Privacy beleid

2020-2024

Inhoud

Inleiding

Vanaf 25 mei 2018 beschermen alle landen uit de Europese Unie de persoonsgegevens volgens dezelfde regels van de Algemene Verordening Gegevensbescherming (AVG). Dit privacy beleid is een uitwerking van één van de regels van de AVG, namelijk artikel 24 AVG. In het tweede lid van dat artikel wordt gezegd dat een gemeente in dit verband over beleid dient te beschikken.

Dit beleid is van toepassing op de gehele organisatie (dus ook bestuur, raad en griffie) en is primair gericht aan alle medewerkers die in het kader van hun taak persoonsgegevens verwerken. Het betreft een overkoepelend kader waarin de maatregelen op abstract niveau zijn uitgewerkt. In werkplannen, procedures en werkinstructies wordt een verdere uitwerking gegeven aan de wijze waarop de bescherming van persoonsgegevens is geborgd.

Inwoners, ondernemers, partners en medewerkers moeten er namelijk op kunnen vertrouwen dat gemeente Hilversum passende bescherming biedt bij de verwerking van persoonsgegevens. Dat is onder andere bepaald in de AVG, de bijbehorende Uitvoeringswet (UAVG) en sector specifieke wetgeving, bijvoorbeeld de Wet maatschappelijke ondersteuning 2015 (Wmo 2015), de Jeugdwet en de Wet structuur uitvoeringsorganisatie werk en inkomen (Wet suwi).

De gemeente Hilversum heeft in veel gevallen voor de uitvoering van haar (wettelijke) taken persoonsgegevens nodig. Zonder de verwerking van persoonsgegevens is het bijvoorbeeld onmogelijk om een uitkering aan een burger te verstrekken of een vergunning te verlenen.
Maar wat te doen bij nieuwe beleidsontwikkelingen of ICT waarin persoonsgegevens nodig zijn. Hoe vindt dan een zorgvuldige afweging plaats van de risico's op de bescherming van privacy. Hoe wordt dat getoetst en wie is daar verantwoordelijk voor? De verwerking van persoonsgegevens leiden tot een zeker risico. Door passende gegevensbescherming wil de gemeente Hilversum risico's tegengaan. Daarom dit privacy beleid.

Dit privacy beleid vervangt het eerder opgestelde privacy beleid en –reglement 2018-2022. Dit is in 2018 opgesteld met het oog op de komst van de AVG, vastgesteld door het college. Een herijking van dit beleid was nodig om onder andere meer aandacht te vestigen op risico-gestuurd werken, de visie van het gemeentebestuur in het digitale tijdperk en verbinding te maken met de planning & control-cyclus.
Op basis van het jaarverslag van de Functionaris Gegevensbescherming (FG) is een meerjarenplan (4 jaar) uitgewerkt om de AVG binnen de gemeentelijke organisatie te borgen. Met deze jaarplannen wordt het volwassenheidsniveau bereikt waar de wetgever vanuit gaat. Dit herziende privacy beleid is een eerste stap in de verdere implementatie van de AVG. Hiermee kan de gemeente Hilversum op ieder moment maatschappelijk en juridisch uitleg geven over de deugdelijkheid van de aanpak en is daarmee aantoonbaar in de naleving van de AVG.

Ambitie en visie privacy

Persoonsgegevens en informatie zijn één van de voornaamste bedrijfsmiddelen van onze gemeentelijke organisatie. Zorgvuldige informatiestromen in de digitale maatschappij binnen de uitvoering van de (wettelijke) taken van de gemeente Hilversum is dan ook van groot belang.

Voor de inwoner is, mede gelet op de afhankelijkheidsrelatie met de overheid, van belang dat zij er op kunnen vertrouwen dat met hun persoonsgegevens zorgvuldig en verantwoord wordt omgegaan. Dit geldt uiteraard ook voor de medewerkers in relatie tot goed werkgeverschap van de gemeente.

Een zorgvuldige verwerking van de persoonsgegevens wordt juist bereikt met de naleving van de AVG en daagt ons uit om een stevige ambitie uit te spreken ten aanzien van het

gegevensbeschermingsniveau. Deze bescherming vindt de gemeente Hilversum dan ook van groot belang, zonder dat dit de dienstverlening aan de inwoner in de weg staat.

De ontwikkelingen in de samenleving en technologie maken dat privacy en informatiebeveiliging steeds belangrijker worden. Toenemende digitalisering en samenwerking met andere partijen in dienstverleningsketens leidt tot meer en sneller uitwisselen van informatie. Onze inwoners willen snel en digitaal geholpen worden, maar willen dit doen zonder dat dit de privacy onevenredig aantast.

Onze medewerkers willen en moeten steeds meer plaats en tijd onafhankelijk kunnen werken, maar dit mag niet leiden tot onrechtmatige toegang tot gegevens. Ook onze kantooromgeving is door het flexwerken, de samenwerking met andere partijen en het openbare karakter van het Raadhuis steeds meer een ontmoetingsplek, waar de gemeente gastheer is. De komende jaren wordt dan ook ingezet op het optimaliseren van gegevensbescherming, informatieveiligheid en het verder professionaliseren van de informatiebeveiligingsfunctie. Er zal steeds worden aangesloten op veranderde wetgeving op het gebied van gegevensbescherming, informatisering, digitalisering en informatiebeveiliging.

De gemeentelijke informatievoorziening faciliteert de gemeentelijke werkprocessen en:

- wij zorgen voor een juiste uitvoering van onze (wettelijke) taken en dienstverlening;
- wij waarborgen de bescherming van persoonsgegevens, zoals de AVG dit voorschrijft;
- wij leven ook overige wet- en regelgeving na op het gebied van gegevensbescherming;
- wij handelen op dit vlak steeds transparant en controleerbaar;
- wij leggen rekenschap af over beleid en maatregelen;
- wij bieden personen medezeggenschap via onze AVG-dienstverlening;
- wij bieden in dit kader voortdurend passende informatieveiligheid volgens de richtsnoeren van de Baseline Informatiebeveiliging Overheid (BIO).

Leeswijzer

Dit privacy beleid is opgedeeld in twee delen en sluit af met een bijlage. Het eerste deel betreft een algemeen deel, waarin onder andere de wettelijke kaders, de totstandkoming van het beleid en de uitgangspunten bij verwerking van persoonsgegevens uiteen zijn gezet. Het tweede deel beschrijft de verantwoordelijkheden voor de uitvoering van dit beleid en hoe de ondersteuning en controle plaatsvinden.

In de bijlage is voorts een toelichting gegeven op belangrijke begrippen, bepalingen en procedures die betrekking hebben op de bescherming van persoonsgegevens in onze organisatie. Dit is met name van belang voor de medewerkers die met persoonsgegevens werken en de lijnmanagers die moeten zorgen dat dit op een verantwoorde wijze gebeurt.

1. Verwerking van persoonsgegevens

Wettelijk kader

Voor de bescherming van persoonsgegevens gelden de volgende wettelijke kaders:

- Algemene Verordening Gegevensbescherming (AVG);
- Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG).

Daarnaast is de verwerking van persoonsgegevens geregeld in diverse andere wet en regelgeving. Bijvoorbeeld de Gemeentewet, Wet maatschappelijke ondersteuning 2015, Jeugdwet, Participatiewet, Wet Suwi, Wet Basisregistraties personen, Wet en besluit justitiële en strafvorderlijke gegevens, Wet en besluit politiegegevens, Telecommunicatiewet, Wet tijdelijk huisverbod, Algemene wet bestuursrecht, Wet openbaarheid van bestuur, Wet hergebruik overheidsinformatie, Archiefwet 1995 en het ministerieel besluit Informatiebeveiliging Overheid.

Uitgangspunten

Iedereen die binnen de gemeente Hilversum werkzaam is, gaat verantwoord om met de bescherming van persoonsgegevens. Hierbij hanteren wij de volgende centrale uitgangspunten:

A) Persoonsgegevens worden rechtmatig, behoorlijk en transparant verwerkt

Wij verwerken alleen persoonsgegevens als dat noodzakelijk is voor het doel en er een geldige grondslag uit de AVG is aan te wijzen. Dat betekent dat de verwerking alleen plaatsvindt als dat in verhouding staat tot het doel en als het doel met een vergelijkbare inspanning bereikt kan worden met een lichter middel, voor dat lichtere middel wordt gekozen.
Daarbij informeren wij de betrokkene meestal vooraf voor welke doelen persoonsgegevens worden verwerkt en hoe dat gebeurt.

B) Doelbinding

Wij verwerken persoonsgegevens alleen als vooraf de doeleinden zijn bepaald en deze precies zijn omschreven. Wanneer de persoonsgegevens later voor een ander doel nodig zijn, dan gebruiken we dat alleen als het nieuwe doel verenigbaar is met het oorspronkelijke doel.

C) Minimale gegevensverwerking

Wij verwerken alleen die persoonsgegevens die minimaal noodzakelijk zijn voor het doel. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.

D) Persoonsgegevens zijn juist

Wij treffen alle redelijke maatregelen om te zorgen dat de gegevens correct en actueel zijn. Gegevens die dat niet (meer) zijn worden gewist of gecorrigeerd.

E) Persoonsgegevens worden niet langer bewaard dan nodig

Wij bewaren persoonsgegevens niet langer dan dat nodig is voor het doel waarvoor ze zijn verzameld. Wanneer de gegevens niet langer nodig zijn, worden ze vernietigd of gewist volgens de geldende regelgeving (Archiefwet 1995).

F) Integriteit en vertrouwelijkheid

Wij zorgen dat:

- persoonsgegevens goed beveiligd worden opgeslagen om misbruik, verlies, onbevoegde toegang en bewerking te voorkomen;

- aandacht wordt besteed bij inrichting van processen en systemen aan privacy verhogende maatregelen (privacy by design);
- persoonsgegevens beveiligd zijn en hierbij de Baseline Informatiebeveiliging Overheid (BIO) gehanteerd wordt;
- persoonsgegevens alleen toegankelijk zijn voor die functionarissen (ambtenaren, externen, leveranciers, convenantpartners) die dat nodig hebben voor de directe taakuitoefening;
- het gebruik van persoonsgegevens wordt vastgelegd met uitgevoerde handelingen (logging);
- er wordt gewerkt met geheimhoudingsverklaringen en contractuele afspraken bij het inschakelen van externen en leveranciers.

Verwerkingsverantwoordelijke

In de AVG is sterk de nadruk gelegd op de verantwoordelijkheid van organisaties en instanties, aangeduid als verwerkingsverantwoordelijke. Binnen de gemeentelijke organisatie kan dat alleen een bestuursorgaan zijn. Dat zijn onder andere de Burgemeester, het college van B&W, de Gemeenteraad, of de commissie Bezwaar en Beroep. Zo is bijvoorbeeld het college verwerkingsverantwoordelijke voor alle verwerkingen die binnen het sociaal domein plaatsvinden. De burgemeester is verwerkingsverantwoordelijke voor de verwerkingen binnen het terrein van de openbare orde en veiligheid. De gemeenteraad is verwerkingsverantwoordelijke voor onder meer de raadsleden en griffiewerkzaamheden. Dat betekent dat de ‘gemeente’ zelf geen bestuursorgaan is en in de zin van de AVG nooit een verwerkingsverantwoordelijke kan zijn.

De verwerkingsverantwoordelijke moet kunnen waarborgen dat er sprake is van passende bescherming bij de verwerking van persoonsgegevens en dat ook kunnen aantonen.

Tegelijk is het zo dat uiteindelijk alle medewerkers van de gemeente medeverantwoordelijk zijn voor de zorgvuldige omgang met persoonsgegevens.

Waarom dit privacy beleid?

Artikel 24 AVG stelt bestuursorganen tot de taak om passende maatregelen te nemen om personen te beschermen bij de verwerking van persoonsgegevens. In het tweede lid van dat artikel wordt gezegd dat een gemeente in dit verband over beleid dient te beschikken.
Dit beleid is van toepassing op de gehele gemeentelijke organisatie en daarmee alle bestuursorganen. Het is primair gericht aan alle medewerkers die in het kader van hun taak persoonsgegevens verwerken.

Naast de wettelijke plicht, is dit beleid een belangrijk onderdeel van het meerjarenplan AVG. Dit meerjarenplan heeft als doel om het volwassenheidsniveau te bereiken waar de wetgever vanuit gaat. Het beleid betreft een overkoepelend kader waarin de maatregelen tot bescherming van persoonsgegevens op algemene wijze zijn uitgewerkt. In werkplannen, procedures en werkinstructies wordt inhoudelijk uitgewerkt hoe uitvoering wordt gegeven aan de bescherming van persoonsgegevens.

Dit privacy beleid vervangt het in 2018 vastgestelde privacy beleid en –reglement 2018-2022. Een herijking van dit beleid is nodig om onder andere meer aandacht te vestigen op risico-gestuurd werken, de visie van het gemeentebestuur in het digitale tijdperk op te nemen en verbinding te maken met de planning & control-cyclus. Dit herziende privacy beleid is een eerste stap in de verdere implementatie van de AVG en volgt daarmee de aanbeveling van de Functionaris Gegevensbescherming op.

Evaluatie privacy beleid

Dit privacy beleid geldt voor de duur van vier jaar (2020-2024) en wordt op doeltreffendheid tweejaarlijks geëvalueerd. Dat zal zijn eind 2021 en eind 2023.

Proceseigenaren doen periodiek verslag binnen de gemeentelijke vastgestelde P&C cyclus over de naleving van dit beleid, waaronder oplossingen en incidenten die zich hebben voorgedaan.

Het college van B&W legt over de privacy beleidsvoering (politieke) verantwoording af aan de raad en is transparant over de verwerkingen van persoonsgegevens naar betrokkenen.
De gemeente Hilversum draagt zorg voor de documentatie van beleid en maatregelen, zodat het op ieder moment maatschappelijk en juridisch uitleg kan geven over de deugdelijkheid van de aanpak (aantoonbaarheid).

De Functionaris Gegevensbescherming (FG) doet jaarlijks rechtstreeks verslag aan het college en geeft aanbevelingen die strekken tot verdere optimalisering van de privacy beleidsvoering. Het college besluit over bijsturen van dit beleid met inachtneming van de aanbevelingen van de FG.

Procedures en formats

In onderliggende beleidsnotities dan wel reglementen is de bescherming van persoonsgegevens uitgewerkt die betrekking hebben op verwerkingen van medewerkers, bestuur en Raad. Daarnaast geldt dit ook voor verwerkingen waar sprake is van bijzondere of gevoelige persoonsgegevens. Bijvoorbeeld voor cameratoezicht, Smart City, de Hilversum Pas of de Persoonsgerichte aanpak.

Samenhang privacy beleid met informatiebeveiligingsbeleid

Bescherming van persoonsgegevens kan niet zonder informatiebeveiliging. Gegevensbescherming gaat over behoorlijk bestuur in het digitale tijdperk en is met name gericht op de bescherming van personen.

Informatiebeveiliging is een onderdeel van gegevensbescherming en is specifiek gericht op de beschikbaarheid, integriteit en vertrouwelijkheid (BIV) van de gemeentelijke informatievoorzieningen. In het informatiebeveiligingsbeleid[1] is opgenomen hoe de omgang met de drie BIV-principes is.

[1] Strategisch Gemeentelijk Informatiebeveiligingsbeleid Hilversum 2020-2024

2. Gemeentelijke organisatie

Het Privacy beleid van de gemeentelijke organisatie wordt opgesteld door het college van Burgemeesters en Wethouders (hierna: het college) en gecontroleerd door de gemeenteraad.

Gemeenteraad

De gemeenteraad ziet er op toe dat het college overkoepelend beleid ten aanzien van bescherming van persoonsgegevens voor de organisatie vaststelt. Door de gemeenteraad worden voor de uitvoering hiervan de benodigde middelen beschikbaar gesteld. Voorts controleert zij het college bij de uitvoering van deze kaders. Zij wordt hiertoe in staat gesteld door de verantwoordingsinformatie. Dit is onder meer het jaarlijkse verslag van de Functionaris Gegevensbescherming (FG), die het college verschaft.

College van B&W

Het college is integraal verantwoordelijk voor zorgvuldigheid van verwerking van persoonsgegevens. Zij is het meest aangewezen bestuursorgaan die de passende bescherming van persoonsgegevens waarborgt. Zo is zij verantwoordelijk voor een duidelijk te volgen privacy beleid, doet aan de gemeenteraad voorstellen over in te zetten middelen en stelt specifieke regelingen en procedures vast. Daarnaast controleert zij het management van de organisatieonderdelen op de maatregelen die verband houden met de bescherming van persoonsgegevens.

Het college heeft een portefeuillehouder aangewezen die namens het college de beleidsvoering waarborgt. Daarnaast legt deze (politieke) verantwoording af over de privacy beleidsvoering aan de Raad.

Aansturing: Gemeentesecretaris /directie

De uitvoeringsverantwoordelijkheid voor gegevensbescherming ligt bij de gemeentesecretaris. De gemeentesecretaris is de Algemeen directeur, de hoogste ambtenaar binnen de ambtelijke organisatie en de eerste adviseur aan het college. Hij of zij vormt dus de schakel tussen het bestuur en ambtelijke organisatie en is in dit kader ambtelijk verantwoordelijk.

De Algemeen directeur is samen met de directie verantwoordelijk voor de uitvoering van het meerjarenplan, een juiste uitvoering van privacy beleid en stuurt op (concern) risico's. Daarnaast zorgen zij voor een passend niveau van informatieveiligheid en gegevensbescherming binnen de organisatie.

Uitvoering: Lijnmanagers

De zorgvuldige omgang van verwerkingen vallen onder de lijnmanagers (proceseigenaar) binnen de verschillende vak-afdelingen. Dat betekent dat zij zelf moeten zorgdragen over het nakomen van de naleving van het privacy beleid binnen hun organisatieonderdeel (bijvoorbeeld burgerzaken, belastingen). Ook zijn zij verantwoordelijk voor voldoende bewustwording. Periodiek worden centraal bewustzijnscampagnes georganiseerd.

De lijnmanager stuurt onder meer aan op:

- risico-gestuurd werken. Hiervoor wordt gebruik gemaakt van de vastgestelde modellen van de DPIA-light en /of de 'schaal van erg' en/of Data Protection Impact Assessments (DPIA's).
- naleving van principes van privacy by design & default;
- het hanteren van daartoe vastgestelde procesplannen en formats, zoals de DPIA en de (door de VNG vastgestelde) verwerkersovereenkomst;

- dat datalekken volgens de daartoe te volgen procedure zo snel mogelijk bij de Privacy Officer of bij het Privacy & Informatieveiligheid Team (PIT) worden gemeld;
- het opnemen van nieuwe verwerkingen en gewijzigde verwerkingen in het register van verwerkingsactiviteiten;
- het informeren en het afhandelen van de rechten van de betrokkene;
- het maken van schriftelijke afspraken bij risicovolle verwerkingen en verwerkingen bij ketensamenwerking (verwerkingen in een samenwerkingsverband);
- het bijstaan van de uitvoering door professionals op het gebied van privacy en informatieveiligheid waar nodig;
- het bekend maken van dit beleid bij haar medewerkers (in samenwerking met het PIT).

Medewerkers

Alle medewerkers (inclusief inhuur/externen) zijn ervoor verantwoordelijk dat zorgvuldig wordt omgegaan met verwerking van persoonsgegevens. Dat betekent dat iedereen, binnen de kaders van zijn taak, zorgt voor een rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens. Indien er twijfel bestaat of aan deze beginselen uitvoering wordt gegeven, schakelt men de lijnmanager en het PIT in.

2.1 Ondersteuning en advies

Om de uitvoering te helpen bij vraagstukken die leven omtrent de bescherming van persoonsgegevens en de directie te ondersteunen bij de uitvoering van het meerjarenplan AVG, zijn de volgende professionals belast.

Privacy Officer (PO)

De Privacy Officer (PO) is specialist op de AVG en adviseert en ondersteunt vanuit de tweede-lijn bij vraagstukken omtrent de bescherming van persoonsgegevens. De PO stelt het meerjarenplan op en rapporteert jaarlijks aan de directie en wethouder Privacy op grond van deze plannen. Daarnaast coördineert de PO de uitvoering van het meerjarenplan, waar nodig in samenwerking met de FG. Tevens stelt de PO beleidsnotities en werkinstructies op en laat deze vaststellen door directie en /of wethouder Privacy. Gevraagd en ongevraagd adviseert de PO over activiteiten ter bescherming van persoonsgegevens.

Daarnaast is de PO de verbindende schakel tussen de organisatie en de FG.

Security Officer (SO)

De Security Officer is verantwoordelijk voor het vormgeven en bewaken van het informatiebeveiligingsbeleid. Daarnaast ondersteunt hij of zij bij het in kaart brengen van de risico's en adviseert welke maatregelen genomen moeten worden ter bescherming van persoonsgegevens.

Chief Information Security Officer (CISO)

In het kader van de privacy heeft de CISO een rol in ondersteuning en advies. Op het gebied van informatiebeveiliging heeft hij een controlerende en toezichthoudende rol. Informatiebeveiliging maakt een wezenlijk onderdeel uit van de bescherming van persoonsgegevens. Hij adviseert voornamelijk bij projecten en het beheersen van risico's.

Adviseur Informatie (AI)

De Adviseur Informatie is de kenner op het gebied van de gemeentelijke producten, informatiestromen, processen en informatiesystemen. Hij is de spin in het web en adviseert op vraagstukken die betrekking hebben op de bescherming van persoonsgegevens.

Privacy en Informatieveiligheid Team (PIT)

De organisatie wordt waar nodig ondersteund door het Privacy en Informatieveiligheid Team (PIT). Dit team bestaat uit een vast kernteam van professionals, waaronder de hierboven beschreven functionarissen, eventueel aangevuld met de FG. Periodiek overlegt dit vaste kernteam en op afroepbasis aangevuld met professionals uit cruciale domeinen. Hiervoor is het van belang dat de betreffende professional affiniteit met de AVG heeft en kennis heeft van sector specifieke wetgeving. Deze professionals spelen een belangrijke rol in de ondersteuning op de uitvoering en geven zo veel mogelijk eerstelijnsadvies.

Juridische Zaken

Indien er sprake is van complexe privacyvraagstukken kan juridische ondersteuning noodzakelijk zijn. Bijvoorbeeld bij de afhandeling van complexe inzageverzoeken of bij datalekken waar schade is ontstaan en waar juridische vertegenwoordiging in rechterlijke procedures nodig is.

2.2 Toezicht en controle

Om het beleid binnen de gemeentelijke organisatie te borgen, is het van belang dat hier toezicht en controle op plaatsvindt. Dit is als volgt geregeld.

Functionaris Gegevensbescherming

De Functionaris voor Gegevensbescherming (FG) is de onafhankelijke toezichthouder op de naleving van de AVG, gerelateerde wetgeving en het gemeentelijke beleid op het gebied van gegevensbescherming conform artikel 37-39 AVG. Het college informeert over de contactgegevens van de FG en communiceert zijn contactgegevens aan de Autoriteit Persoonsgegevens (AP).

De FG:

- informeert en adviseert onze organisatie over de werking van de AVG, overige wetgeving en ons beleid;
- houdt toezicht op de nakoming van het privacy beleid en achterliggende wettelijke verplichtingen;
- helpt privacy-klachten tot een goed einde te brengen (ombudsfunctie);
- adviseert bij privacy-incidenten over ernst en omvang;
- ziet toe op het beheer van het register van verwerkingen conform artikel 30 AVG;
- controleert de naleving van afspraken door onszelf en ketenpartners, eventueel ook in samenwerking met auditors;
- helpt het privacy beleid uit te dragen en bewustzijn te creëren bij interne en externe doelgroepen;
- is het contactpunt voor landelijke toezichthouders – met name de AP.

De FG krijgt goede ruimte voor professionele uitvoering van taken. Dat betekent dat de FG:

- naar behoren en tijdig wordt betrokken bij aangelegenheden die betrekking hebben op de verwerking van persoonsgegevens.
- volledig wordt geïnformeerd over aspecten van onze bedrijfsvoering waarbij persoonsgegevens worden verwerkt of wanneer daartoe voornemens bestaan.

Het college, directie en proceseigenaren ondersteunen de FG door hem op zijn verzoek toegang te geven tot de verwerking van persoonsgegevens en hem de middelen te bieden voor professioneel onderzoek.

De FG wordt niet geïnstrueerd over invulling van taken, onder druk gezet, gestraft, ontslagen of beperkt in de middelen die hij nodig heeft voor de uitvoering van zijn taak. De zienswijze van de FG is zwaarwegend en geldt als de geëigende wijze voor naleving van de AVG.

Minimaal één keer per jaar brengt de FG verslag uit over de stand van zaken aan het college in het kader van de planning & control-cyclus.

Businesscontroller

De businesscontroller rapporteert aan de directie over naleving van wet- en regelgeving en het privacy beleid, richtlijnen en processen. Daarnaast heeft de businesscontroller een belangrijke signaalfunctie om te kijken wat er speelt op het gebied van gegevensbescherming op de werkvloer, schakelt met het PIT en indien nodig met de FG. Dit om de uitvoeringsverantwoordelijkheid binnen de gemeentelijke organisatie te waarborgen.

Verhouding tot en verantwoording aan de Raad

De gemeenteraad controleert vervolgens het college door middel van de verantwoordingsrapportages. Jaarlijks legt het college verantwoording af aan de gemeenteraad over de realisatie en de toepassing van het privacy beleid in relatie tot informatiebeveiligingsbeleid, via de paragraaf bedrijfsvoering in de jaarstukken.

In de verantwoording in de jaarstukken komen in elk geval de volgende onderwerpen aan de orde:

- realisatie en uitvoering privacy beleid en integratie wettelijke eisen AVG in de werkprocessen;
- inventarisatie en implementatie per afdeling van de risico-inventarisatie (afgenomen DPIA's),
- stand van zaken met betrekking tot het verwerkingsregister, conform artikel 30 AVG;
- activiteiten die hebben plaatsgevonden op bewustwording en training;
- aard, omvang en afhandeling van eventuele klachten van de betrokkene;
- aard, omvang en afhandeling van (vermoedelijke) datalekken.

Bijlage 1 Toelichting bepalingen AVG

Belangrijke begrippen

Betrokkene: een natuurlijk persoon op wie de persoonsgegevens betrekking heeft. Dit zal in de gemeentelijke context veelal de inwoner of een medewerker van de gemeente Hilversum zijn. Maar ook een bezoeker kan een betrokkene zijn waar persoonsgegevens over worden verwerkt.

PIT: Privacy en Informatieveiligheid Team.

Data Protection Impact Assessment (DPIA): beoordeelt de effecten en risico's van een nieuwe of bestaande gegevensverwerking op de bescherming van de persoonsgegevens.

Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. Dit betekent dat informatie ofwel direct over iemand gaat, ofwel naar deze persoon te herleiden is. Gegevens van overleden personen of van organisaties zijn geen persoonsgegevens volgens de AVG. In sommige gevallen kan het zijn dat een enkel gegeven geen persoonsgegeven is, maar door deze te combineren met andere gegevens dat dan wel weer is. Bijvoorbeeld een postcode in combinatie met een huisnummer.

Persoonsgegevens zijn bijvoorbeeld:

- Naam, adres, woonplaats (NAW)
- Geboortedatum –plaats
- Geslacht
- Contactgegevens; emailadres, telefoonnummer
- BSN

Bijzondere persoonsgegevens: Bijzondere persoonsgegevens zijn door hun aard bijzonder gevoelig en worden met de AVG extra beschermd en zijn in principe verboden om te verwerken. Dit zijn persoonsgegeven die betrekking hebben op ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, lidmaatschap van een vakvereniging, de gezondheid, iemands seksueel gedrag of seksuele gerichtheid, genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon.

Voor strafrechtelijke persoonsgegevens gelden onder de AVG specifieke eisen.

Privacyverklaring: een verklaring dat is bedoeld voor de betrokkene en tot doel heeft de betrokkene te informeren wat er met zijn gegevens gebeurt en waarom.

Privacy by design: tijdens de ontwikkelingen van producten /diensten wordt aandacht besteed aan privacy verhogende maatregelen.

Privacy by default: de gemeente treft technische en organisatorische maatregelen om alleen persoonsgegevens te verwerken die noodzakelijk zijn voor het specifieke doel.

Proceseigenaar: lijnmanager verantwoordelijke voor de uitvoering van de taken, processen en levering van producten binnen zijn afdeling /team.

Verwerking: alles wat je met een persoonsgegeven doet, zoals verzamelen, vastleggen, bewaren, vernietigen, verstrekken aan een ander, bij elkaar voegen, etc.

Verwerker: Een verwerker is een externe organisatie die in opdracht van de verwerkingsverantwoordelijke persoonsgegevens verwerkt, zoals de salarisadministratie of

clouddienst voor indicatiestellingen in de jeugdzorg of de Hilversum Monitor. Een ingehuurd schoonmaakbedrijf is dat bijvoorbeeld niet.
De dienstverlening moet gericht zijn op het verwerken van persoonsgegevens ten behoeve van de gemeente Hilversum. De verwerker staat nooit onder het rechtstreekse gezag van één van de bestuursorganen, heeft nooit zeggenschap over de gegevens (hij mag bijvoorbeeld niet de bewaartermijnen bepalen) en mag alleen handelen onder de schriftelijke instructies van de gemeente Hilversum, bijvoorbeeld als dat in een verwerkersovereenkomst is bepaald. [2]

Verwerkersovereenkomst: Een verwerker heeft een aantal afgeleide verplichtingen, voor onder meer beveiliging en geheimhouding van de gegevens. Bij het inschakelen van een verwerker worden schriftelijke afspraken gemaakt over hoe om te gaan met de persoonsgegevens en informatieveiligheid. In de praktijk wordt gesproken van een zogenoemde verwerkersovereenkomst. Door VNG realisatie is een standaard model verwerkersovereenkomst voor gemeenten opgesteld, die vanaf 2020 (verplicht) door alle gemeenten wordt gebruikt. Deze overeenkomst is afgestemd op de, eveneens door de VNG opgestelde, Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT).

Waar deze verwerkersovereenkomst ontoereikend is, wordt gebruik gemaakt van het oudere model van de VNG.

Indien één van de bestuursorganen, als verwerker optreedt, dan dient Hilversum zelf deze verplichtingen op te volgen.

Verwerkingsverantwoordelijke: een persoon of instantie die alleen of samen met een ander het doel en de middelen voor de verwerking van persoonsgegevens vaststelt. Dat is in de gemeentelijke organisatie een bestuursorgaan, zoals het College van B&W, de Burgemeester, de gemeenteraad of de Commissie Bezwaar en Beroep. Zie verder ook onder het eerste deel van dit beleid.

Doeleinden verwerking (artikel 5, lid 1, onder b, AVG)

De gemeente Hilversum voert het beleid dat persoonsgegevens alleen verzameld worden voor een doel dat vooraf is vastgesteld is. Dat doel mag dus niet gaandeweg de gegevensverzameling worden bepaald. Dat doel moet specifiek en rechtvaardig zijn. In sommige gevallen is dat vastgelegd per wet. Zo staan er doelen en bijbehorende verwerkingen van persoonsgegevens beschreven in onder andere de Jeugdwet of Participatiewet.

Rechtmatige grondslag (artikel 6 AVG)

Bij het verwerken van persoonsgegevens dient dit altijd noodzakelijk te zijn en gebaseerd te worden op een rechtmatige grondslag. De verwerking kan gebaseerd worden op:

- Algemeen belang / openbaar gezag;
- Wettelijke verplichting;
- Vitaal belang;
- Overeenkomst;
- Ander gerechtvaardigd belang;
- Toestemming (enkel vereist als geen andere grondslag van toepassing is).

De verwerking van *bijzondere persoonsgegevens* is in principe verboden, tenzij er een beroep kan worden gedaan op één van de uitzonderingsgronden die genoemd zijn in de Uitvoeringswet AVG, naast het hebben van één van bovengenoemde grondslagen.

[2] Zie voor meer informatie: Factsheet beslismodel verwerker - verwerkingsverantwoordelijke van de Informatie BeveiligingsDienst (IBD).

Grondslagen gemeentelijke organisatie

Verwerkingen binnen de gemeentelijke organisatie kunnen gebaseerd zijn op één van onderstaande grondslagen:

- Persoonsgegevens die *noodzakelijk* zijn om een *wettelijke verplichting* na te komen. Bijvoorbeeld bij de aanvraag om een bijstandsuitkering, dan bepaalt artikel 53a en 64 Participatiewet voor welk doel welke gegevens nodig zijn.
- Persoonsgegevens die *noodzakelijk* zijn om een *taak van algemeen belang* uit te voeren, ook wel de *uitoefening van de publiekrechtelijke taak* genoemd. Bijvoorbeeld de wet Schuldhulpverlening bepaalt dat de gemeente een taak heeft in de uitvoering van de schuldhulp.

Dat betekent dat telkens uit de wet moet blijken dat de gemeente een taak heeft om een bepaald doel te realiseren. Bijvoorbeeld uit de omgevingswet om een bouwvergunning te realiseren, of de gemeentewet waarin het cameratoezicht is bepaald.

Indien de gemeente Hilversum als **werkgever** optreedt dan kunnen de volgende grondslagen gelden:

- Persoonsgegevens die *noodzakelijk* zijn voor de uitvoering van een overeenkomst, bijvoorbeeld bij de inhuur van een externe medewerker.
- Persoonsgegevens die *noodzakelijk* zijn ten behoeve van het *gerechtvaardigd belang* die de gemeente Hilversum als werkgever heeft, bijvoorbeeld het inzichtelijk maken van het rooster van de BHV'ers om bedrijfshulpverlening zo effectief mogelijk in te zetten.

Let op: het *gerechtvaardigd belang* is alleen van toepassing daar waar privaatrechtelijke wordt gehandeld. Bijvoorbeeld in het kader van de uitoefening van de gemeente als werkgever of wanneer dat noodzakelijk is voor de bedrijfsvoering, bijvoorbeeld bij een medewerkers onderzoek of de beveiliging van de gemeentelijke gebouwen door middel van cameratoezicht. Hiervoor geldt dat telkens een zorgvuldige belangenafweging moet worden gemaakt. Het belang van de gemeentelijke organisatie moet zwaarder wegen dan de rechten en vrijheden van de medewerker. In deze belangenafweging speelt de gevoeligheid van gegevens een rol. Als er sterkere beveiligingsmaatregelen zijn getroffen, kan de verwerking eerder gebaseerd worden op deze grondslag.

Toestemming

Vanwege de afhankelijkheidsrelatie die de betrokkene met de gemeentelijke organisatie heeft, is toestemming meestal niet geschikt. Van vrije toestemming zal over het algemeen geen sprake kunnen zijn, omdat burgers afhankelijk zijn van de gemeente voor hulp of ondersteuning.

Bij het verstrekken van een nieuwsbrief is toestemming wel een aangewezen grondslag.

Bij toestemming moet er voldoende informatie gegeven worden: toegankelijk, in duidelijke en eenvoudige taal. De betrokkene moet immers snappen waar hij precies toestemming voor geeft. Toestemming kan te allen tijde worden ingetrokken en dit dient net zo gemakkelijk te zijn als het geven van de toestemming. Opt-out is dus niet toegestaan. Dat wil zeggen dat het vinkje om toestemming te geven niet van te voren al aangekruist mag zijn. Alleen een actieve handeling om de toestemming aan te vinken is toegestaan, opt-in genoemd.

De toestemming dient te zijn vastgelegd in het daartoe vastgestelde format van de gemeente Hilversum.

Vitaal belang

Het *vitale belang* kan alleen worden toegepast in geval van acute dringende hulp. Bijvoorbeeld in de situatie dat een hulpverlener persoonsgegevens moet verwerken om acuut dringende medische hulp aan de betrokkene te verlenen, bijvoorbeeld omdat iemand buiten bewustzijn is. Deze grondslag zal binnen de gemeentelijke organisatie dan ook niet snel van toepassing zijn.

Verdere verwerking (doelbinding, artikel 6, lid 4, AVG)

Persoonsgegevens mogen niet zomaar voor andere doeleinden verder worden verwerkt. Zo mogen de gegevens die door de ene afdeling zijn verzameld niet zonder meer aan een andere afdeling worden verstrekt. Het verdere gebruik van gegevens mag alleen als dat bij wet is bepaald. Indien dat niet het geval is zal in ieder geval moeten worden bepaald wat:

- het verband tussen het bestaande doel en de voorgenomen verdere verwerking is;
- de context is waarin de gegevens zijn verzameld en de verhouding tussen de betrokkene en de verwerkingsverantwoordelijke;
- de aard van de gegevens zijn; voornamelijk of sprake is van bijzondere of strafrechtrechtelijke gegevens.
- de mogelijke gevolgen voor de betrokkene zijn;
- het bestaan van passende waarborgen zijn, zoals pseudonimiseren.

Ketensamenwerking (artikel 26 AVG)

Wanneer de verwerkingsverantwoordelijke samen met anderen doel en middelen bepaalt, bijvoorbeeld in een samenwerkingsverband, dan kan sprake zijn van *gezamenlijke verantwoordelijkheid.* Bij elk samenwerkingsverband dient op basis van de eigen doelen, de samenstelling van de partners en de taken op basis waarvan zij samenwerken te worden gekeken naar de wettelijke grondslag en het doel van het verstrekken van informatie.

Voor individuele casussen (dus geen beleidsmatige taak) kan alleen een bestuursorgaan deelnemen vanuit een specifieke wettelijke taak. De persoonsgegevens die zij in een verband met een dergelijke taak verkrijgt, mogen niet zomaar voor andere doeleneinden worden gebruikt, tenzij de wet dat uitdrukkelijk toestaat. Voor gegevensuitwisseling op persoonsgerichte aanpak bij complexe problematiek is vanuit de VNG een handvat uitgebracht. Zie voor meer informatie over het Handvat gegevensuitwisseling zorg en veiligheid (maart 2019).

In het geval van ketensamenwerking moeten de partijen onderling duidelijke afspraken maken over wie invulling geeft aan de diverse rechten en plichten uit de AVG. Het is in het bijzonder van belang dat de betrokkene weet waar hij terecht kan om zijn rechten uit te oefenen.

Indien sprake is van gezamenlijke verantwoordelijkheid, dan dienen afspraken conform artikel 26 AVG schriftelijk te worden vastgelegd en aan de betrokkene beschikbaar worden gesteld, bijvoorbeeld door middel van publicatie op de website van alle betrokken partijen.

Bij onduidelijkheden of complexe verhoudingen tussen de verwerkingsverantwoordelijke en de derde partij onder de AVG dient altijd contact gezocht te worden met de Privacy Officer, zodat bekeken kan worden welke afspraken eventueel gemaakt moeten worden.

Register van verwerkingen (artikel 30 AVG)

De gemeente Hilversum vindt het belangrijk dat er een integraal overzicht bestaat op de informatiehuishouding en de getroffen beheersmaatregelen. Hiermee komt zij de wettelijke eis van de registerplicht na. Tevens kan hiermee op ieder moment worden aangetoond hoe aan de verplichtingen van de AVG wordt voldaan. Hiervoor wordt een actueel elektronisch register van verwerkingsactiviteiten bijgehouden.

Wijzigingen en gestaakte verwerkingen worden met het oog op de bewijslast gearchiveerd.

De FG heeft toegang tot het register. Hiermee kan hij zijn taak vervullen rondom het toezicht op naleving op de AVG en de organisatie informeren en adviseren over de gegevensverwerkingen die plaatsvinden. Wanneer de Autoriteit Persoonsgegevens daarom vraagt, stelt het college het register ter beschikking.

Het bijhouden van het register van verwerkingsactiviteiten zal plaatsvinden volgens de daartoe aangewezen procedure.

Datalekken (artikel 33 en 34 AVG)

Een beveiligingsincident kan leiden tot een datalek. In dat geval is sprake van een onrechtmatige verwerking van persoonsgegevens die heeft plaatsgevonden. Hierbij zijn beveiligingsmaatregelen (on)bewust omzeild of doorbroken of er zijn geen voldoende beveiligingsmaatregelen getroffen. Het gaat ook om situaties waarbij persoonsgegevens verloren zijn gaan, waardoor ze niet meer beschikbaar zijn en om situaties waarin gegevens in handen kunnen komen of zijn gekomen van derden die geen toegang tot die gegevens mogen hebben.

Als sprake is van een aanzienlijke kans op ernstige nadelige gevolgen voor betrokkene, dan wel ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, geldt dat dit datalek binnen 72 uur gemeld moet worden bij de Autoriteit Persoonsgegevens (AP). Als dit later dan 72 uur plaatsvindt, wordt er een motivering voor de vertraging bij de melding gevoegd.

Indien het datalek grote gevolgen kan hebben voor de betrokkene, bijvoorbeeld identiteitsfraude, informeert de verwerkingsverantwoordelijke de betrokkene in eenvoudige en heldere taal. Veelal voert het PIT, indien nodig in overleg met de FG, de afhandeling van de datalekken uit. Alle meldingen, en wijze van afhandeling, worden in een register bijgehouden.

De melden van beveiligingsincidenten zal plaatsvinden volgens de procedure datalekken.

Data Protection Impact Assessment (DPIA) (artikel 35 AVG)

De AVG draagt op tot het nemen van passende maatregelen. Hiervoor wordt gebruikt gemaakt van een DPIA als risico-inventarisatie. Op grond van de vastgestelde risico's worden maatregelen genomen. Een DPIA moet altijd worden gedaan voor de start van een geautomatiseerde verwerking, bijvoorbeeld cameratoezicht. Bij een grootschalige verwerking of wanneer er een grootschalige monitoring van openbare ruimten wordt beoogd, geldt ook een DPIA, bijvoorbeeld bij Smart City toepassingen.

DPIA's moeten ook worden uitgevoerd bij al bestaande verwerkingen waarbij:

- een hoog risico geldt, bijvoorbeeld processen binnen het sociaal domein en openbare orde en veiligheid.
- nieuwe technologieën worden toegepast of wijziging van doel aan de orde is.
- de context van de verwerking verandert, bijvoorbeeld door maatschappelijke veranderingen.
- bij organisatorische veranderingen die van invloed zijn op de verwerking.

Op alle bestaande verwerkingen wordt een DPIA-light uitgevoerd om in beeld te krijgen welke risicovolle verwerkingen er binnen de gemeente aanwezig zijn. Hiervoor kan altijd om advies worden gevraagd van de Privacy Officer dan wel PIT.

De resultaten van de DPIA in de hogere risicocategorieën worden aan de FG voorgelegd.

Indien de proceseigenaar niet of onvoldoende maatregelen treft zoals deze blijken uit de DPIA en hierdoor hoge risico's resteren voor personen, wordt hiervan melding gemaakt aan de AP. De FG kan hiertoe nadrukkelijk adviseren en bij niet-opvolging van dit advies, besluiten om zelfstandig signaal af te geven aan de AP.

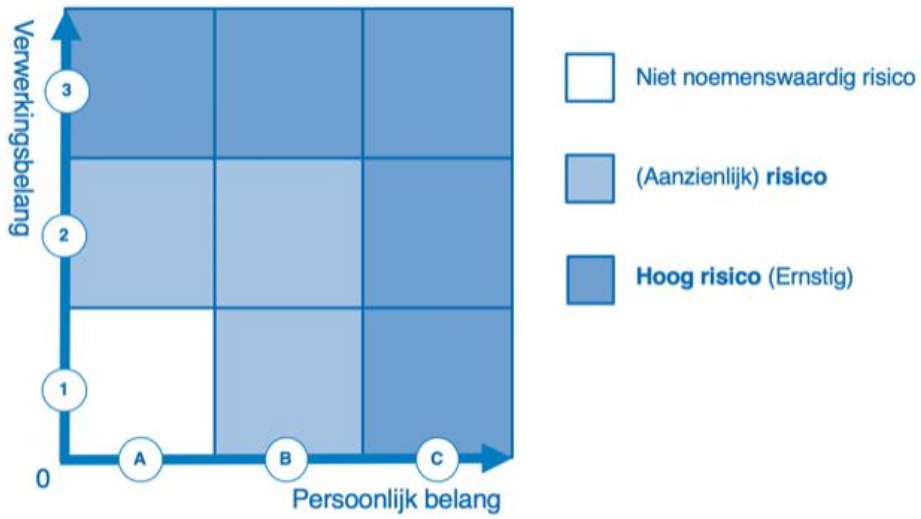
Door de Informatiebeveiligingsdienst (IBD) van de VNG is een gestandaardiseerde procedure beschikbaar voor de uitvoering van de DPIA. Hilversum sluit aan bij het gebruik van dit DPIA proces.

Het afnemen van een DPIA zal plaatsvinden volgens de procedure DPIA.

Risicomatrix (schaal van erg)

Met behulp van de risicomatrix stel je de risicoscore vast voor betrokkenen (de persoon op wie de gegevens betrekking hebben) en voor de organisatie. Het risico wordt gevonden door zowel de kans en de impact van bepaalde negatieve gevolgen van fouten te beoordelen. Een grote kans op een kleine impact kan dus resulteren in een risico met score *'midden'.* Tegelijk kan een zeer kleine kans op een hoog risico ook resulteren in score *'midden'*.

Maak de risico-inschatting bij voorkeur met medewerkers die nauw bij het nieuwe project, de beleidsontwikkeling of het proces betrokken zijn. Daarnaast is deze risicomatrix te gebruiken bij datalekken.



Op de horizontale as staat het risico voor de persoon van wie of over wie de gegevens worden verwerkt op het moment dat er fouten worden gemaakt. Daarbij is de volgende grove indeling:

A. Risico *laag:* lichte problemen, 'irritant'. Denk aan een vraag vanuit de gemeente die voor de tweede keer aan iemand gesteld moet worden, of een telefoonnotitie die voor een collega niet duidelijk is.
B. Risico *midden:* substantieel/ vervelend, vaak is deze schade door fouten te herstellen, soms niet. Denk aan het verwarren van dossiers met een verkeerde aanschrijving tot gevolg, of het zonder goed te informeren doorgeven van gegevens.
C. Risico *hoog*: ernstige problemen, onder meer ernstige reputatieschade en stigmatisering, verlies van vermogen om geld te verdienen, vrijheidsberoving, gevaar voor gezondheid. Denk aan een onterechte afkeuring van cruciale sociale regelingen, of het openbaar worden van aan persoonsgegevens met betrekking tot (verdenking van) huiselijk geweld.

Op de verticale as staat de impact voor gemeente Hilversum (organisatie-risico) als er in het proces fouten zijn gemaakt:

1. Risico *laag:* denk aan extra benodigde administratieve handelingen voor medewerkers.
2. Risico *midden:* denk aan discussies met gemeenteraad en andere stakeholders, onderzoek door Autoriteit Persoonsgegevens, showstopper.
3. Risico *hoog:* denk aan vertrouwensschade (maatschappelijke onrust, verlies in de democratische rechtstaat), boetes opgelegd door de AP, ontslag ambtenaren of politici omwille van onrechtmatige gegevensverwerking.

Informeren (artikel 13 en 14 AVG)

De gemeente is open en transparant over hoe zij met persoonsgegevens omgaat. Dat stelt namelijk de betrokkene in staat om zijn rechten uit te kunnen oefenen.

Wanneer de gemeente persoonsgegevens over personen verwerkt, heeft zij de plicht de betrokkenen hierover te informeren. De betrokkenen dienen in de meeste gevallen al voordat de verwerkingen begonnen zijn, op de hoogte te zijn van de manier waarop de gemeente met persoonsgegevens omgaat. Hiertoe dienen de algemene en specifieke privacy verklaringen. Deze worden gepubliceerd op de website.

Indien de gemeente een externe organisatie wil inschakelen om een dienst aan de inwoner te verlenen, zal altijd om het meest recente privacyverklaring en privacy beleid worden gevraagd.

Rechten betrokkene (artikel 12 en 15-22 AVG)

Om een eerlijke verwerking van persoonsgegevens te waarborgen heeft de betrokkene diverse rechten:

- Recht op inzage
- Recht op correctie als de gegevens niet kloppen
- Recht op verwijdering van de gegevens als de gegevens niet langer nodig zijn.
- Recht om ‘vergeten te worden’. In het geval waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen.
- Recht op beperking en recht op bezwaar
- Recht om niet onderworpen te worden aan geautomatiseerde besluitvorming.
- Recht op contact met de Functionaris Gegevensbescherming
- Recht om een klacht in te dienen bij de nationale toezichthouder, de Autoriteit Persoonsgegevens.

Het afhandelen van de rechten van de betrokkene zal plaatsvinden volgens de daartoe aangewezen procedure.

Doorgifte (artikel 44-49 AVG)

Doorgifte buiten de EER is alleen mogelijk wanneer de Europese Commissie heeft besloten dat het gegevensbeschermingsniveau in dat andere land adequaat is. Wanneer daar geen sprake van is, dan is verstrekking mogelijk op grond van bijvoorbeeld standaard contractbepalingen of kan het gelegitimeerd worden door bindende bedrijfsvoorschriften. Bij doorgifte moet in alle gevallen voldaan worden aan de vereisten uit de AVG. Indien een (sub)verwerker buiten de EER gevestigd is, moet er dus voldaan worden aan de eisen van doorgifte.