Model Privacy Beleid

AVG vertaald naar beleid voor verwerking van persoonsgegevens

Utrecht, November 2021
Versienummer: 3.0

Colofon

Model Privacy Beleid

SURF
Postbus 19035
NL-3501 DA Utrecht
T +31 88 787 30 00

info@surf.nl
www.surf.nl

Deze versie is een update van het Model beleid verwerking persoonsgegevens. De update is tot stand gekomen met hulp van SCIPR, de SURF community voor informatie beveiliging en privacy. Aan deze versie hebben mee gewerkt:

- Herma de Boer (Deltion)
- Erik van den Beld (Saxion)
- Silvia van Dijk (Haagse Hogeschool)
- Charlie van Genuchten (SURF)
- Joyce van der Klugt (Hogeschool Leiden)
- Floor May-Smit (NHL Stenden)
- Alphons Muurlink (KNAW)
- Anita Polderdijk-Rijntjes (Windesheim)
- Raoul Winkens (Universiteit Maastricht)
- Monique Witlam (Saxion)

Versie 3.0 November 2021

SURF is de ICT-samenwerkingsorganisatie van het Nederlandse hoger onderwijs en onderzoek.
Deze publicatie is digitaal beschikbaar via de website van SURF: www.surf.nl/publicaties

Inhoudsopgave

1. Inleiding

Verwerking van Persoonsgegevens is noodzakelijk voor de bedrijfsprocessen van instellingen van onderwijs en onderzoek. Dit dient met de grootste zorgvuldigheid te gebeuren omdat misbruik van Persoonsgegevens grote schade kan berokkenen aan studenten, medewerkers en andere Betrokkenen bij <de instelling>, maar ook bij <de instelling> zelf. <de instelling> hecht dan ook veel waarde aan het beschermen van de Persoonsgegevens die aan haar worden verstrekt en aan de wijze waarop Persoonsgegevens worden verwerkt. Het op een juiste manier verwerken van Persoonsgegevens is de verantwoordelijkheid van het bestuur van <de instelling>.

Met het beschrijven van de maatregelen in dit beleidsdocument beoogt en neemt <de instelling> haar verantwoordelijkheid om de kwaliteit van de verwerking en de beveiliging van Persoonsgegevens te optimaliseren en daarmee te voldoen aan de relevante privacywet- en regelgeving.

1.1. Definities[1]

AVG: Algemene Verordening Gegevensbescherming[2].

Beleid: Dit beleid met betrekking tot het verwerken van Persoonsgegevens door <de instelling>.

Betrokkene: Een geïdentificeerd of identificeerbaar natuurlijk persoon op wie een Persoonsgegeven betrekking heeft.

Verwerkingsverantwoordelijke: Een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, doel en middelen van een verwerking van persoonsgegevens vaststelt. In dit beleid doorgaans <de instelling>.

Persoonsgegeven: Alle informatie over een geïdentificeerd of identificeerbaar natuurlijk persoon.

Bijzondere persoonsgegevens: Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, zoals bedoeld in artikel 9 AVG.

Verwerker: Een partij die ten behoeve van en op instructie van <de instelling> persoonsgegevens verwerkt.

Verwerking: Elke handeling of geheel van handelingen met betrekking tot Persoonsgegevens, waaronder het verzamelen, vastleggen, ordenen, opslaan, raadplegen, bijwerken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, afschermen, wissen of vernietigen van gegevens.

Derde: Een partij, niet zijnde de Betrokkene, noch de Verwerkingsverantwoordelijke, noch de Verwerker, noch enig persoon die onder rechtstreeks gezag valt van de Verwerkingsverantwoordelijke of de Verwerker, die gemachtigd is om Persoonsgegevens te verwerken.

[1] In verband met leesbaarheid zijn sommige definities verkort weergegeven. Voor volledige definities zie AVG.
[2] De Algemene Verordening Gegevensbescherming is op 25 mei 2016 in werking getreden en per 25 mei 2018 van kracht.

Datalek: Een inbreuk op de beveiliging van Persoonsgegevens, die per ongeluk of opzettelijk leidt tot de vernietiging, het verlies, de wijziging of ongeoorloofde toegang tot die gegevens.

Privacy by Default: De verplichting die op de Verwerkingsverantwoordelijke rust om de standaardinstellingen van verwerkingen zo in te stellen dat de privacy van Betrokkenen maximaal wordt gewaarborgd. Dit betekent onder meer dat er zo min mogelijk Persoonsgegevens worden gevraagd en verwerkt.

Privacy by Design: De verplichting die op de Verwerkingsverantwoordelijke rust om gedurende de gehele levenscyclus van Persoonsgegevens passende waarborgen in te bouwen en maatregelen te treffen om de beginselen die de AVG noemt op een doeltreffende manier uit te voeren. Hierbij wordt stelselmatig aandacht besteed aan allesomvattende waarborgen m.b.t. vertrouwelijkheid, integriteit, beschikbaarheid, fysieke veiligheid en verwijdering van de Persoonsgegevens (bv. autorisatiematrices, bewaartermijnen,..).

Data Protection Impact Assessment (gegevensbeschermingseffectbeoordeling): Een beoordeling van een Verwerking die helpt bij het beoordelen van de rechtmatigheid van de Verwerking, het identificeren van privacy risico's en die maatregelen voorstelt om deze risico's te verkleinen om bescherming van persoonsgegevens te garanderen.

Profilering: Elke vorm van geautomatiseerde Verwerking van Persoonsgegevens waarbij aan de hand van Persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geevalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen.

Minderjarige: Iedereen die de leeftijd van 16 jaar nog niet heeft bereikt is in het kader van de privacy wetgeving minderjarig.

Functionaris voor Gegevensbescherming (FG): de persoon die door <de instelling> is aangewezen om intern toe te zien op naleving van privacy wetgeving en te adviseren op nader in de AVG genoemde specifieke onderwerpen. De FG is aangemeld bij de Autoriteit Persoonsgegevens en heeft een FG-nummer toegekend gekregen. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie bij <de instelling>.

UAVG: Uitvoeringswet Algemene Verordening Gegevensbescherming.

Anonimiseren: is een methode waarbij Persoonsgegevens zodanig worden bewerkt dat deze niet meer gebruikt kunnen worden om een persoon te identificeren. Ook niet als deze gegevens gecombineerd worden met andere gegevens. Deze bewerking is onomkeerbaar.

1.2. Reikwijdte en doelstelling van het Beleid

1.2.1. Reikwijdte van het Beleid

Het Beleid heeft betrekking op het verwerken van Persoonsgegevens van alle Betrokkenen binnen <de instelling> waaronder in ieder geval alle medewerkers, studenten, gasten, bezoekers en externe relaties (inhuur/outsourcing) vallen, alsmede op andere Betrokkenen waarvan <de instelling> Persoonsgegevens verwerkt.

In het Beleid ligt de nadruk op de geheel of gedeeltelijk geautomatiseerde/systematische verwerking van Persoonsgegevens die plaatsvindt onder de verantwoordelijkheid van <de instelling>. Eveneens is het Beleid van toepassing op de verwerking van Persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Er is een belangrijke relatie en gedeeltelijke overlap met het aanpalende beleidsterrein informatiebeveiliging, waarbij het gaat om de beschikbaarheid, integriteit en de vertrouwelijkheid van data, waaronder Persoonsgegevens. Op strategisch niveau wordt aandacht geschonken aan deze raakvlakken en wordt zowel planmatig als inhoudelijk afstemming gezocht.
Het Beleid bij <de instelling> heeft als doel om de kwaliteit van de Verwerking en de beveiliging van Persoonsgegevens te optimaliseren waarbij een goede balans moet worden gevonden tussen privacy, functionaliteit en veiligheid.

Beoogd wordt de persoonlijke levenssfeer van de Betrokkene zoveel mogelijk te respecteren. De gegevens die betrekking hebben op een Betrokkene dienen beschermd te worden tegen onwettelijk en ongeautoriseerd gebruik dan wel misbruik op basis van het fundamenteel recht op bescherming van zijn/haar Persoonsgegevens. Dit brengt met zich mee dat het verwerken van Persoonsgegevens dient te voldoen aan relevante wet- en regelgeving en dat Persoonsgegevens veilig zijn bij <de instelling>.

1.2.2. Doelstelling van het Beleid

Doelstelling van het Beleid voor <de instelling> is concreet het volgende:

- Het bieden van een kader: het Beleid biedt een kader om (toekomstige) Verwerkingen van Persoonsgegevens te toetsen aan een vastgestelde 'best practice' of norm; en om de taken, bevoegdheden en verantwoordelijkheden in de organisatie te beleggen.
- Het stellen van normen: vaststellen hoe de organisatie om wil gaan met Persoonsgegevens
- Het SURF Juridisch Normenkader (Cloud)services[3] wordt gehanteerd als best practice voor cloud services en andere outsource contracten.
- Het nemen van de verantwoordelijkheid: door het college van bestuur door de uitgangspunten en de organisatie van het verwerken van Persoonsgegevens vast te leggen voor de hele organisatie <de instelling>.
- Daadkrachtige implementatie van het beleid door duidelijke keuzes in maatregelen te maken en actieve controle toe te passen op de uitvoering van de beleidsmaatregelen.
- Compliant zijn met de Nederlandse en Europese wetgeving.

Naast bovenstaande concrete doelstellingen is een meer algemeen doel het creëren van bewustwording van het belang en de noodzaak van het beschermen van Persoonsgegevens, mede ter vermijding van risico's als gevolg van het niet compliant zijn met de relevante wet- en regelgeving.

1.2.3. De ambities van de instelling

Om inzichtelijk te maken waar de organisatie staat en wat de effecten zijn van de maatregelen die door de organisatie worden getroffen, maakt de <de instelling> gebruik van het toetsingskader Privacy van SURF[4] en het NBA volwassenheidsmodel Informatiebeveiliging. Het maakt benchmarking met andere instellingen mogelijk omdat afgesproken is dat dit model ook gebruikt wordt door de andere instellingen.

OPTIONEEL: De instelling heeft als ambitie een [bepaal het volwassenheidsniveau]

[3] SURF juridisch Normenkader (Cloud)services, vastgesteld door bestuur Platform ICT & Bedrijfsvoering 3 april 2014 en geüpdatet in 2016, te vinden via https://www.surf.nl/kennisbank/2013/surf-juridisch-normenkader-cloudservices.html.
[4] Toetsingskader wordt eind 2021 verwacht.

2. Beleidsprincipes Verwerking Persoonsgegevens

2.1. Beleidsuitgangspunt en -principes

Algemeen beleidsuitgangspunt is dat Persoonsgegevens in overeenstemming met de relevante wet- en regelgeving op behoorlijke en zorgvuldige wijze worden verwerkt. Hierbij dient een goede balans te worden aangebracht tussen het belang van <de instelling> om Persoonsgegevens te verwerken en het belang van Betrokkene ter eerbiediging van zijn persoonlijke levenssfeer en om in een vrije omgeving eigen keuzes te maken met betrekking tot zijn Persoonsgegevens.

Om aan bovenstaand beleidsuitgangspunt te voldoen, gelden de volgende principes:

1. Verantwoordelijkheid:
    - Voor iedere gegevensverwerking is (intern) een verantwoordelijke benoemd.
    - De verantwoordelijke maakt afspraken met verwerkers en eventuele derden over de veilige en zorgvuldige Verwerking van Persoonsgegevens.
2. Legitiem doel en grondslag:
    - Het doel van de Verwerking moet voorafgaande aan de Verwerking voldoende specifiek en helder omschreven zijn.
    - Een Verwerking van Persoonsgegevens is gebaseerd op één van de wettelijke grondslagen zoals genoemd in artikel 6 van de AVG.
3. Ethisch verantwoord
    - Bij het beoordelen van Verwerkingen van Persoonsgegevens wordt ook rekening gehouden met ethische aspecten (het mag misschien, maar willen we dit ook). Meer in het bijzonder Verwerkingen die bedoeld zijn om te Profileren.
4. Dataminimalisatie
    - Er worden niet meer gegevens verzameld dan noodzakelijk is voor het doel dat men wil bereiken. Gegevens dienen toereikend, ter zake dienend en niet bovenmatig te zijn.
    - Verwerking van Persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde (subsidiariteits- en proportionaliteitsbeginsel).
5. Doelbinding
    - Persoonsgegevens worden niet verder verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen.
6. Bewaren en vernietigen
    - Gegevens zijn voorzien van een bewaartermijn.
    - Gegevens worden vernietigd of geanonimiseerd wanneer deze niet langer nodig zijn voor de vastgestelde verwerkingsdoelen.
7. Juistheid
    - Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn.
8. Transparantie en informatie
    - Voor Betrokkenen is het inzichtelijk in hoeverre en op welke manier er Persoonsgegevens worden verwerkt. Informatie en communicatie hierover moet eenvoudig toegankelijk en begrijpelijk zijn.
9. Delen van gegevens
    - Gegevens worden alleen gedeeld met anderen als daar een rechtmatige grondslag voor is.
    - Waar gegevens gedeeld worden met andere partijen dienen daar goede afspraken over gemaakt te worden.

10. Informatiebeveiliging
    - Persoonsgegevens worden beveiligd door het nemen van technische en organisatorische maatregelen (risk-based).
    - Toegang tot Persoonsgegevens wordt gegeven op basis van need-to-know.
    - Systemen worden ontworpen en ingericht volgens de principes Privacy by Design en Privacy by Default.
11. Rechten van Betrokkenen
    - Iedere Betrokkene heeft recht op inzage respectievelijk verbetering, aanvulling, verwijdering of afscherming van zijn/haar Persoonsgegevens, en heeft het recht van bezwaar.
    - Bij alle registraties die gebaseerd zijn op de grondslag “toestemming” wordt voorafgaande aan de verwerking om toestemming gevraagd.
    - Toestemming is voor Betrokkenen net zo eenvoudig in te trekken als deze gegeven is.
12. Verantwoordingsplicht
    - <de instelling> kan aantonen dat zij voldoet aan de AVG.

3. Wet- en regelgeving

Bij <de instelling> wordt op de volgende wijze omgegaan met onderstaande wet- en regelgeving.

3.1. Wet op het Hoger onderwijs en Wetenschappelijk onderzoek

<de instelling> heeft een kwaliteitszorgsysteem, waarin (onder meer) het zorgvuldig omgaan met gegevens in de studentenadministratie en met de studieresultaten is gewaarborgd. Daarnaast worden gedrags- en integriteitscodes voor (niet-)wetenschappelijk personeel nageleefd en toegepast.

3.2. Algemene Verordening Gegevensbescherming en Uitvoeringswet AVG

<de instelling> heeft de wettelijke vereisten (waaronder het rechtmatig en zorgvuldig verwerken van Persoonsgegevens en het nemen van passende technische en organisatorische maatregelen tegen verlies en onrechtmatige Verwerking van data c.q. Persoonsgegevens) geïmplementeerd op basis van het Beleid.

3.3. Arbeidsregelgeving en CAO

<de instelling>draagt zorg voor goed werkgeverschap, waarin (onder meer) het zorgvuldig omgaan met gegevens in de personeelsadministratie is gewaarborgd. Daarnaast worden er persoonsgegevens gedeeld met bijvoorbeeld UWV, Belastingdienst en de bedrijfsarts.

3.4. Archiefwet

<de instelling> houdt zich aan de voorschriften uit de Archiefwet en het Archiefbesluit over de wijze waarop omgegaan moet worden met de bewaartermijnen van informatie vastgelegd in (gedigitaliseerde) documenten, informatiesystemen, websites, e.d. Dit is onderdeel van de jaarlijkse externe accountantsrapportages.

3.5. Telecommunicatiewet

[Optioneel bij Openbare netwerken] De maatregelen die <de instelling> genomen heeft om aan de privacywetgeving te voldoen zijn tevens toereikend om de bescherming van de persoonlijke levenssfeer van gebruikers op onze openbare netwerken te waarborgen. De regelgeving van de Telecommunicatiewet of eventuele vervangende wetgeving met betrekking tot het bevoegd aftappen en de bewaarplicht zijn separaat geïmplementeerd.

De maatregelen die <de instelling> genomen heeft om aan de privacy wetgeving te voldoen zijn ook toereikend om aan de Telecommunicatie wet en eventuele opvolgende wetgeving (ePrivacy verordening) te voldoen aangaande het gebruik van cookies en elektronische communicatie middelen zoals ongevraagd e-mailen en bellen (cookiewet, spamwet, telemarketing).

3.6. Gedragscodes

Naast wet en regelgeving conformeert <de instelling> zich ook aan de volgende gedragscodes en richtlijnen:

- Nederlandse Gedragscode wetenschappelijk integriteit[5]
- Gedragscode praktijkgericht onderzoek[6]
- Gedragscode gebruik van persoonsgegevens in wetenschappelijk onderzoek[7]
- Gedragscode voor medisch wetenschappelijk onderzoek[8]

De volgende gedragscode/richtlijnen zijn in de maak:

- Referentiekader privacy en ethiek voor studiedata

[5] Nederlandse_gedragscode_wetenschappelijke_integriteit_2018_NL.pdf (vereniginghogescholen.nl)
[6] Gedragscode_praktijkgericht_onderzoek_voor_het_hbo.pdf (vereniginghogescholen.nl)
[7] Gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek — KNAW
[8] Update Gedragscode Gezondheidsonderzoek - mei 2021 - Coreon

4. Governance

4.1. Rollen en verantwoordelijkheden met betrekking tot Verwerking Persoonsgegevens

Om de Verwerkingen van Persoonsgegevens gestructureerd en gecoördineerd op te pakken, wordt bij <de instelling> een aantal rollen onderkend die aan functionarissen in de bestaande organisatie zijn toegewezen.

4.1.1. College van Bestuur

Het college van bestuur is de Verwerkingsverantwoordelijke en daarmee de eindverantwoordelijke voor de rechtmatige en zorgvuldige Verwerking van Persoonsgegevens binnen <de instelling> en stelt het Beleid, de maatregelen en de procedures op het gebied van Verwerking vast.

4.1.2. Portefeuillehouder Verwerking Persoonsgegevens

De portefeuillehouder Verwerking Persoonsgegevens is het bestuurslid dat privacy in portefeuille heeft. Hij is eindverantwoordelijk voor de bescherming van Persoonsgegevens binnen <de instelling>.

4.1.3. [Managementteams / faculteits-/domein directie]

De MT's van de diverse [faculteiten/domeinen] zijn verantwoordelijke voor de uitvoering van dit Beleid en rapporteren aan het college van bestuur over de stand van zaken op het gebied van het Verwerken van Persoonsgegevens binnen de eigen [faculteit/domein/organisatieonderdeel].

4.1.4. Leidinggevende

Het creëren van bewustwording en de naleving van het Beleid is onderdeel van de integrale bedrijfsvoering. Iedere leidinggevende heeft de taak om:

- er voor te zorgen dat zijn medewerkers op de hoogte zijn van het Beleid;
- toe te zien op de naleving van het Beleid door zijn medewerkers;
- periodiek het onderwerp privacy onder de aandacht te brengen in werkoverleggen.

4.1.5. [optioneel] (Corporate) Privacy Officer

De Corporate Privacy Officer helpt privacy risico's naar een acceptabel niveau te reduceren. Deze is verantwoordelijke voor het ontwikkelen en uitvoeren van dit Beleid, zorgt ervoor dat privacy taken worden uitgevoerd en dat privacy maatregelen ingebed worden in de organisatie.

De taken van de Corporate Privacy Officer zijn:

- Adviseert over privacy aangelegenheden;
- Bewaakt de kwaliteit van het register van verwerkingen;
- Signaleert privacy-risico's;
- Ondersteunt bij Data Protection Impact Assessments (DPIA's) en bij pré DPIA's;
- Adviseert in geval van het vermoeden van datalekken;
- Behandelt verzoeken van betrokkenen;
- Stelt een concept privacy beleid op en actualiseert deze;
- Stelt een privacy jaarplan op en monitort de voortgang;
- Doet voorstellen voor het implementeren van (nieuwe) privacywetgeving.
- Vervangt de FG in geval van afwezigheid.

4.1.6. [optioneel] Privacy Contactpersoon

De Privacy Contactpersoon (PC) weet wat zich in de haarvaten van de organisatie afspeelt. De PC is eerste aanspreekpunt voor het eigen organisatie onderdeel op het gebied van privacy. De Privacy

Contactpersoon heeft korte lijnen met collega's zodat privacy risico's tijdig gesignaleerd kunnen worden. In voorkomende gevallen kan de PC de CPO en FG raadplegen. Tevens zijn de Privacy Contactpersonen aanspreekpunten voor FG en CPO.

De taken van de Privacy Contactpersoon zijn:

- Het signaleren van vraagstukken op het gebied van privacy in het team.
- Aanspreekpunt voor privacy vragen binnen het eigen team;
- Het leveren van een bijdrage aan het bewustwordingsproces rondom privacy binnen het team.
- Het doorgeven van nieuwe verwerkingen en wijzigingen in verwerkingen van persoonsgegevens aan de Corporate Privacy Officer voor opname in, respectievelijk wijziging van, het register van verwerkingsactiviteiten.

4.1.7. Systeemeigenaar/Proceseigenaar

De systeemeigenaar is er verantwoordelijk voor dat de applicatie en bijbehorende ICT-faciliteiten een goede ondersteuning bieden aan het proces waar deze verantwoordelijk voor is en voldoet aan het Beleid. Dit betekent dat de systeemeigenaar ervoor zorgt dat zowel nu, als in de toekomst de applicatie blijft beantwoorden aan de eisen en wensen van de gebruikers en aan wet- en regelgeving.

De systeemeigenaar/Proceseigenaar heeft de volgende taken:

- Het (laten) opnemen van verwerkingen van persoonsgegevens in het register.
- Het (laten) maken van schriftelijke afspraken over het delen van persoonsgegevens zoals een verwerkersovereenkomst.
- Het in beeld (laten) brengen van risico's in geval van een verwerking (Data Protection Impact Assessment of DPIA).
- Het (laten) uitvoeren van de maatregelen die nodig zijn om de risico's te beperken.

4.1.8. Functionaris voor Gegevensbescherming

<de instelling> stelt, indien dit verplicht is, een interne toezichthouder op de Verwerking van Persoonsgegevens aan. Deze toezichthouder wordt Functionaris voor Gegevensbescherming genoemd (hierna: "FG"). De FG wordt door <de instelling> tijdig betrokken bij alle aangelegenheden waar Persoonsgegevens bij komen kijken. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie bij <de instelling>. <de instelling> meldt de FG aan bij de toezichthoudende autoriteit.

De taken van de FG zijn:

- Het informeren en adviseren van alle betrokken partijen over hun verplichtingen onder de AVG.
- Het toezien op de naleving van de AVG en andere relevante privacywetgeving.
- Het toezien op de naleving van dit Beleid.
- Toezien op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het betrokken personeel en de betreffende audits.
- Adviseren over en toezien op de uitvoering van DPIA's.
- Het behandelen van klachten en/of vragen die rechtstreeks aan de FG zijn gericht.
- Het samenwerken met de toezichthoudende autoriteit.
- Fungeren als eerste aanspreekpunt voor de toezichthoudende autoriteit.

4.2. Three lines of Defence

De Governance bij <naam instelling> is ingericht volgens het zogenaamde Three Lines of Defence model[9] (ook wel '3LoD'). Dit model wordt algemeen toegepast als model om Governance, Risk en Compliance (GRC) te borgen in een operationele organisatie. Het beschrijft niet alleen de rollen binnen de organisatiestructuur, maar ook hun onderlinge samenwerking.

4.2.1. Eerste lijn

Het 3LoD-model heeft als uitgangspunt dat het lijnmanagement (de business) verantwoordelijk is voor haar eigen processen. De <decanen/directeuren> zorgen ervoor dat privacy afspraken ook werkelijk worden geïmplementeerd, dat awareness-programma's worden uitgevoerd, dat personeel wordt opgeleid, etc. Dit is de eerste lijn.

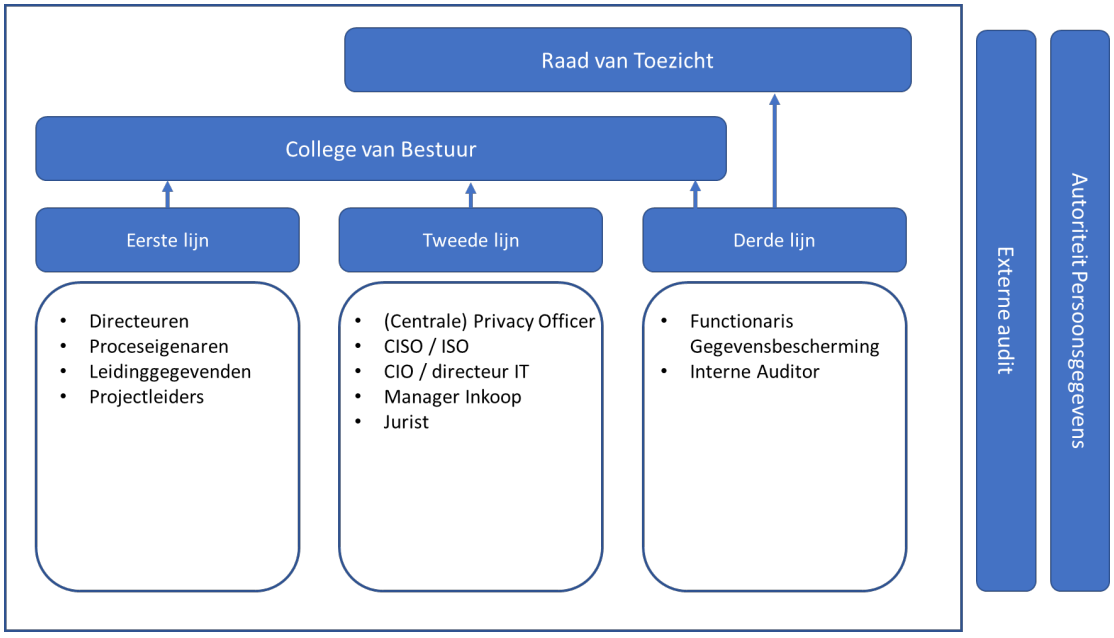
4.2.2. Tweede lijn

Daarnaast moet er een functie zijn die de eerste lijn ondersteunt, adviseert, coördineert en die bewaakt of het management zijn verantwoordelijkheden ook daadwerkelijk neemt. Dit is de tweede lijn. Ook bepaalde beleidsvoorbereidende taken, het organiseren van de PDCA-cyclus, van integrale risicoanalyses en self-assessments en het opstellen van jaarplannen en rapportages zijn taken van de tweede lijn. De (C)PO bevindt zich in de tweede lijn.

4.2.3. De derde lijn

Het is wenselijk dat er binnen de organisatie een functie bestaat die controleert of het samenspel tussen de eerste en tweede lijn soepel functioneert en daarover een objectief, onafhankelijk oordeel velt met mogelijkheden tot verbetering. Daarbij kijkt men ook of er geen overlapping is en of er blinde vlekken bestaan. Deze functie is de derde lijn.

De binnen de AVG verplichte Functionaris voor Gegevensbescherming (FG) en de <afdeling Internal Audit/ internal auditor> behoren typisch tot de derde lijn. Beiden opereren volledig los van alle andere organisatieonderdelen en rapporteren niet alleen aan <het College/de Raad> van Bestuur, maar ook aan de Raad van Toezicht.



[9] https://www.icas.com/ca-today-news/internal-audit-three-lines-of-defence-model-explained

4.3. Verdeling van de verantwoordelijkheden

- Het ***college van bestuur*** van <de instelling> is verantwoordelijk voor Verwerkingen van Persoonsgegevens waarvan zij het doel en de middelen vaststelt. Zij wordt aangemerkt als de **Verwerkingsverantwoordelijke** in de zin van de AVG. De feitelijke Verwerking van Persoonsgegevens wordt echter op allerlei lagen van <de instelling> uitgevoerd.

- Het zorgvuldig verwerken van Persoonsgegevens dient gezien te worden als **een *lijnverantwoordelijkheid***: dat betekent dat de lijnmanagers (afdelingshoofden/centrale stafdiensten) de primaire verantwoordelijk dragen voor een zorgvuldige Verwerking van Persoonsgegevens op hun afdeling/eenheid. Dit omvat ook de keuze van en afstemming met de [FG en/of (C)PO] omtrent de maatregelen en de uitvoering en handhaving ervan. Onder de lijnverantwoordelijkheid valt ook de taak om het beleid met betrekking tot de Verwerking van Persoonsgegevens te communiceren met alle relevante partijen.

- Het zorgvuldig omgaan met Persoonsgegevens is ***ieders verantwoordelijkheid***. Er wordt van medewerkers en studenten verwacht dat ze zich integer gedragen. Niet acceptabel is dat door al dan niet opzettelijk gedrag onveilige situaties ontstaan die leiden tot schade en/of imagoverlies van <de instelling> of van individuen. Het is om deze reden dat er gedragscodes zijn geformuleerd en geïmplementeerd.

- Iedere betrokkene van de instelling, waaronder medewerkers en studenten wordt geacht een datalek of vermoeden daarvan te melden bij de daarvoor aangewezen instantie (servicedesk). Er is een datalek procedure waarbij de FG een adviserende rol vervult.

4.4. Inpassing in de instellingsgovernance / Afstemming met aanpalende beleidsterreinen

Om de samenhang in de organisatie met betrekking tot gegevensbescherming goed tot uitdrukking te laten komen en de initiatieven en activiteiten op het gebied van Verwerking van Persoonsgegevens binnen de verschillende onderdelen op elkaar af te stemmen, is het belangrijk om gestructureerd overleg te voeren over het onderwerp privacy op verschillende niveaus.

Op **strategisch niveau** wordt richtinggevend gesproken over governance en compliance, alsmede over doelen, scope en ambitie op het gebied van privacy-aspecten. [Het strategisch niveau wordt ingevuld in <overlegnaam>]

Op **tactisch niveau** wordt de strategie vertaald naar plannen, te hanteren normen, en evaluatiemethoden. Deze plannen en instrumenten zijn sturend voor de uitvoering. [Het tactisch niveau wordt ingevuld in <overlegnaam>]

Op **operationeel niveau** worden de zaken besproken die de dagelijkse bedrijfsvoering (uitvoering) aangaan. [Het operationeel niveau wordt ingevuld in <overlegnaam>]

4.5. Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van het verwerken van Persoonsgegevens uit te sluiten. Noodzakelijk is het om bij <de instelling> het bewustzijn voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en veilig en verantwoord gedrag wordt aangemoedigd. Onderdeel van het Beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, studenten en gasten. Deze campagnes kunnen aansluiten bij landelijke campagnes in het hoger onderwijs, zo mogelijk in afstemming met andere beveiligingscampagnes. Verhoging van het bewustzijn is een taak van <de Functionaris voor Gegevensbescherming | (C)PO | de (decentrale) Security Managers, |de (centrale) Security Officer>.

4.6. Controle en naleving

4.6.1. PDCA cyclus

De afgesproken ambitie van <de instelling> is dat dit Beleid in opzet en bestaan aantoonbaar geïntegreerd is in de bedrijfsvoering van de instelling. Om dat mogelijk te maken, is inbedding in de PDCA cyclus van belang. Onderdeel van een volledige PDCA-cyclus is het meten van de kwaliteit en het opstarten van verbeteracties. Met een PDCA- cyclus wordt ook inzichtelijk hoever de organisatie staat met het voldoen aan wet- en regelgeving. Daarvoor wordt gebruik gemaakt van het toetsingskader Privacy van SURF.

Proceseigenaren doen verslag van de privacy activiteiten en informeren de Functionaris voor Gegevensbescherming/(Centrale) Privacy Officer hierover. Privacy management is opgenomen binnen de planning en control-cyclus van de instelling. De Privacy Officer en Functionaris voor Gegevensbescherming doet jaarlijks verslag aan het bestuur van de instelling en geeft aanbevelingen voor een verdere optimalisering van de privacy beleidsvoering. Het bestuur van de instelling besluit over bijsturing van dit Beleid in overeenstemming met de aanbevelingen van de Functionaris Gegevensbescherming.

4.6.2. Toezicht en sancties

Audits maken het mogelijk het Beleid en de genomen maatregelen te controleren op effectiviteit. De FG initieert gezamenlijk met de Information Security Officer/CISO en de interne auditor de controle op het rechtmatig en zorgvuldig verwerken van Persoonsgegevens.

Eventuele externe controles worden uitgevoerd door onafhankelijke accountants. Dit is gekoppeld aan het jaarlijkse accountantsonderzoek en wordt zoveel mogelijk gecoördineerd met de normale Planning & Control cyclus. [Peer-reviews van SURFaudit maken onderdeel uit van de externe controles van <de instelling>.]

Mocht de naleving van maatregelen ter bescherming van Persoonsgegevens ernstig tekortschieten, dan kan <de instelling> de betrokken medewerkers een sanctie opleggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

Het verwerken van Persoonsgegevens is een continu proces. Technologische en organisatorische ontwikkelingen binnen en buiten <de instelling> maken het noodzakelijk om periodiek te bezien of men nog voldoende op koers zit met het Beleid.

5. Rechtmatige en zorgvuldige Verwerking van Persoonsgegevens

<de instelling> verwerkt Persoonsgegevens in overeenstemming met de principes zoals benoemd in paragraaf 2.1 van dit Beleid. Ter uitwerking van deze principes treft <de instelling> de in dit hoofdstuk genoemde maatregelen.

5.1. Verantwoordelijkheid

Voor iedere gegevensverwerking is een verantwoordelijke benoemd. In veel gevallen kan dit intern belegd worden bij een proces- of systeemverantwoordelijke. De verantwoordelijke ziet erop toe dat de Verwerking voldoet aan de principes uit dit Beleid en laat zo nodig een Data Protection Impact Assessment (DPIA) uitvoeren. Middels een DPIA worden risico's in verband met de verwerking van persoonsgegevens in beeld gebracht en worden maatregelen ter verkleining van deze risico's door de systeem- of proceseigenaar toegepast.

In samenwerkingsverbanden en bij uitbesteding is niet altijd direct duidelijk wie als Verwerkingsverantwoordelijke aangemerkt dient te worden. Helderheid hierover bij het maken van contractafspraken is noodzakelijk. Verwerkingsverantwoordelijke is degene die doel en middelen van de verwerking bepaalt.

De verantwoordelijke maakt afspraken met verwerkers en eventuele derden over de veilige en zorgvuldige verwerking van Persoonsgegevens. [OPTIONEEL]Voor het maken van afspraken met verwerkers wordt gebruik gemaakt van de model overeenkomsten van SURF (zoals verwerkersovereenkomst en gezamenlijke verwerkingsverantwoordelijke overeenkomst).

5.2. Legitiem doel en grondslag

<de instelling> verwerkt alleen Persoonsgegevens als daar een gerechtvaardigd doel voor is. Het doel van een verwerking wordt voorafgaande aan de verwerking voldoende specifiek en helder omschreven. Dit ligt o.a. vast in het verwerkingsregister.

<de instelling> verwerkt slechts Persoonsgegevens als er sprake is van een van een wettelijke grondslag zoals beschreven in artikel 6 van de AVG:

a. Toestemming van de Betrokkene.
b. Noodzakelijk voor de uitvoering van een overeenkomst met de Betrokkene.
c. Noodzakelijk om te voldoen aan een wettelijke verplichting die op de verwerkingsverantwoordelijke rust.
d. Noodzakelijk om de vitale belangen van de Betrokkene of een ander natuurlijk persoon te beschermen.
e. Noodzakelijk voor de vervulling van een taak van algemeen belang of in het kader van uitoefening van openbaar gezag.
f. Noodzakelijk voor de behartiging van het gerechtvaardigd belang van de verwerkingsverantwoordelijke of een derde.

Bij gebruik van de grondslag "toestemming" wordt de betrokkene voordat deze toestemming geeft geïnformeerd over doel van de gegevensverwerking conform hetgeen in 5.8.1 staat bij het recht op informatie. <de instelling> kan aantonen:

I) op welke wijze deze toestemming is gevraagd;
II) dat deze toestemming specifiek voor het beschreven doel is verleend; en
III) dat deze toestemming ondubbelzinnig is verleend.

<de instelling> draagt er zorg voor dat het intrekken van toestemming net zo eenvoudig is als het geven ervan. Zij informeert de Betrokkene vooraf dat intrekken van toestemming de rechtmatigheid van de Verwerking tot het moment van intrekken niet aantast. Het intrekken van de toestemming werkt niet met terugwerkende kracht.
<de instelling> houdt er rekening mee dat de toestemming vrijelijk moet worden gegeven zonder directe of indirecte druk. Aangezien, er tussen <de instelling> enerzijds en studenten of medewerkers anderzijds een machtsverhouding bestaat zal goed gemotiveerd moeten worden waarom in het specifieke geval de toestemming wel vrij kan worden gegeven.

Bijzondere persoonsgegevens
Het verwerken van Bijzondere persoonsgegevens is in beginsel verboden, tenzij er sprake is van een wettelijke grondslag, uitdrukkelijke toestemming van de betrokkene of een zwaarwegend algemeen belang. Tevens gelden zwaardere eisen voor de beveiliging van deze persoonsgegevens. Daar waar de basisbescherming niet voldoende is moeten voor elk informatiesysteem individueel afgestemde extra maatregelen worden genomen.

[OPTIONEEL] Op basis van artikel 30 lid 2 punt a van de Uitvoeringswet AVG mag <de instelling> gegevens betreffende gezondheid van haar studenten verwerken voor zover de verwerking nodig is met het oog op de speciale begeleiding van studenten of het treffen van bijzondere voorzieningen in verband met hun gezondheidstoestand. Delen van dit soort informatie is op basis van need-to-know en zal nooit zonder medeweten van de betreffende student geschieden.

5.3. Ethisch verantwoord

Bij het beoordelen van verwerkingen van persoonsgegevens wordt ook rekening gehouden met ethische aspecten (het mag misschien, maar willen we dit ook?). Deze aspecten worden meer in het bijzondere meegenomen bij verwerkingen die bedoeld zijn om te profileren of daar naar hun aard om vragen, bijvoorbeeld omdat nieuwe technologieën worden gebruikt.

[OPTIONEEL] Met betrekking tot het gebruik van studiedata hanteert <de instelling> het “referentiekader privacy en ethiek voor studiedata” dat een resultaat is van het “versnellingsplan onderwijsinnovatie met ICT”.

Ethische aspecten spelen ook een rol bij mensgebonden onderzoek. Als het onderzoek daarnaast ook nog WMO[10] plichtig is dient er een toetsing plaats te vinden door een erkende medisch ethische commissies (METC).

5.4. Dataminimalisatie

Er worden niet meer gegevens verzameld dan noodzakelijk voor het doel dat <de instelling> wil bereiken met het verzamelen van die gegevens. Gegevens dienen toereikend, ter zake dienend en niet bovenmatig te zijn.

Verwerking van persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde (subsidiariteits- en proportionaliteitsbeginsel). Als het doel ook bereikt kan worden op een manier die minder inbreuk maakt op de privacy van de betrokkene dan wordt voor deze manier gekozen. (Denk bijvoorbeeld aan het vragen naar een geboortedatum vs het vraag naar een leeftijdscategorie of het anoniem verzamelen van gegevens).

<de instelling> geeft invulling aan deze beginselen door het toepassen van “Privacy by default” en “Privacy by design” bij ingebruikname van nieuwe systemen of processen.

[10] Uw onderzoek: WMO-plichtig of niet? | Onderzoekers | Centrale Commissie Mensgebonden Onderzoek (ccmo.nl)

5.5. Doelbinding

Persoonsgegevens die voor een bepaald doel verzameld zijn mogen alleen verder worden verwerkt voor andere doeleinden als deze doeleinden verenigbaar zijn met het oorspronkelijke doel.

Indien <de instelling> verdere verwerking wenselijk acht, dan dient aan een aantal elementen te worden getoetst of de verdere verwerking verenigbaar is:

- Het verband tussen het nieuwe doel en het oorspronkelijke doel. Hoe dichter de twee doelen bij elkaar liggen, hoe eerder de verdere verwerking van persoonsgegevens verenigbaar is met het oorspronkelijke doel.
- De context waarin de persoonsgegevens zijn verzameld. Hierbij wordt in belangrijke mate rekening gehouden met de redelijke verwachting die de Betrokkene mag hebben betreffende de verdere verwerking van zijn persoonsgegevens voor dit nieuwe doel.
- De aard van de persoonsgegevens. Wanneer het bijvoorbeeld gevoelige persoonsgegevens betreft, geldt dat deze een hoger beschermingsniveau verdienen en dat deze minder snel voor andere doelen mogen worden gebruikt.
- De mogelijke gevolgen van de verdere verwerking voor betrokkenen.
- Het bestaan van passende waarborgen, zoals versleuteling of het gebruik van gepseudonimiseerde persoonsgegevens.

De verdere verwerking van persoonsgegevens voor wetenschappelijk en historisch onderzoek, voor statistische doeleinden en voor archiveringsdoeleinden in het algemeen belang, worden door de AVG als verenigbaar aangemerkt, mits voldoende passende technische en organisatorische maatregelen zijn toegepast, zoals bijvoorbeeld het pseudonimiseren van persoonsgegevens.

Indien <de instelling> persoonsgegevens wenst te verwerken voor een doel dat onverenigbaar is met het oorspronkelijk doel dan kan dat alleen als de Betrokkene hiervoor toestemming heeft gegeven of in geval van een specifieke wettelijke verplichting om bepaalde persoonsgegevens te verstrekken aan een overheidsorgaan.
In zo'n geval is er sprake van een nieuwe verwerking van persoonsgegevens en moet opnieuw de rechtmatigheid, zorgvuldigheid en noodzakelijkheid hiervan worden beoordeeld.

5.6. Bewaren en vernietigen

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld of worden gebruikt, in overeenstemming met het uitgewerkte bewaar- en vernietigingsbeleid[11] van <de instelling>. <de instelling> zal de Persoonsgegevens na het verlopen van de bewaartermijn vernietigen, anonimiseren of, indien de Persoonsgegevens bestemd zijn voor historische, statistische of wetenschappelijke doeleinden, in een archief bewaren en passende technische en organisatorische maatregelen nemen, zoals pseudonimisering.

Bij het archiveren hanteert <de instelling> de [selectielijst HBO/ universiteit] als uitgangspunt voor de bewaartermijnen. De bewaartermijnen in deze selectielijst vinden hun oorsprong in diverse wetgeving zoals WHW, AVG en archiefwet.

Wanneer verwerking van een Persoonsgegeven plaats vindt op basis van toestemming en de betrokkene trekt zijn toestemming in dan zal het gegeven alleen nog verwerkt worden om aan een wettelijke plicht te voldoen. Bestaat zo'n plicht niet dan wordt het gegeven verwijderd.

[11] Bewaartermijnen kunnen wettelijk zijn bepaald, zoals bij financiële gegevens of bij formele studieresultaten, maar ze kunnen ook zijn vastgelegd door <de instelling>, b.v. in een overeenkomst tussen <de instelling> en de Betrokkenen.

Indien het technisch niet mogelijk is om Persoonsgegevens na afloop van de bewaartermijn te vernietigen dienen deze gegevens in ieder geval ontoegankelijk gemaakt te worden.

5.7. Juistheid

Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn. Gegevens die onjuist of achterhaald zijn worden gecorrigeerd of gewist. <de instelling> toont een actieve houding in het juist en actueel houden van Persoonsgegevens. Dit in tegenstelling tot een passieve houding waarbij pas op klachten van Betrokkenen tot actie wordt overgegaan.

Processen en systemen zijn zo ontworpen en ingericht dat juistheid van gegevens zoveel mogelijk afgedwongen en controleerbaar wordt.

5.8. Transparantie en informatie

<de instelling> verwerkt Persoonsgegevens op een manier die ten aanzien van de Betrokkene behoorlijk en transparant is. Dit houdt in dat <de instelling> aan de Betrokkene op een toegankelijke wijze en in begrijpelijke taal inzichtelijk maakt in hoeverre en op welke manier diens Persoonsgegevens worden verwerkt. Bij het verzamelen van de Persoonsgegevens zal <de instelling> middels een privacyverklaring of informatiebrief de Betrokkene inlichten. Inlichting zal plaatsvinden voorafgaand aan de Verwerking, tenzij dit redelijkerwijs niet mogelijk is.

5.8.1. Recht op informatie

De Betrokkene heeft het recht om door <de instelling> te worden geïnformeerd over bepaalde aspecten van de Verwerking van zijn Persoonsgegevens. <de instelling> informeert de Betrokkene over de Verwerking van diens Persoonsgegevens, zowel in de situatie waarin de Persoonsgegevens direct bij de Betrokkene zijn verzameld, als wanneer ze langs een andere route zijn verkregen. <de instelling> kan aantonen dat de informatie verstrekt is.

A. Verkrijging direct van Betrokkene

<de instelling> verstrekt de Betrokkene voorafgaand aan de verzameling van de gegevens, tenminste de volgende informatie indien de gegevens direct bij de Betrokkene worden verzameld:

- De identiteit en contactgegevens van de Verwerkingsverantwoordelijke en, in voorkomend geval, de FG.
- De specifieke doeleinden van Verwerking waarvoor de Persoonsgegevens zijn bestemd alsook de rechtsgrond voor de verwerking.
- De gerechtvaardigde belangen van de Verwerkingsverantwoordelijke of Derde als de Verwerking is gebaseerd op de rechtsgrond ‘gerechtvaardigd belang’.
- De ontvangers of categorieën van ontvangers van de Persoonsgegevens.
- In voorkomend geval, het voornemen van de Verwerkingsverantwoordelijke om de Persoonsgegevens door te geven aan een derde land, welk land dit is en op grond van welk wettelijk doorgiftemechanisme de Persoonsgegevens daarnaartoe worden verstuurd en in bepaalde gevallen welke de passende of geschikte waarborgen zijn, hoe er een kopie van kan worden verkregen of waar ze kunnen worden geraadpleegd
- De periode gedurende welke de Persoonsgegevens worden opgeslagen, of indien niet mogelijk, de criteria die dienen om deze termijnen te bepalen.
- Het bestaan van het recht om de Verwerkingsverantwoordelijke te verzoeken om inzage, rectificatie of wissen van de Persoonsgegevens, beperking van de hem betreffende verwerking, alsmede het recht tegen de Verwerking bezwaar te maken en het recht op gegevensoverdraagbaarheid.
- Indien de Verwerking is gebaseerd op de grondslag ‘toestemming’, het recht van de Betrokkene om die toestemming te allen tijde in te trekken en wat de gevolgen hiervan zijn ten aanzien van de verwerking voorafgaand aan de intrekking.

- Het recht om een klacht in te dienen bij de toezichthoudende autoriteit.
- Of de Persoonsgegevens nodig zijn voor de uitvoering van een overeenkomst of om te voldoen aan een wettelijke verplichting.
- Of de Persoonsgegevens mede worden gebruikt voor geautomatiseerde besluitvorming. Tevens moet de onderliggende logica, alsmede het belang en de te verwachte gevolgen van de Verwerking voor de Betrokkene worden gemeld.

B. Verkrijging niet direct van Betrokkene

Als de Persoonsgegevens niet direct bij de Betrokkene zelf zijn verzameld maar langs een andere route, zal aan de Betrokkene, in aanvulling op de hiervoor genoemde punten, de volgende informatie worden verstrekt:

- De categorieën van Persoonsgegevens.
- De bron waar de Persoonsgegevens vandaan komen.

Deze informatie zal zo snel mogelijk, maar niet later dan één maand, na verkrijging van de gegevens, dan wel bij het eerste contact met de Betrokkene, worden verstrekt.

5.9. Delen van gegevens

5.9.1 Verwerking door een Verwerker

Indien <de instelling> Persoonsgegevens laat verwerken door een *Verwerker*, wordt de uitvoering van Verwerkingen geregeld in een verwerkersovereenkomst, tussen <de instelling>, de Verwerkingsverantwoordelijke, en deze Verwerker. Wanneer de andere partij alleen de hosting van een website verzorgt is er ook sprake van een Verwerker. Een Verwerkersovereenkomst wordt overeengekomen voor de aanvang van de betreffende Verwerking.

5.9.2. Verwerking door of gezamenlijk met een andere Verwerkingsverantwoordelijke

Indien <de instelling> samen met één of meerdere partijen de doelen en middelen voor de Verwerking van Persoonsgegevens bepaalt dan is er sprake van een gezamenlijke verwerkingsverantwoordelijkheid en worden afspraken omtrent de zorgvuldige en veilige verwerking van Persoonsgegevens vastgelegd in een passende overeenkomst, zoals een gezamenlijke verwerkingsverantwoordelijken overeenkomst. Indien <de instelling> Persoonsgegevens moet aanleveren om gebruik te kunnen maken van diensten van een andere partij, waarbij die partij een zelfstandige verantwoordelijkheid heeft met betrekking tot de Verwerking van die Persoonsgegevens, dan worden de afspraken vastgelegd in een gegevens uitwisselingsovereenkomst.

5.9.3 Doorgifte Persoonsgegevens binnen de Europese Economische Ruimte (hierna 'EER')

<de instelling> verstrekt Persoonsgegevens alleen aan een ontvanger (zijnde verwerker, verwerkingsverantwoordelijke of derde) gevestigd binnen de EER, als de verwerking is gebaseerd op een van de grondslagen voor gegevensverwerking uit artikel 6 en voldoet aan artikel 9 AVG en als de ontvanger voldoet aan de wettelijke vereisten uit de AVG. De EER omvat alle landen van de Europese Unie plus Noorwegen, IJsland en Liechtenstein.

5.9.4 Doorgifte Persoonsgegevens buiten de EER

Naast de voorwaarden die gelden voor verstrekking binnen de EER hanteert <de instelling> voor verstrekking aan ontvangers buiten de EER de volgende aanvullende voorwaarden:

1. Het derde land, gebied, welbepaalde sector in een derde land, of de internationale organisatie in kwestie biedt volgens de Europese Commissie een passend beschermingsniveau.
   Als passend beschermingsniveau hanteert <de instelling> de algemene lijst van landen met passend beschermingsniveau gepubliceerd door de Europese Commissie[12];

[12] Deze kunt u vinden via de volgende link http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.

2. Doorgifte vindt plaats op basis van **passende waarborgen** uit de AVG, artikel 46 en 47. Daarbij maakt <de instelling> gebruik van de Standard Contractual Clauses zoals vastgesteld door de Europese Commissie en aanvullende beveiligingsmaatregelen, die per voorgenomen doorgifte (opnieuw) worden beoordeeld.
3. Doorgifte vindt plaats op basis van een van de **wettelijke uitzonderingen** uit artikel 49 van de AVG.

5.10. Informatiebeveiliging

<de instelling> draagt zorg voor een adequaat beveiligingsniveau en legt passende technische en organisatorische maatregelen ten uitvoer om Persoonsgegevens te beveiligen tegen verlies of tegen enige vorm van onrechtmatige Verwerking. Deze maatregelen zijn er mede op gericht onnodige c.q. onrechtmatige verzameling en Verwerking van Persoonsgegevens te voorkomen. [OPTIONEEL:<de instelling> heeft een intern beveiligingsbeleid geïmplementeerd waarin maatregelen zijn uitgewerkt die werknemers van <de instelling> hanteren.]

Een risicoanalyse op privacybescherming en informatiebeveiliging maakt deel uit van het intern risicobeheersings- en controlesysteem van <de instelling>. Toegang tot persoonsgegevens wordt gegeven op basis van need-to-know en systemen worden ontworpen en ingericht volgens de principes Privacy by Design en Privacy by Default.

Bij <de instelling> worden alle Persoonsgegevens als vertrouwelijk geclassificeerd. Eenieder behoort de vertrouwelijkheid van Persoonsgegevens te kennen en daarnaar te handelen.

Ook personen voor wie niet reeds uit hoofde van ambt, beroep of wettelijk voorschrift een geheimhoudingsplicht geldt, zijn verplicht tot geheimhouding van de Persoonsgegevens waarvan zij kennisnemen, behoudens voor zover enig wettelijk voorschrift hen tot mededeling verplicht of uit hun taak de noodzaak tot mededeling voortvloeit.

5.11. Rechten van betrokkenen

De AVG geeft Betrokkenen bepaalde rechten waarmee zij controle kunnen uitoefenen op de Verwerking van hun Persoonsgegevens. Een verzoek kan schriftelijk worden ingediend bij [e-mailadres van de instelling | adres van de instelling].

Conform art 44 van de UAVG geldt voor de Verwerking van Persoonsgegevens voor wetenschappelijk onderzoek dat het recht op inzage, het recht op rectificatie en het recht op beperking van de verwerking niet geldt mits er voorzieningen zijn getroffen die garanderen dat de Persoonsgegevens alleen voor wetenschappelijke doeleinden kunnen worden gebruikt.

Voor alle in dit hoofdstuk uitgewerkte rechten van Betrokkenen gelden de volgende punten:

- **Mededeling aan Betrokkene**

<de instelling> draagt er zorg voor dat de informatie en communicatie op een beknopte, toegankelijke en begrijpelijke manier en in duidelijke en eenvoudige taal wordt verstrekt aan Betrokkene. De taal zal worden afgestemd op de doelgroep.

- **Termijn**

Op een verzoek van een Betrokkene wordt zo spoedig mogelijk, doch uiterlijk binnen één maand na indiening schriftelijk gereageerd. Hierbij zal de Betrokkene in ieder geval in kennis worden gesteld van het gevolg dat aan het verzoek is gegeven. Indien de termijn van één maand redelijkerwijs niet haalbaar is, zal Betrokkene daarvan binnen deze termijn op de hoogte worden gesteld. <de instelling> zal in dat geval binnen twee maanden na het verstrijken van de eerste termijn gevolg geven aan het verzoek van de Betrokkene.

- **Identiteit Betrokkene**

<de instelling> draagt bij het verstrekken van de betreffende informatie zorg voor een deugdelijke vaststelling van de identiteit van de verzoeker. Hiertoe kan <de instelling> extra informatie verzoeken.

- **Minderjarigen**

Een verzoek tot uitoefening van een van de rechten zoals uitgewerkt in dit hoofdstuk door een Betrokkene, zijnde Minderjarig, onder curatele gesteld of ten behoeve van wie een bewind of mentorschap is ingesteld, geschied door diens wettelijk vertegenwoordiger. Een reactie door <de instelling> zal ook naar deze wettelijke vertegenwoordiger worden verstuurd.

5.11.1.1. Recht op inzage

Verzoek

Iedere Betrokkene heeft het recht om te informeren of zijn Persoonsgegevens worden verwerkt en, als dat het geval blijkt, het recht op inzage in hem betreffende verwerkte Persoonsgegevens. Als <de instelling> veel gegevens van Betrokkene verwerkt dan mag <de instelling> de Betrokkene voorafgaand aan de informatieverstrekking verzoeken om te preciseren op welke informatie of welke verwerkingsactiviteiten het verzoek betrekking heeft.[13]

Mededeling

Indien gegevens worden verwerkt, bevat de mededeling van <de instelling> een volledig overzicht van de gevraagde gegevens, dit kan mogelijk zijn:

- De persoonsgegevens zelf
- Een omschrijving van de doeleinden van de Verwerking.
- De categorieën van gegevens waarop de Verwerking betrekking heeft.
- De ontvangers of categorieën van ontvangers, met name ontvangers in derde landen of internationale organisaties.
- Beschikbare informatie over herkomst van de gegevens.
- De termijn van bewaring van gegevens of indien dat niet mogelijk is, de criteria om die termijn te bepalen.
- Alle beschikbare informatie over de bron van de gegevens, als de gegevens niet bij de Betrokkene zijn verzameld.
- Of de Persoonsgegevens mede worden gebruikt voor geautomatiseerde besluitvorming. Tevens moet de onderliggende logica, alsmede het belang en de verwachte gevolgen van de Verwerking voor de Betrokkene worden gemeld.
- De passende waarborgen die zijn getroffen, indien de gegevens worden doorgegeven aan een derde land.
- Het recht van Betrokkene om de Verwerkingsverantwoordelijke te verzoeken om rectificatie of wissen van gegevens, beperking of bezwaar van Verwerking alsmede het recht op gegevensoverdraagbaarheid.
- Het recht van de Betrokkene om een klacht in te dienen bij een toezichthoudende autoriteit.

Kopie

De Betrokkene kan om een kopie van zijn Persoonsgegevens verzoeken maar heeft niet zondermeer recht op een kopie van alle documenten met zijn Persoonsgegevens[14]. Deze kopie dient in een gangbare elektronische vorm te worden verstrekt, tenzij het verzoek op papier is gedaan of de Betrokkene expliciet om een papieren kopie verzoekt.

---

[13] Zie o.a. nummer 63 van de considerans van de AVG, rechtbank Amsterdam 20 juni 2019 ECLI:NL:RBAMS:2019:4418, Hof Den Bosch 1 februari 2018 ECLI:GHSHE:2018:363 en rechtbank Noord-Holland 23 mei 2019, ECLI:NL:RBNHO:2019:4283

[14] ECLI:NL:RBMNE:2020:5275

Kosten
Ieder [eerste] kopie kan kosteloos worden aangevraagd. [OPTIONEEL: Per [additioneel] kopie zal <de instelling> [echter] een vergoeding van administratieve kosten a € … in rekening brengen bij de Betrokkene.]

Rechten en vrijheden van anderen
<de instelling> zal bij verstrekking van de gegevens rekening houden met de rechten en vrijheden van anderen. Dit kan er bijvoorbeeld toe leiden dat bij het verstrekken van inzage in de persoonsgegevens van Betrokkene, de gegevens die herleidbaar zijn tot anderen worden afgeschermd of weggelakt.

5.11.1.2. Recht op gegevensoverdraagbaarheid

Gronden voor verzoek
Iedere Betrokkene kan een verzoek indienen bij <de instelling> om zijn gegevens te verkrijgen in een gestructureerde, gangbare en machine leesbare vorm dan wel deze rechtstreeks aan een andere Verwerkingsverantwoordelijke over te laten dragen, zonder daarbij te worden gehinderd door <de instelling>, indien is voldaan aan beide volgende voorwaarden:

1. De Verwerking door <de instelling> berust op de grondslag ‘toestemming’ dan wel ‘uitvoering van een overeenkomst met de Betrokkene’.
2. De Verwerking in kwestie is geheel geautomatiseerd.

Rechten en vrijheden van anderen
<de instelling> zal bij verstrekking van de gegevens rekening houden met de rechten en vrijheden van anderen.

Verwijderen van gegevens
Indien een Betrokkene zijn recht van gegevensoverdraagbaarheid heeft uitgeoefend in het kader van een Verwerking ter uitvoering van een overeenkomst, mag <de instelling> niet besluiten de gegevens te wissen. Na het verstrijken van de bewaartermijn, dient <de instelling> de gegevens echter alsnog te wissen.

Indien het recht is uitgeoefend in het kader van een Verwerking op grond van toestemming van de Betrokkene, mag <de instelling> wel besluiten om de gegevens te wissen na uitoefenen van het recht.

5.11.1.3. Recht op rectificatie, aanvulling, verwijdering of beperking van de Verwerking

Verzoek tot rectificatie, aanvulling, verwijdering of beperking
Iedere Betrokkene kan met betrekking tot over hem opgenomen Persoonsgegevens bij <de instelling> van deze gegevens verzoeken die te corrigeren, aan te vullen, te verwijderen of de Verwerking te beperken. Bij het recht op beperking worden de Persoonsgegevens tijdelijk afgeschermd en niet meer verwerkt door <de instelling>. De beperking wordt duidelijk in het bestand aangegeven.

Kennisgeving
Indien blijkt dat de verwerkte Persoonsgegevens van de Betrokkene feitelijk onjuist zijn, voor het doel of doeleinden van de Verwerking onvolledig of niet ter zake dienend zijn dan wel anderszins in strijd met een wettelijk voorschrift zijn verwerkt, zal de gegevensbeheerder (dat kan zowel de Verwerkingsverantwoordelijke als de Verwerker zijn) deze gegevens verbeteren, permanent verwijderen, aanvullen dan wel beperken.

Bovendien worden Derden aan wie de gegevens, voorafgaand aan de rectificatie, aanvulling, verwijdering dan wel beperking, zijn verstrekt hiervan in kennis gesteld, tenzij dit redelijkerwijs niet mogelijk of gezien de omstandigheden niet relevant is. De verzoeker mag opgave verzoeken van degene aan wie <de instelling> deze mededeling heeft gedaan.
Termijn voor uitvoering

De verwerkingsverantwoordelijke zorgt ervoor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd. De uitvoering hiervan geschiedt voor de Betrokkene.

5.11.1.4. Recht van bezwaar

Gronden voor bezwaar

Voor Betrokkenen bestaan er twee gronden om bezwaar te maken tegen een Verwerking:

1. In verband met zijn of haar persoonlijke omstandigheden, mag iedere Betrokkene bezwaar maken tegen Verwerking bij <de instelling>, als deze Verwerking plaatsvindt op grond van
   a. de vervulling van een taak van algemeen belang of in het kader van de uitoefening van het openbaar gezag van de Verwerkingsverantwoordelijke, of
   b. de behartiging van het gerechtvaardigd belang van <de instelling> of van een Derde aan wie de gegevens worden verstrekt.

   <de instelling> zal bij bezwaar de verdere Verwerking in beginsel staken. Indien <de instelling> kan aantonen dat zijn dwingende gerechtvaardigde belangen zwaarder wegen dan de belangen of grondrechten en de fundamentele vrijheden van de Betrokkene, zal de Verwerking worden voortgezet. Indien het bezwaar gerechtvaardigd is, treft <de instelling> (kosteloos) maatregelen die nodig zijn om de Persoonsgegevens voor de betreffende doeleinden niet meer te verwerken.

2. Bij een Verwerking met het doel ‘direct marketing’, heeft een Betrokkene te allen tijde het recht om bezwaar te maken. <de instelling> zal bij bezwaar de Verwerking voor direct marketing doeleinden direct staken en gestaakt houden.

5.11.1.5. Geautomatiseerde besluitvorming

Gronden

Betrokkenen hebben het recht om niet onderworpen te worden aan een uitsluitend op geautomatiseerde Verwerking gebaseerd besluit, waaraan voor hem rechtsgevolgen zijn verbonden. Onder een ‘besluit gebaseerd op een geautomatiseerde Verwerking’ wordt verstaan een besluit dat is gemaakt zonder menselijke tussenkomst. Hieronder valt onder andere Profilering.

Slechts in de volgende drie situaties mag <de instelling> besluiten nemen op grond van geautomatiseerde Verwerking:

1. Indien het besluit noodzakelijk is bij de sluiting of uitvoering van een overeenkomst met de Betrokkene.
2. Indien het besluit is toegestaan bij een Europese of nationale wet, mits deze wet voorziet in passende maatregelen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de Betrokkene.
3. Indien het besluit berust op uitdrukkelijke toestemming van de Betrokkene. Deze toestemming kan te allen tijde worden ingetrokken.

In alle hierboven beschreven situaties, zal <de instelling> passende maatregelen nemen ter bescherming van de rechten en vrijheden en gerechtvaardigde belangen van de Betrokkene. Hieronder zullen tenminste vallen het recht op menselijke tussenkomst door <de instelling>, het recht van de Betrokkene om zijn standpunt kenbaar te maken, alsmede het recht om het besluit aan te vechten. Minderjarigen zullen nimmer worden onderworpen aan geautomatiseerde besluitvorming.

5.11.1.6. Rechtsbescherming

Algemene klachten

Indien de Betrokkene van mening is dat de wettelijke bepalingen inzake de privacybescherming dan wel de bepalingen van dit beleid jegens hem niet correct worden gehandhaafd, kan hij een schriftelijke klacht indienen bij <de instelling | een algemeen klachtenloket van de instelling | FG>.

Overige bezwaarmogelijkheden

Naast de algemene interne klachtenprocedure zoals hierboven beschreven, heeft de Betrokkene de volgende mogelijkheden als hij het idee heeft dat <de instelling> een hem rakende overtreding van de AVG heeft begaan:

A. *Verzoekschriftprocedure bij de rechtbank*

Indien <de instelling> afwijzend heeft beslist op een verzoek zoals beschreven in paragraaf 8.1 t/m 8.6 van dit Beleid, of <de instelling> heeft het verzoek van de Betrokkene afgewezen, dan wel naar de opvatting van de Betrokkene onvoldoende beantwoord, dan heeft de Betrokkene op grond van artikel 35 lid 2 Uitvoeringswet Algemene Verordening Gegevensbescherming de mogelijkheid een verzoekschriftprocedure te starten bij de rechtbank.

Het verzoekschrift dient binnen zes weken na ontvangst van het antwoord van <de instelling> ingediend te worden bij de rechtbank. Indien <de instelling> niet binnen de gestelde termijn heeft geantwoord op het verzoek van Betrokkene, moet het verzoekschrift binnen zes weken na afloop van die termijn worden ingediend. Indiening van het verzoekschrift hoeft niet door een advocaat te geschieden.

[OPTIONEEL: indien een besluit wordt aangemerkt als besluit van bestuursorgaan (rijksuniversiteiten?): dan is A niet van toepassing en dan A vervangen door dit artikel

Bezwaar en beroep

Indien <de instelling> afwijzend heeft beslist op een verzoek zoals beschreven in paragraaf 8.1 t/m 8.6 van dit Beleid, of <de instelling> heeft het verzoek van de Betrokkene afgewezen, en het besluit van <de instelling> is aan te merken als een besluit van een bestuursorgaan in de zin van artikel 6 lid 4 van de Awb, heeft de Betrokkene de mogelijkheid een bezwaarschriftprocedure te starten. Een bezwaarschriftprocedure moet altijd gestart worden binnen 6 weken na bekendmaking van een besluit van <de instelling>. Tegen de beslissing op bezwaar, staat beroep open bij de rechtbank.

B. *Verzoek tot handhaving bij toezichthoudende autoriteit*

Indien <de instelling> afwijzend heeft beslist op een verzoek zoals beschreven in paragraaf 8.1 t/m 8.6 van dit Beleid, of <de instelling> heeft het verzoek van de Betrokkene afgewezen, heeft de Betrokkene de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens, dan wel om een belangenorganisatie namens hem op te laten treden.

5.12. Verantwoordingsplicht

<de instelling> heeft meerdere maatregelen getroffen om aan te tonen te voldoen aan de wettelijke eisen uit de AVG, waaronder implementatie van het onderhavige Beleid. [OPTIONEEL: <de instelling> maakt gebruik van het toetsingskader Privacy van SURF en neemt twee jaarlijks deel aan de benchmark]

5.12.1. Register van verwerkingsactiviteiten

De intern verantwoordelijke van <de instelling> zorgt ervoor dat iedere (geheel of gedeeltelijk geautomatiseerde) verwerking van Persoonsgegevens wordt opgenomen in het Register van Verwerkingsactiviteiten, waarmee het onder toezicht valt van de FG. De <FG/CPO/informatiemanager> beoordeelt de rechtsgeldigheid van de verwerking en de <CPO/informatiemanager> draagt zorg voor adequate documentatie van alle relevante gegevens. De FG toetst of de inrichting van het Register van verwerkingsactiviteiten voldoet aan de vereisten van artikel 30 AVG en draagt zorg voor de controle en monitoring van de documentatie/ bewijsvoering van de geregistreerde verwerkingen.

5.12.2. Data Protection Impact Assessments

Tevens voert <de instelling> een Data Protection Impact Assessment (DPIA) uit, bij (onderzoeks-)projecten, infrastructurele wijzigingen of de aanschaf van nieuwe systemen die waarschijnlijk een hoog risico inhouden voor de rechten en vrijheden van natuurlijke personen. Bij het opstellen van een DPIA wordt de FG om advies gevraagd.

Indien de Verwerking een hoog risico zou betekenen als <de instelling> geen maatregelen neemt om het risico te beperken, raadpleegt <de instelling> voorafgaand aan de verwerking, de toezichthoudende autoriteit.

[OPTIONEEL: Vanwege de aanzienlijke materiële risico's is de risicoanalyse op privacybescherming en informatiebeveiliging opgenomen in de Governance Code van <de instelling> en daarmee ondergebracht in het aandachtgebied van <de toezichthouder>].

[OPTIONEEL: <de instelling> gebruikt [deze methode] voor het opstellen van een DPIA. Criteria om te bepalen of een DPIA verplicht is staan in bijlage A].

5.12.3. Datalek register

Van een Datalek is sprake als er een inbreuk op de beveiliging van Persoonsgegevens plaatsvindt, die per ongeluk of op onrechtmatige wijze leidt tot enige ongeoorloofde Verwerking daarvan. Het kan hierbij bijvoorbeeld gaan om een diefstal van een laptop, een verloren usb-stick, verkeerd uitgegeven autorisatie of een e-mail die naar de verkeerde persoon is verstuurd. Alle datalekken moeten intern gemeld worden bij [de FG/ servicepunt datalekken]. Sommige datalekken moeten worden gemeld bij de toezichthoudende autoriteit en in sommige gevallen ook bij de Betrokkene. De beoordeling of een melding bij de Autoriteit Persoonsgegevens gedaan wordt ligt bij […FG/CvB/CPO…]. Melding bij de toezichthoudende autoriteit dient binnen 72 na ontdekking plaats te vinden en wordt gedaan door […..FG/CvB/CPO….]

<de instelling> heeft een procedure voor het afhandelen van datalekken.

6. Tot slot

Dit Beleid is vastgesteld door <het CvB | de directie> van <de instelling> dd. <datum> [, na <instemming|positief advies> van <het medezeggenschapsorgaan>].
[Een review van het beleid maakt onderdeel uit van de <1|2 jaarlijkse plan-do-check-act cyclus> van <de instelling>. Daarin is ook een controle op de effectiviteit van de maatregelen opgenomen.]

Aanpassingen van dit beleid worden aangekondigd via < Instellingsbrede email | een huisorgaan | …> en de meest recente versie is gepubliceerd op <een internetpagina van de instelling>.

Voor vragen of opmerkingen met betrekking tot dit Beleid kunt u terecht bij <FG| servicedesk |…>.

Bijlage A: Criteria voor uitvoering DPIA

De Europese privacy toezichthouders hebben 9 criteria opgesteld om te beoordelen of een voorgenomen Verwerking van Persoonsgegevens een hoog privacy risico voor Betrokkenen oplevert. De vuist regels is dat een DPIA uitgevoerd moet worden als de Verwerking aan 2 of meer van onderstaande criteria voldoet. Voor uitgebreide toelichting zie het richtsnoer van de EDPB hierover[15].

1. Evaluatie of score toekenning (incl. profielbepaling en voorspelling)
2. Geautomatiseerde besluitvorming met rechtsgevolg of vergelijkbaar wezenlijk gevolg
3. Stelselmatige monitoring
4. Gevoelige gegevens of gegevens van zeer persoonlijke aard
5. Op grote schaal verwerkte gegevens
6. Matching of samenvoeging van datasets
7. Gegevens met betrekking tot kwetsbare betrokkenen
8. Innovatief gebruik of innovatieve toepassing van nieuwe technologische of organisatorische oplossingen
9. De situatie waarin als gevolg van de verwerking zelf ″betrokkenen [...] een recht niet kunnen uitoefenen of geen beroep kunnen doen op een dienst of een overeenkomst″

De Autoriteit Persoonsgegeven heeft een lijst samengesteld van Verwerking waarvoor het uitvoeren van een DPIA altijd verplicht is. Uitgebreide toelichting is te vinden op de website van de Autoriteit Persoonsgegevens[16].

Verwerkingen met verplichte DPIA:

1. Heimelijk onderzoek
2. Zwarte lijsten
3. Fraudebestrijding
4. Creditscores
5. Financiële situatie
6. Genetische Persoonsgegevens
7. Gezondheidsgegevens
8. Samenwerkingsverbanden
9. Cameratoezicht
10. Flexibel cameratoezicht
11. Controle werknemers
12. Locatiegegevens
13. Communicatiegegevens
14. Internet of things
15. Profilering
16. Observatie ene beïnvloeding van gedrag
17. Biometrische gegevens

[15] wp248 rev.01_nl (autoriteitpersoonsgegevens.nl)
[16] Data protection impact assessment (DPIA) | Autoriteit Persoonsgegevens