbestanden gaat via Office365. Als alternatief kunnen encryptietechnieken worden toegepast op het bestand zelf.

Bijzondere persoonsgegevens (bijvoorbeeld over iemands strafrechtelijk verleden) of gevoelige persoonsgegevens (bijvoorbeeld over iemands inkomen of privésituatie) mogen niet per e-mail verstuurd worden. Indien dit vanuit HR-oogpunt toch noodzakelijk is om het algemeen belang of het belang van betrokkene te borgen, moeten aanvullende beveiligingsmaatregelen worden genomen, zoals hierboven vermeld.

12 E-mail, bewaren

Bewaar e-mails niet langer dan noodzakelijk. Zie ook *E-mail, opschonen*.

13 E-mail, controleer het adres van de ontvanger

Controleer het e-mailadres zorgvuldig. Stuur eventueel zelf eerst een e-mail, die de ontvanger kan beantwoorden.

LET OP: bij het sturen van persoonsgegevens in een e-mail aan een verkeerde persoon, is er vrijwel altijd sprake van een "datalek": Zie *Datalek* en het Protocol datalekken NVAO. Neem bij twijfel of vragen contact op met JZ via privacy@nvao.net

14 E-mails, opschonen

Schoon je e-mail box regelmatig en ten minste één keer per jaar op. Beleid volgt (P.M.). Zie ook *E-mail, bewaren*.

15 E-mail, verdachte berichten

Open geen verdachte e-mailberichten die mogelijk SPAM, virussen en/of phishing bevatten. Stuur verdachte berichten altijd toe aan je IT-verantwoordelijke. Mocht er twijfel bestaan over een verdacht e-mailbericht, neem dan ook contact op met de IT-verantwoordelijke.

16 E-mail, verkeerd verzonden

Een te verzenden e-mailbericht vanaf de NVAO-account bevat een verzoek van de NVAO, ongeacht of dit een persoonlijk e-mailbericht is, zodat ontvangers verzocht worden om verkeerd verzonden berichten te verwijderen.

"Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en dit bericht te verwijderen."

17 Gedragsregels

Spreek elkaar aan op het overtreden van gedragsregels en meld het overtreden van gedragsregels zo nodig bij je leidinggevende en/of de IT-verantwoordelijke. Dit melden kan zowel gaan om overtredingen van jezelf (bijv. het per ongeluk sturen van een vertrouwelijke e-mail aan een externe partij c.q. het verkeerde kantoor) als (on)bewuste overtredingen van anderen. Bij datalekken, informeer ook de juristen (privacy@nvao.net).

18 Geheimhoudingsverklaring

Diegenen die de eed of belofte hebben afgelegd bij de NVAO hebben gezworen of beloofd: "...dat ik plichtsgetrouw en nauwgezet de mij opgedragen taken zal vervullen en zaken die mij uit hoofde van mijn functie vertrouwelijk ter kennis komen of waarvan ik het vertrouwelijke karakter moet inzien, geheim zal houden voor anderen dan die personen aan wie ik ambtshalve tot mededeling verplicht ben."

Externe partijen en gedetacheerden die in opdracht van de NVAO werkzaamheden verrichten tekenen een geheimhoudings- of integriteitsverklaring.

19 Gebruik van e-mail en internet

E-mail en internet zijn in beginsel voor zakelijk gebruik; persoonlijk gebruik is beperkt toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden van de betrokken medewerker of de collega's en het de goede werking van het netwerk niet verstoort. Stuur geen zakelijke informatie door naar je privé-e-mailadres of privé-telefoon.

Teams: Gebruik Teams voor het versturen van berichten in plaats van andere messaging applicaties.

20 IT-systeem van de NVAO

Het opslaan van informatie in de IT-systemen van de NVAO is alleen toegestaan via het beveiligde netwerk van de NVAO. Wijzigingen in het IT-systeem worden in een log bijgehouden. Het is in het algemeen niet de bedoeling dat thuiswerken hierdoor wordt bemoeilijkt. Dit beleid wordt nader uitgewerkt (technisch).

21 Media

Indien een medewerker door een journalist of een persoon die werkzaam is voor een (social)mediabedrijf rechtstreeks wordt benaderd, moet de laatstgenoemde persoon altijd naar de directeur doorverwezen worden en wordt in afstemming met Communicatie een reactie/beantwoording opgepakt. *Zie ook evt. social media en whatsapp.*

22 OneDrive

Gebruik uitsluitend OneDrive om persoonlijke vertrouwelijke bestanden op te slaan. Het opslaan van persoonlijke bestanden (zakelijk en privé) mag de goede werking van het netwerk niet verstoren.

23 Openbaar Vervoer

Zie Thuiswerken of onderweg naar huis.

24 Papier met persoonsgegevens of vertrouwelijke informatie

Om stukken te printen kun je de toegangspas gebruiken of een printcode. Laat prints en faxen niet voor anderen zichtbaar liggen.

Uitgangspunt is een clean desk policy. Hierdoor wordt de kans op oneigenlijk gebruik van vertrouwelijke informatie en datalekken verkleind. Berg alle geprinte stukken op buiten het zicht van anderen. Dit sluit aan bij het flexibel werken op Parkstraat 83 en de afspraken die hierover gemaakt zijn.

Papier met persoonsgegevens of vertrouwelijke informatie dat je niet meer nodig hebt, moet altijd worden weggegooid in een gesloten blauwe bak. Gooi papier niet weg in een open papierbak/vuilnisbak – thuis noch op kantoor.

25 Pseudonimiseren

Het is niet altijd noodzakelijk om directe persoonsgegevens te delen met derden. Pseudonimiseren is een ander woord voor anonimiseren; dit is een extra beveiligingsmaatregel, zie *E-mail, beveiliging?*

26 Registratie of monitoren

Beleid P.M.

27 Schermbeveiliging of screensaver

Pc's en laptops zijn voorzien van een screensaver of schermbeveiliging. Je gebruikt schermbeveiliging voor als je niet achter je pc, laptop of tablet zit ter voorkoming van oneigenlijk gebruik van informatie. Wanneer je van je werkplek/laptop wegloopt, zet je het scherm met Windows+L (voor de meeste computers) op beveiligingsmodus. Je kunt zelf instellen na hoeveel minuten inactiviteit de schermbeveiliging er automatisch opgaat. Door het invoeren van je wachtwoord wordt dit weer ongedaan gemaakt.

28 Sleutels

De uitgifte van een toegangspas wordt gedaan door HR. De toegangspas geeft toegang tot de parkeergarage (inclusief fietsenstalling) en het gebouw zelf. De NVAO is evenwel uitsluitend op de volgende openingstijden toegankelijk voor personeel en servicediensten: Maandag tot en met vrijdag van 7.00-21.00.

Buiten deze tijden is er geen toegang tot de NVAO. Externe en tijdelijke medewerkers krijgen ook de beschikking over een toegangspas. Berg toegangspas en sleutels van de kasten altijd veilig en uit het zicht op; leen deze niet uit.

29 Social media

Werknemers mogen actief zijn op social media, mits de informatie die wordt gedeeld: geen werkgerelateerde vertrouwelijke informatie bevat (zie ook Geheimhoudingsverklaring en de Personeelsregeling); de NVAO en haar medewerkers niet op enige wijze schade toebrengt; en de werkzaamheden van de werknemers er niet onder lijden.

Iedere werknemer is persoonlijk verantwoordelijk voor zijn gedragingen in het kader van social media. Alles wat de werknemer publiceert, dat het imago van de NVAO schaadt of anderszins schadelijk is of kan zijn voor de organisatie, valt onder verantwoordelijkheid van de betrokken medewerker.

De werknemer is zich ervan bewust dat alles wat hij publiceert mogelijk voor langere tijd gewenst of ongewenst openbaar zal zijn, met mogelijke gevolgen voor zijn privacy en/of de geheimhoudingsplicht.

30 Teams

Zie *Gebruik van e-mail en internet*.

31 Thuiswerken of onderweg naar huis

Voor het zorgvuldig thuiswerken op door de NVAO ter beschikking gestelde (digitale) middelen wordt/is aan alle medewerkers een of meerdere bruikleenovereenkomst(en) uitgereikt, die ook door de medewerker moet worden ondertekend. Deze overeenkomsten worden bewaard bij de personeelsdossiers.

Vervoer documenten en communicatiemiddelen buiten het zicht in een afgesloten tas of koffer. Laat ze nooit onbeheerd achter, bijvoorbeeld op de achterbank van je auto.

Houd de tas of koffer in principe gesloten als je met het openbaar vervoer reist. Let op welke stukken je leest in het openbaar vervoer en wat de zichtbaarheid daarvan is voor derden. Ga geen stukken lezen waarin individuele gegevens voorkomen.

Berg documenten en communicatiemiddelen thuis ook goed op. Bewust en zorgvuldig omgaan met NVAO documenten en communicatiemiddelen wordt van iedereen verwacht. Bij diefstal van fysieke dossiers/stukken wordt na overleg met de directie aangifte gedaan.

Leen je pc, laptop, smartphone of tablet niet uit aan anderen, ook niet aan familieleden.

32 USB-stick

Het overdragen van digitale informatie door gebruikmaking van een USB-stick is alleen toegestaan als de USB-stick door je IT-verantwoordelijke versleuteld is of op een door de IT-verantwoordelijke voorgeschreven wijze is beveiligd.

Overige externe gegevensdragers, bijvoorbeeld een externe harde schijf, worden altijd pas na overleg met de IT-verantwoordelijke in gebruik genomen.

33 Verdachte omstandigheden

Meld verdachte omstandigheden bij je leidinggevende en je IT-verantwoordelijke. Zie verder *Zorgvuldigheid*.

34 Verlies of diefstal

Doe bij verlies of diefstal van (bedrijfs)middelen altijd direct aangifte bij de politie. Meld dit zo snel mogelijk bij je leidinggevende en bespreek dit met het privacy office, zodat onderzocht kan worden of er (tevens) sprake is van een datalek.

35 Videoconferencing

Binnen de NVAO wordt in principe alleen gebruik gemaakt van Microsoft Teams voor digitale gesprekken.

Wees terughoudend in het gebruik van andere applicaties hiervoor. Indien je Zoom wil gebruiken, zorg er dan voor dat je gebruik maakt van één van de betaalde accounts van de NVAO. Zet de instelling zo dat er altijd een password nodig is en dat er "gebeld" wordt vanuit de EU. Op die manier ben je ervan verzekerd dat de data-uitwisseling onder de Europese wetgeving valt.

36 Virus

Zie *E-mail, verdachte berichten*

37 Wachtwoorden, toegangscode

Hanteer een wachtwoord voor de mobiele telefoon, laptop en tablet of andere mobiele apparatuur. Na diefstal bemoeilijkt dit het misbruiken van gegevens op de telefoon. Deel uw wachtwoord nooit met anderen. Niet met directe collega's noch met systeembeheerders of medewerkers van de servicedesk. Een systeembeheerder heeft immers geen wachtwoord nodig om bij calamiteiten toegang te krijgen tot het account.

Er worden kwaliteitseisen gesteld aan wachtwoorden, die inbraakpogingen bemoeilijken en die door het gebruikte IT systeem opgelegd worden. Het is niet verstandig (een deel van) de eigen naam te gebruiken; verzin een sterk wachtwoord; het systeem geeft aan waaraan je wachtwoord moet voldoen.

Elke 150 dagen dient het wachtwoord te worden gewijzigd; het nieuwe wachtwoord mag niet gelijk zijn aan één van de voorgaande 3 wachtwoorden.

Na 10 keer een verkeerd wachtwoord te hebben ingevuld, wordt het account vergrendeld en geblokkeerd. Er zal daarna contact moeten worden opgenomen met de IT-verantwoordelijke. Schrijf wachtwoorden en toegangscode's nooit op; gebruik desnoods ezelsbruggetjes.

38 Whatsapp

Gebruik geen Whatsapp voor zakelijk verkeer. Dit is hier niet voor geschikt.

39 Zorgvuldigheid, goed werkgever- en werknemerschap

Laat mobiele apparatuur nooit onbeheerd achter.

Ga zorgvuldig te werk wanneer er een mobiele telefoon, laptop, tablet of andere mobiele apparatuur in openbare ruimten worden gebruikt. Denk ook aan de nodige risico's bij het gebruik van openbare Wi-Fi.

Lever bij uitdiensttreding alle bedrijfsmiddelen in bij HR.

Update je software op telefoon, laptop, tablet, apps en pc zodra het apparaat dit aangeeft. Meld verdachte omstandigheden bij je leidinggevende en je IT-verantwoordelijke. Dit betreft ook zaken als computervirussen of andere onverwachte meldingen van het IT-systeem. Stop met waar je mee bezig was; neem met een ander communicatiemiddel contact op met je IT-verantwoordelijke; schakel niet direct je pc uit, maar overleg eerst. Ga niet naar het netwerk of je account.

Wees alert op manipulatie van handtekeningen, stempels en andere validatiemiddelen. Indien er twijfel bestaat over de echtheid van een bepaald validatiemiddel of wanneer er op andere wijze sprake is van fraude, zal dit bij je leidinggevende gemeld moeten worden. Bij vermeende fraude zal aangifte worden gedaan.

40 Slotbepaling

Deze Handreiking veilige omgang persoonsgegevens is een eerste uitwerking van het Privacy Beleidskader (dat op 15 maart 2021 werd goedgekeurd door het Algemeen Bestuur) en werd vastgesteld door het gemandateerde DB op 24 augustus 2021 na instemming van de OR. Deze Handreiking treedt per 1 september 2021 in werking.

Diverse ondersteunende afdelingen leverden hun input voor deze Handreiking, zoals IT, HR en Communicatie. Het Privacy Office beheert deze handreiking en is afhankelijk van de samenwerking met andere afdelingen voor een goed beheer van de inhoud.

Deze Handreiking wordt ieder jaar op juistheid getoetst. Wijzigingen worden t.z.t. in een versiebeheer hieronder bijgehouden.

Colofon

Handreiking Veilige omgang met Persoonsgegevens

1 september 2021

Samenstelling: NVAO



Nederlands-Vlaamse Accreditatieorganisatie
Accreditation Organisation of the Netherlands and Flanders

Parkstraat 83 2514 JG Den Haag
P.O. Box 85498 2508 CD The Hague
The Netherlands

T +31 (0)70 312 23 00
E info@nvao.net
www.nvao.net

Toestemmingsverklaring gebruik beeldmateriaal NVAO

Ondergetekende:

Naam:

Adres:

Postcode en woonplaats:

Telefoonnummer:

E-mailadres:

verklaart hierbij dat hij/zij aan de **Nederlands-Vlaamse Accreditatieorganisatie (NVAO)** toestemming geeft voor het gebruik van beeldmateriaal (foto's en/of video-opnames) waarop ondergetekende herkenbaar in beeld is.

Doeleinden van gebruik

De NVAO mag het beeldmateriaal gebruiken voor de volgende doeleinden:

- Publicatie op de website van de NVAO;
- Gebruik in nieuwsbrieven, rapportages en sociale media van de NVAO;
- Gebruik in interne en externe communicatie-uitingen (zoals presentaties, brochures en jaarverslagen).

Voorwaarden

1. Het beeldmateriaal wordt uitsluitend gebruikt voor bovengenoemde doeleinden.
2. De toestemming geldt voor onbepaalde tijd, tenzij ondergetekende deze schriftelijk intrekt. Intrekking kan op elk moment, waarna het materiaal niet meer voor nieuwe publicaties zal worden gebruikt.
3. De NVAO gaat zorgvuldig om met het beeldmateriaal en zal dit niet aan derden verstrekken voor commerciële doeleinden.

Uw rechten

U heeft op grond van de Algemene verordening gegevensbescherming (AVG) het recht om:

- Uw toestemming op elk moment in te trekken;
- Inzage te vragen in de gegevens die de NVAO van u verwerkt;
- Correctie of verwijdering van het beeldmateriaal te verzoeken.

Voor vragen of verzoeken kunt u contact opnemen met de **Functionaris Gegevensbescherming van de NVAO** via privacy@nvao.net.

Verklaring ondertekenaar

Ik verklaar kennis te hebben genomen van bovenstaande informatie en ga akkoord met het gebruik van beeldmateriaal zoals omschreven.

Plaats:

Datum:

Handtekening:

Naam (voluit):



DB VERSLAG

FASTGESTELD VERSLAG

dd. 16/02/2021

21DB07 - Dagelijks Bestuur

Datum

dinsdag 16 februari 2021

Tijd

10u30 - 12u30

Bijlagen

3

Locatie

NVAO, Den Haag

Artikel 5.1 lid 2 sub e

Aanwezig

Anne Flierman (voorzitter); Wouter Duyck (neemt niet deel aan beraadslaging over de aanvragen van de Universiteit Gent); Anneke Luijten-Lub (neemt niet deel aan beraadslaging over de aanvragen van de Hanzehogeschool); Luut Kroes; Axel Aerden

Afwezig met kennisgeving

Artikel 5.1 lid 2 sub e

0. OPENING

BR

3.1

3.2

3.3

BR

3.4

3.5

4.1

BR

5.1

5.2

BR

5.3

5.4

5.5

5.6

BR

5.7

6.1

4.2

BR

4.3 Privacybeleidskader NVAO

Het DB gaat akkoord met het afhandelvoorstel. (actiepunt DB/JUZA)

Het DB stelt vast dat het eens is met het voorgestelde privacybeleidskader.

BR

Besluit 18

Het DB stemt in om het Algemeen Bestuur te vragen om mandaat te verlenen aan het DB voor het opstellen van beleid t.a.v. privacy aangelegenheden (en aan te passen in de mandaatregeling op een later moment).

Besluit 19

Het DB stemt in met het voorleggen van het concept Privacy Beleidskader (versie 0.4) aan het Algemeen Bestuur.

Besluit 20

Het DB stemt in met het aanpassen van het Privacy Beleidskader door het privacy office indien dit geen inhoudelijke wijzigingen zijn en slechts naam- of nummeringswijzigingen. Het DB wordt geïnformeerd over eventuele wijzigingen.

6.4

6.5

BR

7.1

8.1

8.2

8.3

BR

10.1

10.2

BR

Den Haag, 16 februari 2021

Anne Flerman
(voorzitter)

Artikel 5.1 lid 2 sub e



NVAO

AB VERSLAG

FASTGESTELD VERSLAG

ed. 15/03/2021

21AB01 - Algemeen Bestuur

Datum

Maandag 15 maart 2021

Tijd

14u30 - 17u00

Locatie

Digitaal

Art 5.1 lid 2e

@nvao.net

@nvao.net

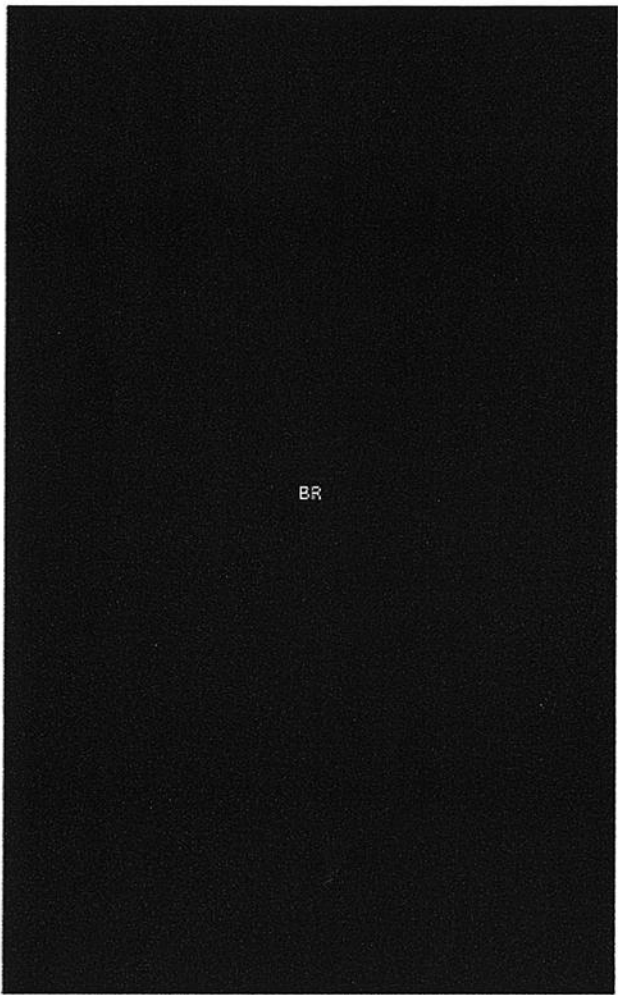
Aanwezig

A. F. Berman (voorzitter); W. Duyck (vicevoorzitter); L. Behoydt (lid AB); J. Beysens (lid AB); J. Hulsman (lid AB); M. Koster-Wentink (lid AB); M. Krom (lid AB); A. Lütjen-Lub (lid DB); T. Omta (lid AB); M. van Straalen (lid AB); L. Kroes (directeur afdeling Nederland); A. Aerden (directeur afdeling Vlaanderen);

Art 5.1 lid 2 e

Afwezig met kennisgeving

BR



BR

Document released under the provisions of the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

BR

6.2 Privacy Beleidskader

Luit Kroes geeft aan dat dit kader dient als fundament voor het privacy beleid. Wanneer er veranderingen in de organisatie komen, dan wordt o.e.s. aangepast.

Thuis Omte begrijpt dat het AB over deze kwestie een mandaat verleent aan het DB. Luit Kroes antwoordt dat de mandaatregeling over privacy nog was niet geregeld en daarvoor dit mandaat nodig was. Daarnaast is de vaststelling van het privacy beleid nodig.

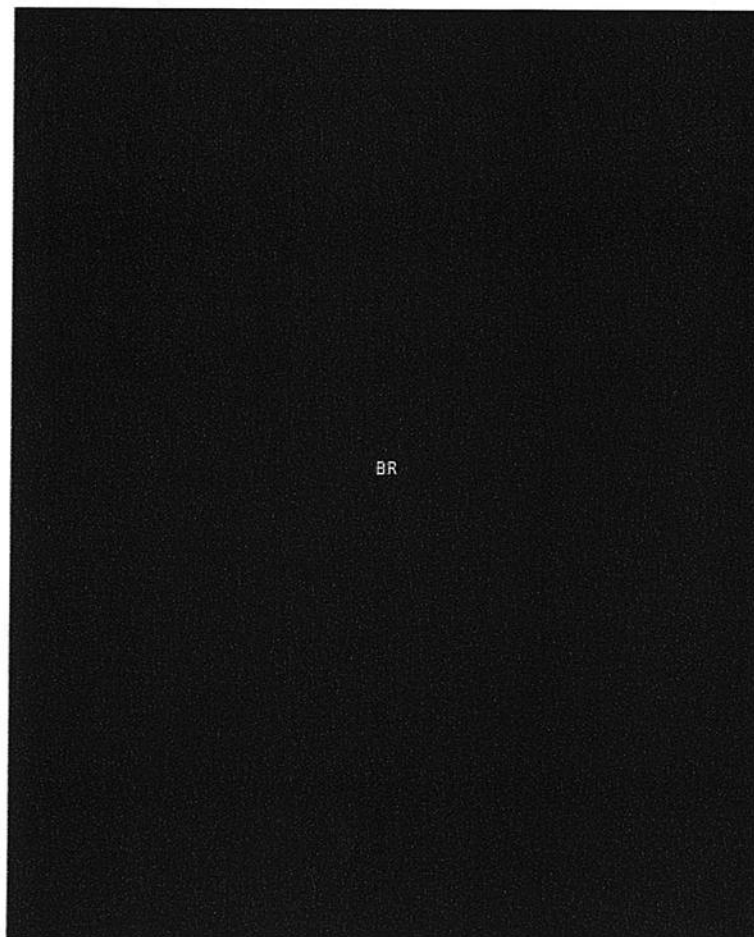
Wouter Duyck geeft aan dat VL een apart kader hanteert dat in alle instellingen is ingevoerd. VL schikt zich nu naar de NL regeling, maar wanneer de VL entiteit wordt opgericht, zal de General Data Protection Regulation (GDPR) gelden.

Thuis Omte meent dat de AVG een Europese aangelegenheid is.

Anne Flinterman licht toe dat de GDPR een Europese regeling is die rechtstreeks doorwerkt en in NL, en in VL, op dezelfde manier van kracht is. Zolang wij spreken over een NL zbo, geldt de privacywetgeving ook voor de VL medewerkers. Bij wijziging naar NVAO 2.0 zal de VL entiteit de VL regels op het gebied van privacy volgen. Hij concludeert dat het AB de uitwerking van het privacy beleidskader accordeert.

Result 4

Het Algemeen Bestuur gaat akkoord met het Privacy Beleidstadeel.



BIJLAGE 1: RESULTATENLIJST ALGEMEEN BESTUUR JIB01 - 15 MAART 2021

BR			
4.	Het Algemeen Bestuur gaat akkoord met het Privacy Beleidskader.	AB	2 LAB01



DB VERSLAG

VASTGESTELD VERSLAG

dd. 24/08/2021

21DB30 – Dagelijks Bestuur

Artikel 5.1 lid 2 e

Aanwezig

Michaël van Straalen (voorzitter); Wouter Duyck (neemt niet deel aan beraadslaging over de aanvragen van de Universiteit Gent); Anneke Luijten-Lub (neemt niet deel aan beraadslaging over de aanvragen van de Hanzehogeschool Groningen); Luut Kroes; Axel Artikel 5.1 lid 2 e

0. OPENING

BR

BR

BR

6. BELEIDSBERAAD

6.1 Ontwikkelingen stelsels – vast agendapunt

- *Nederland*

- *Vlaanderen*
nihil

6.2 NVAO 2.0 - vast agendapunt

6.3 Privacy Beleidsdocumenten

Het DB gaat akkoord met het afhandelvoorstel. (actiepunt DB/juristen)

LK licht toe dat de documenten door de OR zijn geaccordeerd en nu ter definitieve vaststelling voorliggen.

WD merkt op dat punt 19 in de Handreiking veilige omgang persoonsgegevens spreekt over 'Stuur geen zakelijke informatie door naar uw privé e-mailadres of telefoon', maar dat hier zal zijn bedoeld de privé telefoon. Het woord 'privé' moet dan worden toegevoegd. LK ondersteunt dit, want het is niet de bedoeling dat je op je telefoon geen e-mail kunt lezen.

Besluit 53

Het Privacy Office verzoekt het DB het volgende te besluiten, met medeneming van genoemde tekstwijziging:

1. Het Dagelijks Bestuur stelt de volgende documenten vandaag vast, met inwerkingtreding per 1 september 2021:

- a. Privacyverklaring NVAO*
- b. Cookieverklaring*
- c. Privacyverklaring medewerkers*
- d. Handreiking veilige omgang persoonsgegevens*

BR

From: Artikel 5.1 lid 2 e @nvao.net>
Sent on: Tuesday, November 3, 2020 9:22:52 AM
To: Luut Kroes <l.kroes@nvao.net>
CC: Artikel 5.1 lid 2 e @nvao.net>; Artikel 5.1 lid 2 e @nvao.net>
Subject: privacybeleid 0.3 en rasci model
Attachments: Pr Beleidskader 0.3 naar Luut.docx (107.16 KB), rasci model 12 okt 20.docx (69.78 KB)

Artikel 5.1 lid 2e

Bijgaand het concept privacybeleid en het concept rasci model. Laatste bijlage is wel even kauwen en willen we samen met jou (Artikel 5.1 lid 2 e) doornemen.

De Informatiemanager staat erin en in bijlage 2 staat een handige tabel van genoemde documenten die een overzicht geven welke documenten hiermee samenhangen en hoe het ermee staat.

BR

Het privacybeleid is een tijdje geleden ook door Artikel 5.1 lid 2 e bekeken.

Ik hoor graag je op- en aanmerkingen!

Vriendelijke groet,

Artikel 5.1 lid 2 e



Nederlands-Vlaamse Accreditatieorganisatie
Parkstraat 83 • 2514 JG Den Haag
P.O. Box 85498 • 2508 CD Den Haag
artikel 5.2 lid 1 e
www.nvao.net

From: Luut Kroes <l.kroes@nvao.net>

Sent on: Wednesday, November 4, 2020 3:13:02 PM

To: artikel 5.1 lid 2 e@nvao.net>

CC: artikel 5.1 lid 2 e @nvao.net>; artikel 5.1 lid 2 e @nvao.net>

Subject RE: privacybeleid 0.3 en rasci model artikel 5.1 lid 2 e

artikel 5.1 lid 2 e,

Ik heb beide documenten zorgvuldig gelezen. Het beleidsdocument beschrijft helder en volgens mij compleet de situatie. Ik heb daar geen opmerkingen bij.

Het rasci model moeten we dus samen doornemen, regel je daarvoor een afspraak? Daarna is het volgens mij wel rijp voor een eerste bespreking in het DB.

We moeten ons realiseren dat de uitkomsten van de discussie over de NVAO 2.0 al wel eens snel zouden kunnen nopen tot wijzigingen maar dat zien we dan tzt wel.

Wijzigingen is denk ik eenvoudige als de structuur helder beschreven is.

BR

Met vriendelijke groet,

Luut



Nederlands-Vlaamse Accreditatieorganisatie
Parkstraat 83 • 2514 JG Den Haag
P.O. Box 85498 • 2508 CD Den Haag

artikel 5.2 lid 1 e

www.nvao.net

From: Artikel 5.2 lid 1 e @nvao.net>
Sent on: Thursday, February 4, 2021 12:02:00 PM
To: Anne Flierman <a.flierman@nvao.net>; Anneke Luijten-Lub <a.luijten-lub@nvao.net>; Axel Aerden <a.aerden@nvao.net>; Luut Kroes <l.kroes@nvao.net>
CC: Artikel 5.2 lid 1 e @nvao.net>; Artikel 5.2 lid 1 e @nvao.net>
Subject: Privacy Beleidskader 0.4
Attachments: NVAO notitie DB - Privacy Beleidskader 16 februari 2021.docx (131.31 KB), Privacy Beleidskader 0.4 naar DB.docx (103.68 KB), Bijlage 2 Instrumenten Privacybeleid.docx (26.42 KB), Bijlage 3 RASCI model 2021.docx (69.61 KB)

Aan: Anne, Anneke, Axel en Luut,

Bijgaand een notitie voor het DB en een herzien Privacy Beleidskader, versie 0.4 met daaronder bijlage 1. In losse documenten bijlage 2 Instrumenten en 3 het Rasci model.

Graag uiterlijk dinsdag a.s. eventuele wijzigingen/aanpassingen doorgeven aan Artikel 5.1 lid 2 e, zodat nog voor donderdag 11 februari verwerking kan plaatsvinden. Indien wij geen opmerkingen hebben ontvangen, vertrouwen wij jullie hiermee akkoord en volgt agendering op 16 februari a.s.

De onderliggende documenten (zoals privacyverklaring intern/extern e.d.) volgen later.

Vriendelijke groet,

Artikel 5.2 lid 1 e



Nederlands-Vlaamse Accreditatieorganisatie
Parkstraat 83 • 2514 JG Den Haag
P.O. Box 85498 • 2508 CD Den Haag

artikel 5.2 lid 1 e

www.nvao.net

DB NOTITIE

Datum 28-1-2021	Dossiernummer N.V.T.	Agendapunt 21DB07/6.3
Portefeuillehouders Anne Flierman Anneke Luijten akkoord met agendering	Tweede lezer Luut Kroes akkoord met agendering	Artikel 5.2 lid 1 e artikel 5.1 lid 2 e artikel 5.1 lid 2 e akkoord met agendering
Behandelaar artikel 5.1 lid 2 e		
Onderwerp Privacy Beleidskader 0.4		

1. Privacy Beleidskader

De Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG) schrijven voor dat de NVAO beleid voert op het gebied van privacy.

Dit Privacy Beleidskader geeft het kader aan waarbinnen de NVAO, CDHO en CMMBO op het gebied van gegevensbescherming bewegen. Verder gaat het kader in op de privacy uitgangspunten en de privacy governance.

Het RASCI model gaat meer in detail in op de taken die verdeeld zijn binnen de organisatie en wie welke rol speelt. Dit model is dynamisch en zal in het kader van NVAO 2.0 herzien moeten worden, maar geeft nu houvast voor de huidige situatie.

2. Proces

Op dit ogenblik is er in de mandaatregeling niet voorzien in het mandateren van het opstellen van privacy beleid of onderliggende beleidsdocumenten, waardoor het Algemeen Bestuur dit beleid zal moeten goedkeuren. Dit is ook terug te zien in een deel van de taken/verantwoordelijkheden in het RASCI model. Ook hier geldt dat aanpassing voor de hand ligt bij een verandering van de organisatiestructuur maar wachten tot het zover is, is onwenselijk. Met dit gegeven is ervoor gekozen het RASCI model zo vorm te geven dat de belangrijkste verantwoordelijkheden primair bij het DB liggen, maar bekrachtiging van het AB zal in voorkomend geval nog nodig zijn. Het verdient de voorkeur om als Dagelijks Bestuur aan het Algemeen Bestuur mandaat te verzoeken en dit in de mandaatregeling te zijner tijd vast te leggen.

Afstemming

Deze versie 0.4 van dit Privacy Beleidskader is in overleg **Artikel 5.2 lid 1 e** en Luut Kroes tot stand gekomen.

Nog te ondernemen acties na goedkeuring van deze regelingen:

Op advies van de FG en in samenwerking met de nieuwe Informatiemanager zullen diverse instrumenten (documenten) nader worden uitgewerkt.

Het onderliggend Privacy Beleidskader wordt telkens aangepast aan de documenten die nog moeten worden opgesteld. Naamgeving wordt geüniformeerd etc. Zodra inhoudelijke wijzigingen in het Privacy Beleidskader moeten worden aangebracht worden deze weer in het DB gebracht.

3. Afhandelvoorstel

1. Verzoek aan het Algemeen Bestuur om het Dagelijks Bestuur mandaat te geven voor het opstellen van beleid t.a.v. privacy aangelegenheden (en aan te passen in de mandaatregeling op een later moment).
2. Verzoek om instemming om het concept Privacy Beleidskader (versie 0.4) inclusief de bijlagen ter instemming voor te leggen aan het Algemeen Bestuur.
3. Verzoek om naam- of nummeringswijzigingen in het Privacy Beleidskader die geen inhoudelijke consequenties hebben voor het kader buiten een DB-vergadering te kunnen doorvoeren (ondermandaat aan het privacy office). Het DB wordt geïnformeerd over eventuele wijzigingen.

4. Ontwerpbesluit

1. Het DB stemt in om het Algemeen Bestuur te vragen om mandaat te verlenen aan het DB voor het opstellen van beleid t.a.v. privacy aangelegenheden (en aan te passen in de mandaatregeling op een later moment).
2. Het DB stemt in met het voorleggen van het concept Privacy Beleidskader (versie 0.4) aan het Algemeen Bestuur.
3. Het DB stemt in met het aanpassen van het Privacy Beleidskader door het privacy office indien dit geen inhoudelijke wijzigingen zijn en slechts naam- of nummeringswijzigingen. Het DB wordt geïnformeerd over eventuele wijzigingen.

5. Bijlagen

1. Privacy Beleidskader inclusief Bijlage 1
2. Bijlage 2 Instrumenten
3. Bijlage 3 RASCI model

28

From: Artikel 5.1 lid 2 e@nvao.net>
Sent on: Tuesday, March 2, 2021 1:16:21 PM
To: Luut Kroes <l.kroes@nvao.net>
CC: Artikel 5.1 lid 2 e@nvao.net>; Artikel 5.1 lid 2 e@nvao.net>; Artikel 5.1 lid 2 e@nvao.net>; Artikel 5.1 lid 2 e@nvao.net>
Subject: AB 15 maart - Privacybeleid
Attachments: Bijlage 2 Instrumenten Privacybeleid.docx (23.5 KB), Bijlage 3 RASCI model 2021.docx (69.61 KB), NVAO notitie AB_Privacy Beleidskader maart 2021.docx (106.98 KB), Privacy Beleidskader DB 16-2-2021.docx (101.67 KB)

Beste allen,

Hierbij de stukken voor het AB voor het Privacybeleid.

Groeten,

Artikel 5.1 lid 2 e



Nederlands-Vlaamse Accreditatieorganisatie

Parkstraat 83 • 2514 JG Den Haag

P.O. Box 85498 • 2508 CD Den Haag

artikel 5.2 lid 1 e

www.nvao.net

AB NOTITIE

Datum 18-2-2021	Dossiernummer N.V.T.	Agendapunt
Portefeuillehouders Dagelijks Bestuur akkoord met agendering	Tweede lezer Luut Kroes Axel Aerden akkoord met agendering	Artikel 5.1 lid 2 e Artikel 5.1 lid 2 e Artikel 5.1 lid 2 e akkoord met agendering
Behandelaar Artikel 5.1 lid 2 e		
Onderwerp Privacy Beleidskader		

1. Privacy Beleidskader

De Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemeen Verordening Gegevensbescherming (UAVG) schrijven voor dat de NVAO beleid voert op het gebied van privacy.

Dit Privacy Beleidskader geeft het kader aan waarbinnen de NVAO, CDHO en CMMBO op het gebied van gegevensbescherming bewegen. Verder gaat het kader in op de privacy uitgangspunten en de privacy governance.

Het RASCI model gaat meer in detail in op de taken die verdeeld zijn binnen de organisatie en wie welke rol speelt. Dit model is dynamisch en zal in het kader van NVAO 2.0 herzien moeten worden, maar geeft nu houvast voor de huidige situatie.

2. Proces

Op dit ogenblik is er in de mandaatregeling niet voorzien in het mandateren van het opstellen van privacy beleid of onderliggende beleidsdocumenten, waardoor het Algemeen Bestuur dit beleid zal moeten goedkeuren. Dit is ook terug te zien in een deel van de taken/verantwoordelijkheden in het RASCI model. Ook hier geldt dat aanpassing voor de hand ligt bij een verandering van de organisatiestructuur maar wachten tot het zover is, is onwenselijk. Met dit gegeven is ervoor gekozen het RASCI model zo vorm te geven dat de belangrijkste verantwoordelijkheden primair bij het DB liggen, maar bekrachtiging van het AB zal in voorkomend geval nog nodig zijn. Het verdient de voorkeur om als Dagelijks Bestuur aan het Algemeen Bestuur mandaat te verzoeken en dit in de mandaatregeling te zijner tijd vast te leggen.

Afstemming

Deze versie 0.4 van dit Privacy Beleidskader is in overleg met **Artikel 5.1 lid 2 e**, Luut Kroes en Axel Aerden tot stand gekomen.

Nog te ondernemen acties na goedkeuring van deze regelingen:

Op advies van de FG en in samenwerking met de nieuwe Informatiemanager zullen diverse instrumenten (documenten) nader worden uitgewerkt.

Het onderliggend Privacy Beleidskader wordt telkens aangepast aan de documenten die nog moeten worden opgesteld. Naamgeving wordt geüniformeerd etc. Zodra inhoudelijke wijzigingen in het Privacy Beleidskader moeten worden aangebracht worden deze weer in het DB gebracht.

3. Afhandelvoorstel

1. Verzoek aan het Algemeen Bestuur om het Dagelijks Bestuur mandaat te geven voor het (laten) opstellen en goedkeuren van beleid t.a.v. privacy aangelegenheden (en aan te passen in de mandaatregeling op een later moment).
2. Verzoek om instemming met het concept Privacy Beleidskader inclusief de bijlagen.

4. Ontwerpbesluit

1. Het AB stemt in om het Dagelijks Bestuur mandaat te verlenen voor het (laten) opstellen en goedkeuren van beleid t.a.v. privacy aangelegenheden (en aan te passen in de mandaatregeling op een later moment).
2. Het AB stemt in met het concept Privacy Beleidskader.

5. Bijlagen

1. Privacy Beleidskader inclusief Bijlage 1
2. Bijlage 2 Instrumenten
3. Bijlage 3 RASCI model

From: Arnold Jonk <a.jonk@nvao.net>
Sent on: Thursday, February 13, 2025 9:46:33 AM
To: Artikel 5.1 lid 2 e @nvao.net>; René Hageman <r.hageman@nvao.net>
CC: Artikel 5.1 lid 2 e @nvao.net>; NVAO
Subject: Re: Aangepaste versies AVG documenten

Follow up: Opvolgen

Follow up status: Completed

Completed on: Thursday, February 13, 2025 12:11:00 PM

Categories: ter info

Akkoord en grote dank, Artikel 5.1 lid 2 e

Groeten,

Arnold

Van: Artikel 5.1 lid 2 e @nvao.net>

Datum: dinsdag, 11 februari 2025 om 20:36

Aan: René Hageman <r.hageman@nvao.net>, Arnold Jonk <a.jonk@nvao.net>

CC: Artikel 5.1 lid 2 e @nvao.net>, NVAO | Juridische Zaken Artikel 5.1 lid 2 e @nvao.net>

Onderwerp: Aangepaste versies AVG documenten

Dag Arnold en René,

Ik merkte dat ik nog niet op de verzendknop had gedrukt, dus ik stuur de mail bij deze alsnog.

Bijgaand sturen wij jullie de aangepaste versies van de *Privacyverklaring (extern)* en

de *Privacyverklaring voor medewerkers* NVAO, versie februari 2025. Tevens hebben we het aangepaste *privacybeleid* en de aangepaste *protocollen voor Datalekken* en de *Rechten van Betrokkenen*.

De aanpassingen in alle documenten omvatten: Het toevoegen van de formulering dat de documenten naar aanleiding van klachten en signaleringen aangepast zullen worden. Er stond al een passage over periodieke aanpassingen in alle stukken, maar we hebben enkele woorden toegevoegd. Daar waar een onderdeel van de privacyverklaring niet volledig in overeenstemming was met de AVG hebben we een zorgvuldig nagelopen en hier en daar een klein detail aangetroffen (bijvoorbeeld de vermelding van overeenkomst en gerechtvaardigd belang als grondslagen in de externe privacyverklaring). Deze zijn ook meegenomen.

Versie februari is overal doorgevoerd. **Artikel 5.1 lid 2 e** mag, na jullie akkoord, publiceren. Medewerkers zijn op de hoogte dat dit eraan komt. Ter volledigheid sturen we het overzicht met de gesignaleerde en nu aangepaste knelpunten mee.

Artikel 5.1 lid 2 e wij nemen jou alvast mee in deze mail. Wij kunnen jou zeker nog wel gebruiken om de stukken NVAO-huisstijlproof te maken. We hebben deze week nog wel even contact hieromtrent.

Met vriendelijke groet,



Nederlands-Vlaamse Accreditatieorganisatie

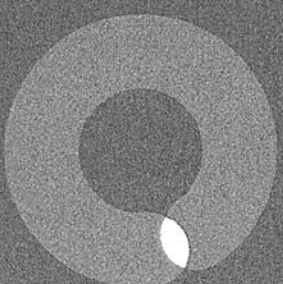
Parkstraat 83 • 2514 JG Den Haag

P.O. Box 65498 • 2508 CD Den Haag

artikel 5.2 lid 1 e

www.nvao.net

30



NVAO

Nieuwjaars digitale opruimdag

NVAO

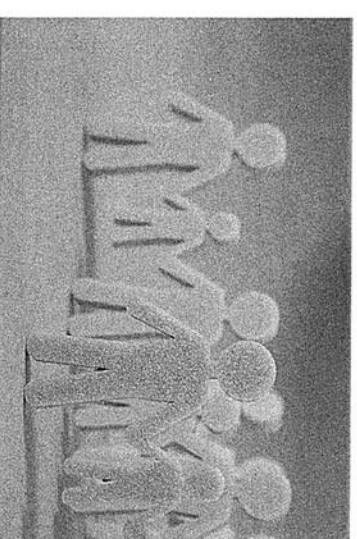
10 januari 2022

Functionaris Gegevensbescherming (FG)

Kennismaking

Taken:

- Controle en toezicht op naleving AVG
- Rapportage aan management
- Informatie en advies
- Formele rol bij klachten, DPIA's en datalekken
- Optreden als contactpersoon voor de Autoriteit Persoonsgegevens (AP)
- Bewustwording



Waarom ruimen we op?

Privacy Office en FG zien voor de hele NVAO toe op naleving:

- Algemene Verordening Gegevensbescherming (AVG)
- Archiefwet
- Selectielijst NVAO (zie intranet/HR & Organisatie/Informatiehuishouding)



- Nuance nodig voor (CDHO) & CMIMBO
- Bewustwording privacy vaker op de agenda

Niet langer bewaren dan noodzakelijk! Hoe lang is lang?

Boekentip: "Grip" van Rick Pastoor (ondertitel: Het geheim van slim werken)

Eerste aanzet: opruimen e-mail

- Ruis
 - Privé-mail
 - Koffiemomentjes
 - Mail in cc
- Dossiergegevens – is het al ergens anders opgeslagen?
- CV's

Handige links

Hoe schoon je je outlook mailbox op? Filmpje 12 minuten, dame met demo

Hoe krijg je je mailbox leeg? Filmpje 2 minuten, man in Scheveningen:

Ter inspiratie

Informatiehuishouding

Koot & de Bie, 3 minuten

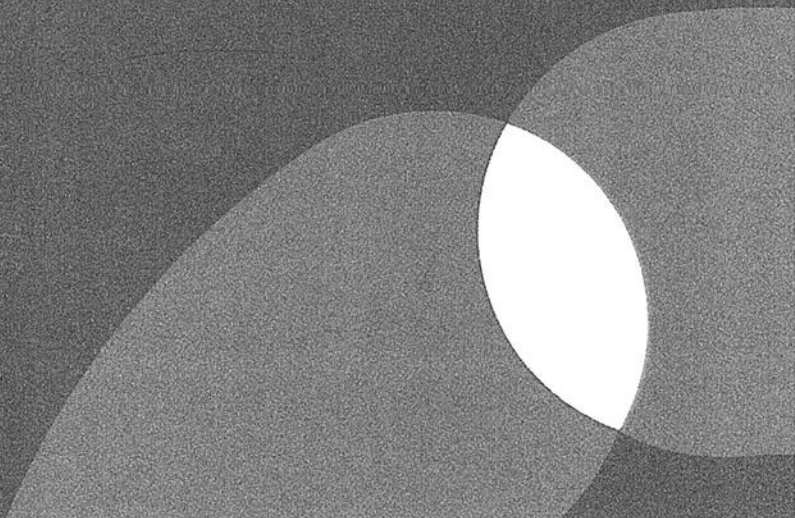
Deel II

- 12.50 - 13.40 uur: Zelf aan de slag
- 13.40 - 13.50 uur: Gezamenlijke behandeling
- 13.50 - 14.00 uur: pauze - offline
- 14.00 - 14.30 uur: Pubquiz en afronding



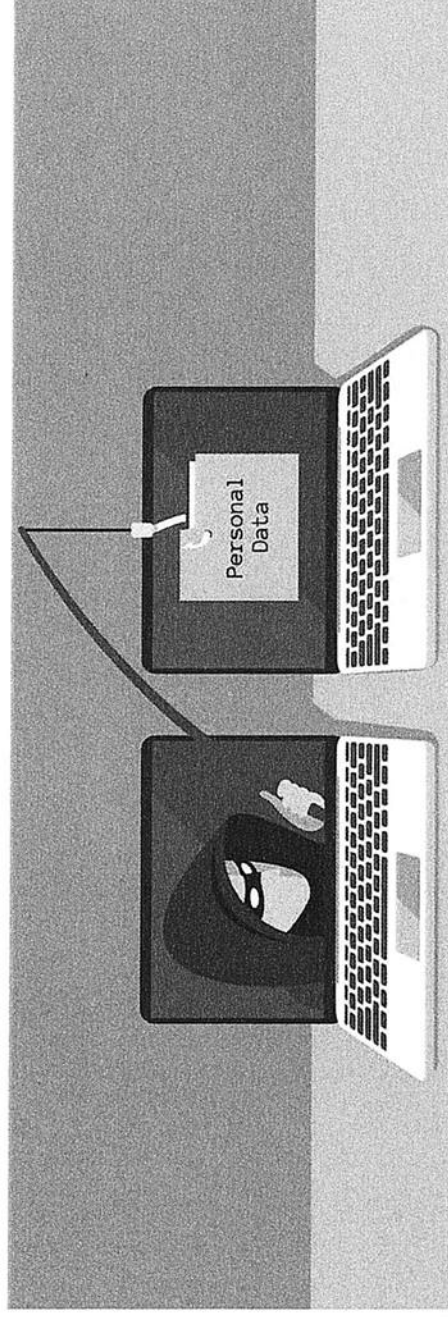
NVAO

Privacy opfrismoment juni 2023



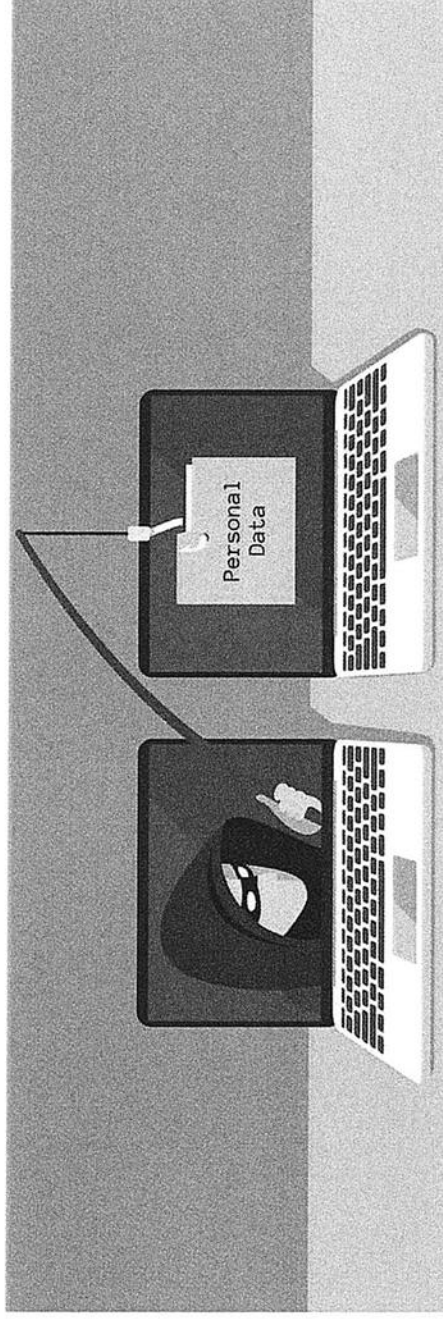
Wat doen we vandaag?

- 11.30 - 11.35: Opfris digitaal opschonen
- 11.35 - 12.00: Phishing (wat is het, hoe herken je het, voorbeelden, wat doe je)
- 12.00 - 12.15: Fysieke (bedrijfs)middelen (intern/extern)



Terugblik

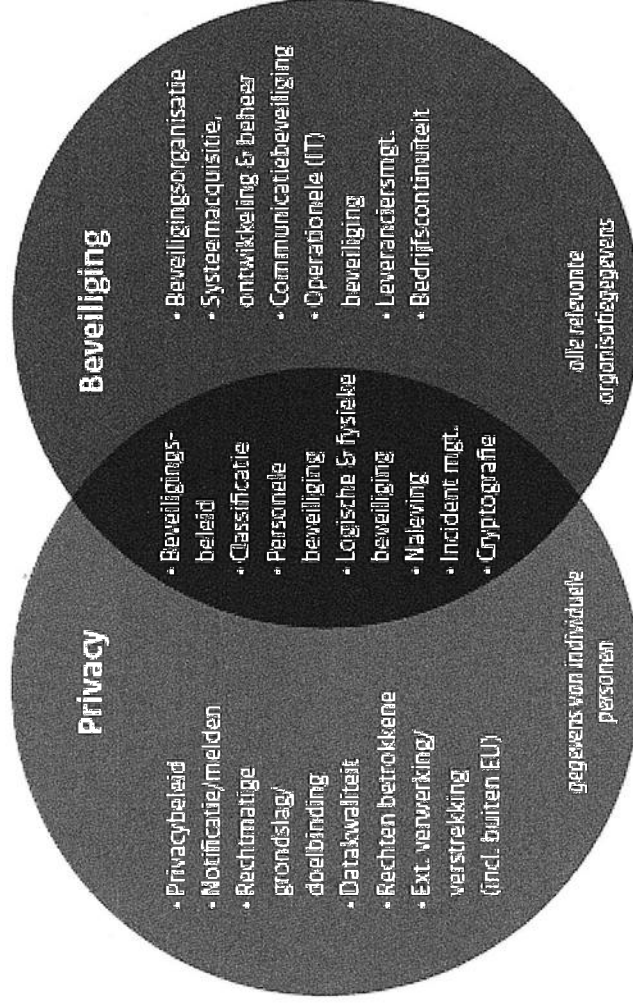
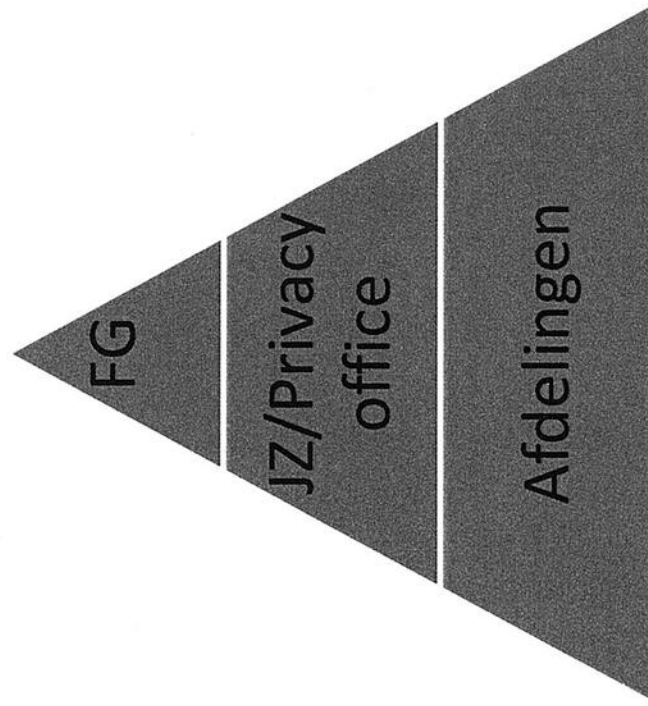
Opfrismoment schonen E-mail



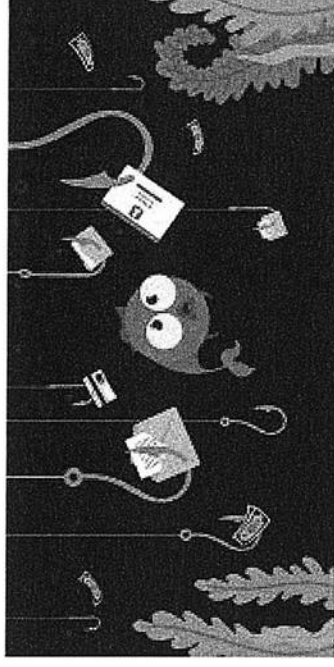
FG en CISO

- Verschillen en overeenkomsten tussen CISO en FG
- Gezamenlijke taak: o.a. Bewustwording

AP



Wat is phishing?

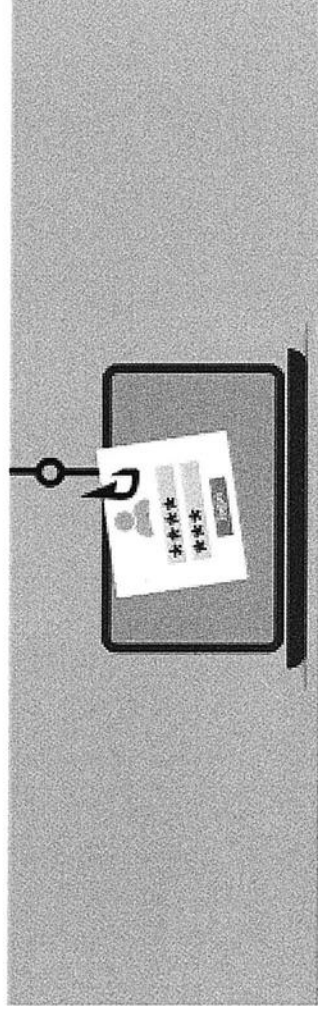


Phishing is een vorm van internetfraude.

Het bestaat uit het oplichten van mensen door ze te lokken naar een valse website, die een kopie is van de echte website, om ze daar – nietsvermoedend – te laten inloggen met hun inlognaam en wachtwoord of hun creditcardnummer.

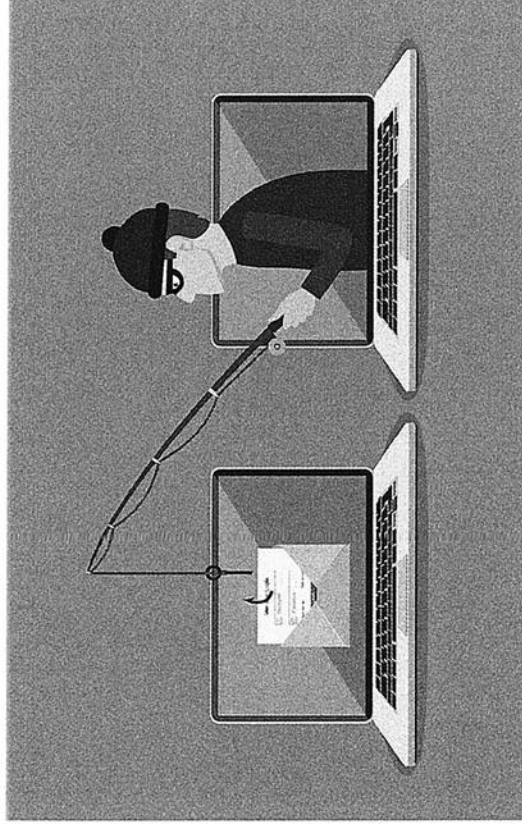
5 belangrijkste soorten 'phishing'

- Telefonisch (vishing)
- E-mail (phishing)
- Sms of whatsapp bericht (smishing)
- Applicaties op smartphones
- Samenwerkingsapplicaties (teams/zoom)



Phishing: methoden

- Grote schaal phishing
- Spear Phishing
- Whaling



NOS: 1 juni 2022

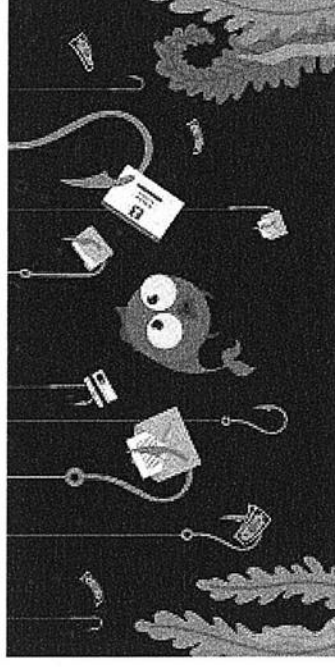
Onderzoekers: hackers vallen succesvol Nederlands defensiebedrijf aan

Nep-recruiter van Amazon

Wel duidelijk is, hoe ze te werk zijn gegaan. Er is, zo zegt Maasland, gebruikgemaakt van zogeheten *spearphishing*. Dit betekent dat de hackers gericht mensen hebben benaderd. Uit het onderzoek blijkt dat medewerkers van het defensiebedrijf in 2021 zijn benaderd door een iemand die zich voordeed als een recruiter van Project Kuiper, het internetsatellietproject van techgigant Amazon.

Hoe herken je e-mail phishing?

- Onpersoonlijk/ bulkmails
- Taalfouten of heel veel hoofdletters
- Afzender
- Spoed
- Schadelijke link of bijlage
- Bestanden ingepakt/zip
- Vervalste website



Hoe herken je e-mail phishing?

Vervalste websites:

Gespoofde websites kunnen er echt uitzien.

Vervalste links

Zweef erover met je muis. Klopt het echt??



Geachte Klant,

ING heeft zijn website en internetbankier omgeving vernieuwd. De aanpassingen waren nodig om mee te gaan met de laatste ontwikkelingen op online-bankier gebied. We hebben de site gebruiksvriendelijker en veiliger gemaakt. Niet alle online-functionaliteiten van uw internetbankieren is actief. Hiervoor dient u uw gegevens up te daten in onze systeem.

Na verificatie zal ook uw rekening omgezet worden naar het nieuwe systeem. Let er op dat u de omzetting zo snel mogelijk moet doen. Wij ondersteunen het oude systeem tot 01-05-2015.

Klik hier



Niet doen!

Na de stappen neemt een medewerker contact met u op om de laatste stappen te doorlopen.

Met vriendelijke groet,

Ir. Drs. M.D.C. Homler
Algemeen Directeur
ING NEDERLAND N.V.



NVAO



Pakket Gemist

Geachte Klant/Geachte,

U hebt ons bericht van 1-1-2015 op 11:23:2071 over de bezorging van uw pakket gemist. Het pakket is nu in bezorging genomen. Er wordt nu een nieuwe bezorging gepland op de volgende werkdag.

Uw bestelling ligt klaar bij onze officiële partner.

Bij een post in de buurt dient u uw bestelling op te halen. Het is mogelijk dat de informatie, aangezien u nu u uw track and trace code aanwijst het. Ook weten we ook gedurende de tijd die u hier voor we het pakket kunnen bezorgen. Word de bezorging niet binnen 14 dagen opgehaald wordt het pakket gereturneerd.

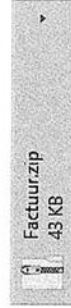
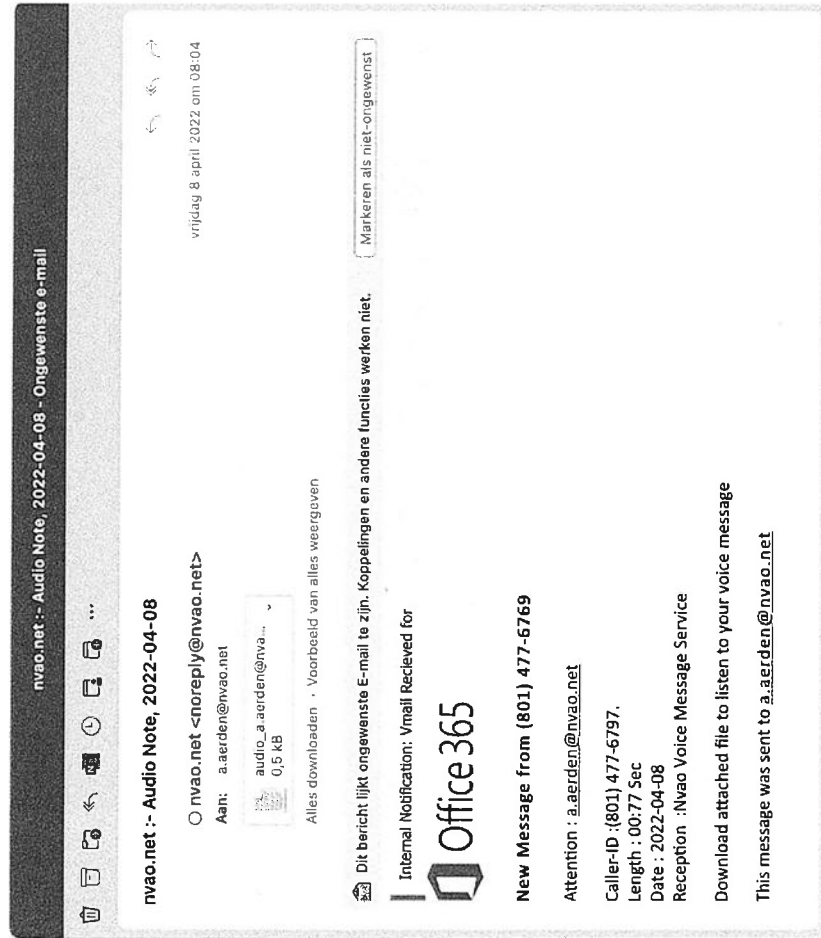
Hoogachtend,

De Pakket

Hoe herken je e-mail phishing?

Bestanden

link of zijn vaak ingepakt/zip



Van: Susan Hagenaar [mailto:administratie@action.nl]
Verzonden: donderdag 14 april 2016 10:16
Aan: [e-mailadres]
Onderwerp: Fout geadresseerde factuur

Beste heer/mevrouw,

Wij hebben een factuur van u ontvangen maar wij zijn helemaal geen klant van u. Wij hebben de factuur die wij van u ontvangen hebben bijgevoegd in de bijlage. Kunt u ons laten weten hoe dit in onze mailbox terecht is gekomen? Wij hopen spoedig van u te vernemen.

Met vriendelijke groet,

Susan Hagenaar
www.action.nl



Action Service & Distributie B.V.

Perenmarkt 15
1681 PG Zwaagdijk-Oost

<http://www.action.nl>

Melden datalek of beveiligingsincident

- Als je je telefoon of laptop kwijt bent
- Als je een e-mail verkeerd geadresseerd verstuurd hebt
- Alleen als er persoonsgegevens in verkeerde handen zijn gekomen, spreken we in beginsel van een datalek maar ook beveiligingsincidenten moeten bij privacy@nvaio.net worden gemeld en geregistreerd!
- Vragen?

Fysiek, hoe doen we dat intern?

- Windows L om je scherm zwart te maken
- Vertrouwelijke stukken in je eigen locker of in een gedeelde teamkast
- Lege bureaus
- Papierbakken (links vertrouwelijk; rechts gewoon papier)
- Postvakken (onbeveiligd; check je eigen postvak)
- Printer (geen originelen laten liggen)
- NL: nieuwe computers/telefoons > bruikleenovereenkomst



Nederlands-Vlaamse Accreditatieorganisatie
Accreditation Organisation of the Netherlands and Flanders

www.nvao.net • info@nvao.net



Bewustwordingskwartet
privacy

22



AUTORITEIT
PERSOONSgegevens
Bijeenkomst 2015

Nieuwe privacywetgeving vanaf 25 mei 2018 De AVG in een notendop



Op basis hiervan mag je persoonsgegevens verzamelen De grondslag



Toestemming
van de gebruiker



Vitale belangen



Wettelijke
verplichting



Overeenkomst



Algemeen belang



Gerechtvaardigd
belang

Het begint aan de tekentafel Zorgvuldigheid



Functionaris gegevens-
bescherming



Privacy by design



Impact assessment

Technische en organisatorische maatregelen Verplichtingen



Register met alle
verwerkingen



Gegevens-
beschermingsbeleid



(Digitale)
beveiliging

Mensen moeten controle kunnen uitoefenen Rechten van de betrokkenen



Recht om
in te zien



Recht om
te wijzigen



Recht om vergeten
te worden



Recht om gegevens
over te dragen

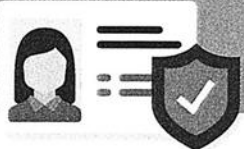


Recht op
informatie

De AVG geldt vanaf 25 mei 2018



Gegevens zijn
beschermd!



U heeft een goed privacyverhaal



Voor uw
doelgroep



Voor de
Autoriteit Persoonsgegevens

Aan de slag met het AVG-stappenplan!
Bereid je nu voor op de AVG

Naar het stappenplan →

Planning privacywerkzaamheden Afdeling Nederland 2024

nr.	Wat	Benodigde actie	Wie	Planning	Status
1	Privacybeleid Afdeling Nederland met onderliggende documenten	Herschrijven privacybeleid ivm verbijzondering.	jz	Q3	Concept voorleggen Directie
2	Instrumenten privacybeleid: verwerkersovereenkomst	Evalueren en zo nodig herschrijven	jz	Q1	voltooid
3	Instrumenten Privacybeleid Cookieverklaring	Herschrijven tbv Afdeling NL	Communicatie/ Ict iam directie en jz	Q3	Gesprekken gevoerd met communicatie en directie, voorbereiding voor wijziging in gang gezet
4	Instrumenten Privacybeleid DPIA Proces	Controle en herschrijven Afdeling Nederland	jz	Q3	-
5	DPIA-register	Bijwerken (tool). Betreft reeds uitgevoerde DPIA's die in een ander bestand of document staan. Omzetten naar PN	jz	Q2/Q3	Omzetting voltooid DPIA ICT (ontwikkeling + beheer) nagenoeg voltooid
6	Privacyverklaring medewerkers + CDHO + CMMBO	Herschrijven Afdeling NL	jz	Q2/Q3	Gestart herschrijven
7	Externe Privacyverklaring Afdeling NI	Herschrijven Afdeling NI	jz iam HR	Q2/Q3	Gestart Herschrijven
8	Protocol datalekken	Herschrijven Afdeling NL	jz	Q2/Q3	Concept afgestemd met ISO, voorleggen Directie oktoberr024

9	Protocol Rechten Betrokkenen	Herschrijven afdeling NI	jz	Q2 en Q3	Herschrijven gestart
10	Register datalekken en beveiligingsincidenten	Controle en bijwerken in PN	jz	Q1/Q2/Q3/Q4	Registratie verder up-to-date
11	Register van verwerkingen	Tool bijwerken. Verwerkingen zijn in 1 overzicht bij elkaar gezet, moet overgezet naar de tool, bewerkelijk.	jz	Q2/Q3/Q4	Registratie naar nieuw register overgezet
12	Awareness bevordering	Regelmatig bijeenkomsten organiseren voor afdeling NL	jz iam directie	Q1/Q2/Q3/Q4	➤ Introductie privacyzaken (6x) nieuwe medewerkers NVAO-NI, CDHO, CMMBO ➤ Awareness bijeenkomst in kader van meironde (16 april 2024) ➤ Awareness lunch-bijeenkomst IB door ISO iam JZ ➤ Nog in beraad: organiseren serious game
13	Afstemming	Diverse onderwerpen, waaronder implicaties	jz, Communicatie ICT en Directie	Q1/Q2/Q3/Q4	Going concern

		en samenhang AVG en Nis2, doorgaande AVG/WOO afstemming	Directie in afstemming met JZ	Q1/2/3/4	
14	Scholing/PE	Afstemming FG kwartaaloverleg Deelname aan permanente educatie en professionaliseringsbijeenkomsten/congressen	jz iam directie Communicatie/ICT iam Directie	Q1/Q2/Q3/Q4	Q1/Q2 ➤ Kennisbijeenkoms Lef (maat 2024) AVG en NIS2 ➤ Actualiteiten AVG Kantoor Lands- advocaat (april 2024) ➤ CIP cursus wijzigingen Cookiewet (april 2024) ➤ Bijwonen cursus actualiteiten privacyrecht, oktober 2024

JZ 2025

JZ 2025				
Activiteiten	Q1	Q2	Q3	Q4
Borging AVG Bijwerken register	Nalopen alle verwerkingen	Nalopen alle verwerkingen	Nalopen alle verwerkingen	Nalopen alle verwerkingen
Borging AVG Nieuwe VWO/ Overeenkomst gegevensver- werking	VWO's nalopen	LEO		
Nalopen interne en externe P- verklaringen			Geldigheidsduur, vragen/klachten/ contact	Geldigheidsduur, vragen/klachten/ contact
Protocol datalekken				
Protocol rechten van betrokkenen				
AVG Dpia's				Co-pilot/Atlas TI Interviews (start 2025, vervolg 2026)
AVG Ontwikkelingen AI	12/2 kennisdeling AP sessie over verordering AI PP 27-3-25 Korte presentatie over alle privacydocumenten.	Kennisdeling AI en AVG bij kwaliteitszorg- organisaties	kennisdeling	kennisdeling

1. Beschrijving van het project

beschrijving	persoon verantwoordelijk	Gegevens	
		Persoonsgegevens? Soorten persoonsgegevens	afkomstig van Frequentie verwerking
Behandeling van klant-/service vragen	Informatie manager? (Of Directeur NL?)	Ja	Contactgegevens (Naam, email, telefoonnummer) 0 Een tot meerdere keren per dag
Technisch beheer documentopslag	Informatie manager? (Of Directeur NL?)	Nee	Contactgegevens (Naam, email, telefoonnummer) Een tot meerdere keren per 0 maand
Reserveer en uitleen (ICT middelen)	Informatie manager? (Of Directeur NL?)	Ja	Contactgegevens (Naam, email, telefoonnummer) Een tot meerdere keren per 0 maand
Identity & access management	Informatie manager? (Of Directeur NL?)	Ja	Contactgegevens (Naam, email, telefoonnummer) Een tot meerdere keren per 0 maand

2. Beschrijving van de verwerking van persoonsgegevens

categorieën betrokkenen	kwetsbare personen	hoeveel betrokkenen	doel van de verwerking	Persoonsgegevens al eerder verwerkt	Toegang al mw delen met derden?	Gegevensopslag	Land	Bewaartermijn
Medewerkers	Nee	1 - 1.000	Registratie van incident- en wijzigingsmeldingen teneinde problemen op te lossen en wijzigingen uit te kunnen voeren	Nee	20 - 50 Ja	Op een externe locatie	NL	Gedurende looptijd contract
Medewerkers, Panelleden, Leveranciers/onderaannemers	Nee	1 - 1.000	Opslaan en uitwisselen van documenten tbv werkzaamheden	Nee	20 - 50 Ja	Op een externe locatie	NL	Geldende bewaartermijn
Medewerkers	Nee	1 - 1.000	Het (tijdelijk) verstrekken van ICT middelen aan medewerkers van de organisatie	Nee	20 - 50 Ja	Op een externe locatie	NL	Gedurende looptijd arbeidscontract
Medewerkers	Nee	1 - 1.000	Toegang verschaffen tot het (IT) domein en applicaties	Nee	20 - 50 Ja	Op een externe locatie	NL	Tot maximaal 60 dagen na einde arbeidscontract

				3. Beoordeling van de evenredigheid en de noodzaak van de verwerking			
Doorgifte							
Vernietiging	Gearchiveerd	buiten EER	Verwerkers	Grondslag	Dataminimalisatie	Datakwaliteit	Wetgeving zonder? minder? gevoeliger Nieuwe informatie? Belangen gewogen?
Ja	Nee	Nee	Ja	Gerechtigd belang	Alleen strikt noodzakelijke gegevens worden gedeeld met de dienstverlener.	Gebruik maken van een gevalideerde bron (Active Directory)	Nee Nee Nee Nee Nee Ja
Ja	Ja	Nee	Ja	Gerechtigd belang			Nee Nee Nee Nee Nee Ja
Ja	Nee	Nee	Ja	Gerechtigd belang	Alleen strikt noodzakelijke gegevens worden gedeeld met de dienstverlener.	Gebruik maken van een gevalideerde bron (Active Directory)	Nee Nee Nee Nee Nee Ja
Ja	Nee	Nee	Ja	Gerechtigd belang		Gebruik maken van een gevalideerde bron (P&O)	Nee Nee Nee Nee Nee Ja

4. Beoordeling van de risico's

5. Maatregel

Hoge risico's	Risico's voor de betrokkene	Andere risico's	"privacy by design" maatregelen	standaardinstellingen	technische beveiligingsmaatregelen
-	Onterecht inzicht in toegangsgegevens van andere gebruikers	Encryptie Toegangscontrole	Ja	Toegangscontrole, rollen en rechten (obv least privileged)	
-	Onterechte toegang tot documenten en daarmee toegang tot persoonsgegevens	Toegangscontrole	Ja	Toegangscontrole, rollen en rechten (obv least privileged)	
-		Dataminimalisatie	Ja	Toegangscontrole, rollen en rechten (obv least privileged)	
-		Toegangscontrole Dataminimalisatie	Ja	Toegangscontrole, rollen en rechten (obv least privileged)	

len om de risico's te mitigeren

organisatorische beveiligingsmaatregelen	overige maatregelen	evaluatie maatregelen	gedragscode?	FG aanwezig?	advies betrekkenen?
autorisatiematrix, verwerkersovereenkomst		Ja	Ja		Nee
autorisatiematrix, verwerkersovereenkomst		Ja	Ja		Nee
autorisatiematrix, verwerkersovereenkomst		Ja	Ja		Nee
autorisatiematrix, verwerkersovereenkomst		Ja	Ja		Nee

36



Aanpassing procedures website (afd. NL)

Art 5.1 lid 2e

Beste collega's,

Zoals vanmorgen tijdens het koffiemoment is toegelicht gaan we wat veranderen aan de procedures die op de website staan weergegeven. Op dit moment zijn deze procedures persoonsgebonden. Dit betekent dat de procescoördinator met zijn/haar naam op de website staat en dat vragen direct naar de persoonlijke mailbox worden gestuurd.

Vanwege een aanscherping van de AVG-regels en het feit dat vanaf 1 januari 2022 de website wordt gedeeld met het Nationaal Archief, gaan we de persoonsgegevens verwijderen van de website. We gaan de vragen die binnenkomen via de website centraliseren, waardoor alle vragen die binnenkomen naar info@nvao.net worden gestuurd. Vanuit daar wordt bekeken of de vraag moet worden doorgestuurd naar de procescoördinator (of andere medewerker) of dat er direct een antwoord gegeven kan worden. Het voordeel van deze werkwijze is dat er een betere werkverdeling ontstaat.

Naast een betere werkverdeling is het ook belangrijk dat we vragen en antwoorden gaan registreren. Het is daarom belangrijk om te antwoorden vanuit de infobox of met de infobox in de cc. De registratie zorgt voor eenduidige antwoorden en op termijn helpt het ook bij de verbetering van de FAQ op onze website.

Het kan zijn dat je in de toekomst vragen ontvangt via je persoonlijke e-mail. Dat is uiteraard geen enkel probleem, echter willen we oproepen om de infobox hierbij te betrekken. Dit geldt uiteraard niet voor het gehele conversaties met betrokken over een lopende procedure.

Zijn er vragen met betrekking tot deze aanpassing? Stuur dan een bericht naar

Art 5.1 lid 2e

Weergegeven in SharePoint

37

Selectielijst voor de neerslag van de Nederlands-Vlaamse Accreditatieorganisatie en diens
taakvoorganger de Nederlandse Accreditatieorganisatie 2002 | Nationaal Archief

<https://www.nationaalarchief.nl/archiveren/kennisbank/selectielijst-voor-de-neerslag-van-de-nederlands-vlaamse>