Model beleid verwerking persoonsgegevens

Utrecht, maart 2018
Versienummer: 2.0

Colofon

Model beleid verwerking persoonsgegevens

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 Gezamenlijk product van de SURF Projectgroep 'Voorbereiding Implementatie Algemene Verordening Gegevensbescherming' en SURFibo (nu SCIPR). Aan de oorspronkelijke versie werkten mee Frans Pingen (Wageningen University), Bart van den Heuvel (Maastricht University) Sedat Capkin (SURFsara), Ronja Meijer (Wageningen University) Jaap Gall (Hogeschool Arnhem Nijmegen) Chloë Baartmans (SURFnet).

Versie 2.0 maart 2018

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

Opslag en 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

AVG: Algemene Verordening Gegevensbescherming[1].

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

Betrokkene: een individueel en natuurlijk persoon op wie een Persoonsgegeven betrekking heeft.

Verwerkingsverantwoordelijke: college van bestuur van <de instelling> die het doel en de middelen van de Verwerking van Persoonsgegevens vaststelt.

Persoonsgegeven: elk gegeven betreffende een geïdentificeerd of identificeerbaar natuurlijk persoon.

Verwerker: een door <de instelling> ingeschakelde (derde) partij die ten behoeve van <de instelling>, en op basis van diens schriftelijke instructies, Persoonsgegevens verwerkt.

Verwerking: elke handeling of geheel van handelingen met betrekking tot Persoonsgegevens, waaronder het verzamelen, vastleggen, ordenen, opslaan, raadplegen, bijwerken, afschermen, wissen of vernietigen van gegevens.

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

Datalek: een inbreuk op de beveiliging van Persoonsgegevens, die leidt tot enige ongeoorloofde Verwerking daarvan. Hier vallen zowel opzettelijke als onopzettelijke datalekken onder.

Privacy by Default: een gegevensverwerking waarbij de standaardinstellingen van producten en diensten zo zijn ingesteld dat de privacy van Betrokkenen maximaal wordt gewaarborgd. Dit betekent onder meer dat er zo min mogelijk gegevens worden gevraagd en verwerkt.

Privacy by Design: Het beheer van de gehele levenscyclus van Persoonsgegevens, vanaf het verzamelen tot het verwerken en verwijderen, waarbij mechanismen zo zijn ontworpen dat zij zo veel mogelijk rekening houden met de privacy van Betrokkenen. Hierbij wordt stelselmatig aandacht be-

[1] De Algemene Verordening Gegevensbescherming is op 25 mei 2016 in werking getreden en per 25 mei 2018 van kracht.

steed aan allesomvattende waarborgen m.b.t. nauwkeurigheid, vertrouwelijkheid, integriteit, fysieke veiligheid en verwijdering van de Persoonsgegevens.

Privacy Impact Assessment (gegevensbeschermingseffectbeoordeling): Een beoordeling die helpt bij het identificeren van privacy risico's en de handvaten levert om deze risico's te verkleinen tot een acceptabel niveau.

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

Minderjarige: iedere persoon die de leeftijd van 16 jaar nog niet heeft bereikt.

1.2. Reikwijdte en doelstelling 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> alsmede op de daaraan ten grondslag liggende documenten die in een bestand zijn opgenomen. Eveneens is het Beleid van toepassing op niet-geautomatiseerde verwerking van Persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.

Bij <de instelling> wordt het beschermen van Persoonsgegevens breed geïnterpreteerd. 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>.

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: de basis voor de beveiliging van Persoonsgegevens is ISO 27001[2]. Maatregelen worden op basis van 'best practices' in het hoger onderwijs en o.b.v. ISO 27002 genomen[3].
- Het SURF Juridisch Normenkader (Cloud)services[4] 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.

[2]Voluit: NEN-ISO/IEC 27001: Eisen aan Managementsystemen voor informatiebeveiliging
[3]Voluit: NEN-ISO/IEC 27002: Code voor Informatiebeveiliging
[4]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.

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:

- Een Verwerking van Persoonsgegevens is gebaseerd op een van de wettelijke grondslagen zoals genoemd in artikel 6 van de AVG (“rechtmatigheid”).
- Persoonsgegevens worden alleen verwerkt op een manier die ten aanzien van de Betrokkene behoorlijk en transparant is. Dit houdt in dat het voor betrokkenen inzichtelijk moet zijn in hoeverre en op welke manier er Persoonsgegevens worden verwerkt. Informatie en communicatie hierover moet eenvoudig toegankelijk en begrijpelijk zijn (“behoorlijkheid en transparantie”).
- Persoonsgegevens worden alleen verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Het gaat hier om specifieke en gerechtvaardigde doeleinden, die zijn vastgelegd en omschreven voordat men begint met de Verwerking. Persoonsgegevens worden niet verder Verwerkt op een wijze die onverenigbaar is met de doeleinden waarvoor ze zijn verkregen (“doelbinding”).
- Bij een Verwerking van Persoonsgegevens blijft de hoeveelheid en het soort gegevens beperkt tot de Persoonsgegevens die noodzakelijk zijn voor het specifieke doeleinde. De gegevens dienen met het oog op dat doel toereikend, ter zake dienend en niet bovenmatig te zijn (“minimale gegevensverwerking”).
- Verwerking van Persoonsgegevens gebeurt op de minst ingrijpende wijze en dient in redelijke verhouding te staan tot het beoogde doeleinde (“minimale gegevensverwerking”).
- Er worden maatregelen getroffen om zoveel mogelijk te waarborgen dat de te verwerken Persoonsgegevens juist en actueel zijn (“juistheid”).

Persoonsgegevens worden adequaat beveiligd volgens de geldende beveiligingsnormen (“integriteit en vertrouwelijkheid”). Persoonsgegevens worden niet langer verwerkt dan noodzakelijk is voor de doeleinden van de Verwerking. Hierbij worden de van toepassing zijnde bewaar- en vernietigtermijnen in acht genomen (“opslagbeperking”).

3. Wet- en regelgeving

Bij <de instelling> wordt op de volgende wijze omgegaan met relevante 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

<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 door middel van het Beleid.

3.3. Archiefwet

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

3.4. [OPTIONEEL bij Openbare netwerken] Telecommunicatiewet

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.

4. 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. 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.

4.2. Portefeuillehouder beveiliging Persoonsgegevens

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

4.3. Functionaris gegevensbescherming

<de instelling> zal een interne toezichthouder op de Verwerking van Persoonsgegevens aanstellen. Deze toezichthouder wordt functionaris gegevensbescherming genoemd (hierna: “FG”). De FG zal door <de instelling> tijdig worden 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> zal de FG aanmelden bij de toezichthoudende autoriteit.

De taken van de FG zullen inhouden:

- 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 privacybeleid door <de instelling>;
- het toezien op een Privacy Impact Assessment;
- het samenwerken met de toezichthoudende autoriteit;
- fungeren als eerste aanspreekpunt voor de toezichthoudende autoriteit.

4.4. Systeemeigenaar

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.

4.5. 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.

5. Implementatie Beleid

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 goed, efficiënt en verantwoord leiden van een organisatie wordt vaak aangeduid met de term governance. Het omvat vooral ook de relatie met de belangrijkste belanghebbenden van <de instelling>, zoals de eigenaren, werknemers, studenten, andere afnemers en de samenleving als geheel. Een goed corporate governance-beleid draagt zorg voor de rechten van alle Betrokkenen.

5.1. Verdeling van de verantwoordelijkheden

- 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 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.

5.2. 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>]

5.3. 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 de verantwoordelijkheid van <de functionaris gegevensbescherming | de (decentrale) Security Managers, |de (centrale) Security Officer>.

5.4. Controle en naleving

Audits maken het mogelijk het Beleid en de genomen maatregelen te controleren op effectiviteit. De FG initieert gezamenlijk met de Information Security Officer 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 op de bescherming van data- en privacygegevens ernstig tekortschieten, dan kan <de instelling> de betrokken verantwoordelijke 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.

6. Rechtmatige en zorgvuldige Verwerking van Persoonsgegevens

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

6.1. Grondslag

<de instelling> verwerkt slechts Persoonsgegevens als er sprake is van een van de wettelijke gronden 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.

6.2. Privacyverklaring

<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 inzichtelijk maakt in hoeverre en op welke manier diens Persoonsgegevens verwerkt worden. Bij het verzamelen van de Persoonsgegevens zal <de instelling> middels een privacyverklaring de Betrokkene inlichten. Inlichting zal plaatsvinden voorafgaand aan de Verwerking, tenzij dit redelijkerwijs niet mogelijk is. Zie nader paragraaf 8.1 van dit Beleid.

6.3. Bewaartermijnen

Persoonsgegevens worden niet langer bewaard dan noodzakelijk is voor de doeleinden waarvoor zij zijn verzameld of worden gebruikt, in overeenstemming met het uitgewerkte bewaarbeleid van <de instelling>. Persoonsgegevens dienen na het verlopen van de bewaartermijn[6] buiten het bereik van de actieve administratie gebracht te worden. <De instelling> zal de Persoonsgegevens na het verlopen van de bewaartermijn vernietigen of, indien de Persoonsgegevens bestemd zijn voor historische, statistische of wetenschappelijke doeleinden, in een archief bewaren.

6.4. Passende beveiligingsmaatregelen

<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>.

6.5. Documentatieplicht

<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.

Daarnaast dient elke geheel of gedeeltelijk geautomatiseerde Verwerking van Persoonsgegevens gemeld te worden bij de FG van <de instelling>. De FG beoordeelt de rechtsgeldigheid van de Verwerking en draagt zorg voor adequate documentatie van alle relevante gegevens.

Tevens voert <de instelling> een Privacy Impact Assessment 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. Als hieruit blijkt dat de Verwerking een hoog risico zou betekenen indien <de instelling> geen maatregelen neemt om het risico te beperken, raadpleegt <de instelling> voorafgaand aan de verwerking, de toezichthoudende autoriteit.

6.6. Privacy by Design en Privacy by Default

<De instelling> hanteert bij de implementatie van iedere Verwerking de principes “Privacy by Design” en “Privacy by Default”.

[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>].

6.7. Geheimhouding

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.

6.8. Bijzondere Persoonsgegevens

Het verwerken van bijzondere Persoonsgegevens is in beginsel verboden, tenzij er sprake is van een van de wettelijke uitzonderingen uit de AVG, waar onder meer 'uitdrukkelijke toestemming van de Betrokkene' en een 'zwaarwegend algemeen belang' onder vallen. Tevens gelden zwaardere eisen voor de beveiliging van deze bijzondere Persoonsgegevens. Daar waar de basisbescherming niet voldoende is moeten voor elk informatiesysteem individueel afgestemde extra maatregelen worden genomen.

Onder bijzondere Persoonsgegevens vallen de volgende gegevens:

- gegevens waaruit ras of etnische afkomst blijkt;
- politieke opvattingen;
- religieuze of levensbeschouwelijke overtuigingen;
- gegevens waaruit lidmaatschap van een vakbond blijkt;
- genetische gegevens met het oog op de unieke identificatie van een persoon;
- biometrische gegevens met het oog op de unieke identificatie van een persoon;
- gegevens over gezondheid;
- gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.

Voor twee soorten Persoonsgegevens geldt dat zij niet onder de categorie bijzondere Persoonsgegevens vallen, maar dat de Verwerking en beveiliging ervan wel aan strenge eisen zijn gebonden:

a. Verwerking van Persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten mag slechts onder toezicht van de overheid of binnen Europese of nationale wetgeving.

b. Onder de Nederlandse wetgeving mag een nationaal identificatienummer (het BSN of het onderwijsnummer) alleen worden verwerkt als dat wettelijk is bepaald.

6.9. Doorgifte Persoonsgegevens

6.9.1. Uitbesteden van Verwerking aan 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.

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

<de instelling> verstrekt Persoonsgegevens alleen aan een Verwerker gevestigd binnen de EER, als de verwerking is gebaseerd op een van de grondslagen voor gegevensverwerking uit artikel 6 of artikel 9 AVG en als de Verwerker voldoet aan de wettelijke vereisten uit de AVG.

6.9.3. Doorgifte Persoonsgegevens buiten de EER

<de instelling> verstrekt Persoonsgegevens alleen aan Verwerkers die zich bevinden in een land buiten de EER, indien aan een van de volgende voorwaarden is voldaan:

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[7];
- Het Privacy Shield voor bedrijven in de Verenigde Staten, gepubliceerd door de Europese Commissie i.s.m. de US Department of Commerce[8].

2. Doorgifte vindt plaats op basis van **passende waarborgen** uit de AVG, artikel 46 en 47.

3. Doorgifte vindt plaats op basis van een van de **wettelijke uitzonderingen** uit artikel 49 van de AVG.

6.10. Vragen- en klachtenprocedure

6.10.1. Melding en registratie

Vragen of klachten in verband met (de verwerking van) Persoonsgegevens kunnen gemeld worden bij […]. Van vragen of klachten met een (potentiele) significante impact, zal een register bijgehouden worden.

Vragen en klachten kunnen worden gemeld door eenieder, waaronder Betrokkenen, Verwerkers of Derden.

6.10.2. Zwakke plekken in de beveiliging

Werknemers zullen waargenomen zwakke plekken in systemen of diensten registreren en direct rapporteren bij [het meldpunt Datalekken persoonsgegevens/ […]]. Van alle meldingen betreffende zwakke plekken in de beveiliging zal een register bijgehouden worden.

6.10.3. Afhandeling

Vragen, klachten en zwakke plekken in de beveiliging worden doorgezet naar de verantwoordelijke afdeling of persoon en vervolgens conform de daarvoor vastgestelde procedures zo snel mogelijk afgehandeld.
Als de Persoonsgegevens van Betrokkene(n) of de bedrijfsprocessen, de financiën of goede naam van
<de instelling> ernstig in gevaar zijn, wordt in ieder geval het college van bestuur en indien aanwezig ook de FG op de hoogte gesteld.

6.10.4. Evaluatie

Het is van belang om te leren van de feedback die middels de vragen- en klachtenprocedure wordt geleverd. Registratie van significante vragen, klachten en zwakke plekken en een periodieke rapportage daarover horen thuis bij een professionele manier van verwerken van Persoonsgegevens. De rapportage hierover maken daarom een vast onderdeel uit van de jaarrapportage van het college van bestuur, en indien aanwezig die van de FG.

---

[6] 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.
[7] Deze kunt u vinden via de volgende link http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.
[8] Deze kunt u vinden via de volgende link https://www.privacyshield.gov/list.

7. Datalek

Dit hoofdstuk beschrijft het beleid met betrekking tot de melding, registratie en afhandeling van een Datalek of het vermoeden van een Datalek in de reguliere bedrijfsvoering en in bijzondere omstandigheden.

7.1. Datalek

Van een Datalek is sprake als er een inbreuk op de beveiliging van Persoonsgegevens plaatsvindt, die leidt tot enige ongeoorloofde Verwerking daarvan. Het kan hierbij bijvoorbeeld gaan om een diefstal van een laptop, een in de trein vergeten usb-stick of een e-mail die naar de verkeerde persoon is verstuurd. Datalekken moeten worden gemeld bij de toezichthouder binnen 72 uur na ontdekking daarvan en in sommige gevallen ook bij de Betrokkene.

7.2. Melding en registratie

Een Datalek kan bij <de instelling> zowel binnen de eigen organisatie ontstaan, maar ook bij een door <de instelling> ingeschakelde Verwerker. De volgende situaties moeten hierbij worden onderscheiden:

a. *Medewerker*: medewerkers moeten, indien zij een (mogelijk) Datalek waarnemen of vermoeden zelf onderdeel te zijn van een Datalek, contact opnemen met [het meldpunt datalekken Persoonsgegevens] via [het meldpunt Datalekken persoonsgegevens] of in uitzonderlijke gevallen bij [de vertrouwenspersoon of personeels- / studentbegeleiding] van <de instelling>.
b. *Verwerker:* het is ook mogelijk dat er een Datalek plaatsvindt bij een door <de instelling> ingeschakelde Verwerker. De Verwerker zal overeenkomstig de afgesloten verwerkersovereenkomst het Datalek melden aan <de instelling>.

c. *Andere personen:* indien een ander dan een medewerker of een Verwerker een (mogelijk) Datalek waarneemt of zelf onderdeel is van een Datalek, dient contact opgenomen te worden met [het meldpunt datalekken Persoonsgegevens] via [contactgegevens het meldpunt Datalekken persoonsgegevens].

Een melding van een (mogelijk) Datalek dient zo spoedig mogelijk te worden gemaakt. De volgende gegevens dienen doorgegeven te worden bij melding van een Datalek:

- Wie heeft er gemeld?
- Wat is er gemeld?
- Waar kwam de melding vandaan?
- Om welke data (gegevens) gaat het?
- Hoe heeft het incident plaatsgevonden?
- Welke systemen zijn betrokken bij/geraakt door het incident?
- Wanneer heeft het incident plaatsgevonden?
- Indien de melding is gedaan door een medewerker van <de instelling>: wat is er gedaan om het incident op te lossen/in de toekomst te voorkomen?

Elk Datalek en de afhandeling daarvan zal worden bijgehouden in een register.

7.3. Afhandeling

Indien sprake is van een Datalek wordt deze conform de in de relevante wet- en regelgeving opgenomen specifieke bepalingen over Datalekken afgehandeld, zoals beschreven in de beleidsregels meldplicht datalekken van de Autoriteit Persoonsgegevens[10], zodat de melding van het Datalek tijdig de juiste personen, en uiteindelijk de toezichthouder en Betrokkenen bereikt.

Als de Persoonsgegevens van Betrokkene(n) of de bedrijfsprocessen, de financiën of goede naam van
<de instelling> ernstig in gevaar zijn, wordt in ieder geval het college van bestuur en indien aanwezig ook de FG op de hoogte gesteld.

7.4. Besluitvorming

Nadat er een melding heeft plaatsgevonden van een (mogelijk) Datalek overeenkomstig de voorgaande paragrafen, zal [het meldpunt Datalekken persoonsgegevens] een advies uitbrengen omtrent de verplichting om te melden aan de toezichthoudende autoriteit en de Betrokkene. Dit advies zal door [de FG/het college van bestuur] in overweging worden genomen. [De FG/Het college van bestuur] zal verantwoordelijk zijn voor het besluit om al dan niet de melding te maken.

7.5. Evaluatie

Het is van belang om te leren van Datalekken om de waarschijnlijkheid van toekomstige Datalekken te verkleinen. Registratie van Datalekken en een periodieke rapportage daarover horen thuis bij een professionele manier van verwerken van Persoonsgegevens. De rapportage over Datalekken met betrekking tot Persoonsgegevens maken daarom een vast onderdeel uit van de jaarrapportage van het college van bestuur en van de FG.

7.6. [OPTIONEEL: Bijzondere omstandigheden]

Om voorbereid te zijn op (de dreiging tot) Datalekken op het gebied van Persoonsgegevens in bijzondere omstandigheden heeft <de instelling> een [speciaal operationeel team | Privacy Incident Response Team (PIRT)[11]] ingesteld.

Dit team heeft als voornaamste taak om te acteren bij incidenten met Persoonsgegevens in die gevallen waarbij de staande organisatie een incident niet via de standaardprocedures kan oplossen. Dit kan zijn omdat het incident plaatsvindt buiten de reguliere openingstijden van <de instelling>, in een periode waarbij de reguliere bedrijfsprocessen verstoord zijn of omdat de aard van het incident vraagt om noodmaatregelen en/of specifieke mandaten om deze maatregelen uit te voeren.

Het [PIRT-]team werkt volgens een door [het college van bestuur] vastgesteld Operationeel Model <referentie> en heeft bijzondere mandaten die overeenkomen met de mandaten van de FG, waarbij het team altijd achteraf verantwoording moet afleggen waarom en op welke wijze het team van deze mandaten gebruik heeft gemaakt.

Het team heeft een directe link naar het college van bestuur van <de instelling> als Verwerkingsverantwoordelijke in het kader van de relevante wet- en regelgeving.

[10] Beleidsregels meldplicht datalekken van de Autoriteit Persoonsgegevens: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf.
[11] Vergelijkbaar met het [CSIRT- | CERT-]team: [Computer Security Incident Response Team | Computer Emergency Response team]

8. 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].

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

- **Melding 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 vier weken na indiening schriftelijk gereageerd. Hierbij zal de Betrokkene in ieder geval in kennis worden gesteld over het gevolg dat aan het verzoek is gegeven. Indien de termijn van vier weken 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.

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 kosteloos 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.

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’.
- In voorkomend geval, het voornemen van de Verwerkingsverantwoordelijke om de Persoonsgegevens door te geven aan een derde land, welk land dit is en op welke grond de Persoonsgegevens daarnaartoe worden verstuurd.

- 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 dataportabiliteit.
- Het recht om een klacht in te dienen bij de toezichthoudende autoriteit.
- De ontvangers of categorieën van ontvangers van de Persoonsgegevens.
- Indien de Verwerking is gebaseerd op de grondslag 'toestemming', het recht van de Betrokkene om die toestemming te allen tijde in te trekken.
- 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 vier weken, na verkrijging van de gegevens, dan wel bij het eerste contact met de Betrokkene, worden verstrekt.

8.2. 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.

•*Mededeling*

Indien gegevens worden verwerkt, bevat de mededeling van <de instelling> een volledig overzicht van de volgende gegevens:

- Een omschrijving van de doeleinden van de Verwerking.
- De categorieën van gegevens waarop de Verwerking betrekking heeft.
- Categorieën van ontvangers.
- 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.
- Het recht van Betrokkene om de Verwerkingsverantwoordelijke te verzoeken om rectificatie of wissen van gegevens, beperking of bezwaar van Verwerking alsmede het recht op dataportabiliteit.
- Het recht van de Betrokkene om een klacht in te dienen bij een toezichthoudende autoriteit.
- 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.

Kopie
De Betrokkene kan om een kopie van alle Persoonsgegevens verzoeken. 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.

- *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.

8.3. Recht op dataportabiliteit

- *Gronden voor verzoek*

Iedere Betrokkene kan een verzoek indienen bij <de instelling> om (kosteloos) zijn gegevens te verkrijgen in
een gestructureerde, gangbare en machineleesbare 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 de 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 dataportabiliteit 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.

8.4. 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 opgenomen 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 functioneel beheerder 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 gegevensbeheerder zorgt ervoor dat een beslissing tot verbetering, aanvulling, verwijdering of afscherming zo spoedig mogelijk wordt uitgevoerd. De uitvoering hiervan geschiedt kosteloos voor de Betrokkene.

8.5. 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. Zie voor een beschrijving van de grondslagen, paragraaf 6.1.

   <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 (kosteloos) staken en gestaakt houden.

8.6. 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.

8.7. Rechtsbescherming

- *Algemene klachten*

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

- *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. <u>Verzoekschriftprocedure bij de kantonrechter</u>

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 een verzoekschriftprocedure te starten bij de kantonrechter.

Het verzoekschrift dient binnen zes weken na ontvangst van het antwoord van <de instelling> ingediend te worden bij de kantonrechter. 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.

B. <u>Bezwaar en beroep</u>

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.

C. <u>Verzoek tot handhaving bij toezichthoudende autoriteit</u>

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 een toezichthoudende autoriteit, dan wel om een belangenorganisatie namens hem op te laten treden.

9. 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 |…>.