Hoogheemraadschap van
Schieland en de Krimpenerwaard

Nota
Privacybeleid

Privacybeleid Hoogheemraadschap van Schieland en de Krimpenerwaard

Beleidsregels van de Algemene Verordening Gegevensbescherming (AVG)

Colofon

Auteurs	Nalinie Somar (Bestuur, Informatie en Juridisch Advies)
Status	Definitief, versie 1.0
Taakveld	Privacywetgeving, Juridisch
Kwalificatie conform Beleidshuis	Beleidsuitwerking
D&H-besluitdatum	22 mei 2018
Datum inwerkingtreding	25 mei 2018
Afdeling	Bestuur, Informatie en Juridisch Advies
Registratienummer	2018.05586

Inhoudsopgave

1 Waarom beleid en voor wie?
1.1 Relatie Informatiebeveiligingsbeleid – Privacybeleid
1.2 Leeswijzer

2 Belangrijkste definities en maatregelen uit de verordening verklaard
2.1 Wat zijn persoonsgegevens?
2.2 Wanneer worden persoonsgegevens “verwerkt”?
2.2.1 Verwerkingenregister
2.3 De betrokkene
2.4 De verwerkingsverantwoordelijke
2.5 De verwerker
2.6 De verwerkersovereenkomst
2.7 Privacy-principes
2.8 Voorwaarden (grondslagen) voor verwerken
2.9 Privacy by design
2.10 Privacy by default

3 Data Protection Impact Assessment (risicoanalyse)
3.1 DPIA bij verwerkingen
3.2 DPIA bij veranderingen

4 Rechten van betrokken
4.1 De verschillende rechten van betrokkenen
4.2 Privacy-verzoeken van betrokkenen
4.3 Rechtsbescherming

5 Protocol “Meldplicht Datalekken” en Incident Response Team
6.1 Wat is een datalek?
6.2 Protocol “Meldplicht Datalekken”
6.3 Incident Response Team

Bijlage A: Checklist voor het werken met persoonsgegevens

1. Waarom beleid en voor wie?

Het hoogheemraadschap van Schieland en de Krimperwaard (hierna ‘HHSK’) spant zich in om de privacybescherming voor burgers en medewerkers te verbeteren. We willen laten zien dat we, als het gaat om de bescherming van persoonsgegevens, “in control” zijn conform de Algemene Verordening Gegevensbescherming (AVG). Deze Europese wetgeving op het gebied van privacy is per 25 mei 2018 in werking is getreden. Die wet heeft op die datum de Wet Bescherming Persoonsgegevens (WBP) vervangen en daardoor geldt nu in heel Europa dezelfde wetgeving.

Omdat HHSK vaak bijzondere en/of gevoelige persoonsgegevens verwerkt, is HHSK verplicht om een gegevensbeschermingsbeleid te hebben. Daarnaast moet HHSK - door het hanteren van gegevensbeschermingsbeleid (kortweg: ‘privacybeleid’) voldoen aan de verplichting uit de AVG om aan te tonen dat wij de zogenaamde verantwoordingsplicht in acht nemen. Verder kan dit privacybeleid er aan bijdragen dat besluiten op grond van de AVG binnen HHSK op een eenduidige manier worden genomen, en dat ook de procedures eenduidig zijn.

HHSK wil daarnaast transparant zijn richting de burger en deze adequaat informeren. Omgevingsgerichtheid staat hierbij centraal. De burger moet er op kunnen vertrouwen dat HHSK zorgvuldig en veilig met de persoonsgegevens omgaat. Het is van belang dat de burger op eenvoudige wijze toegang krijgt tot het gevoerde privacybeleid, aangezien van deze zelfde burger allerlei persoonsgegevens worden verwerkt. Dit beleid wil daar in voorzien.

De AVG verplicht HHSK om steeds te kijken of het beleid nog voldoet en of het aangepast moet worden. Technologische en maatschappelijke ontwikkelingen volgen elkaar snel op. Dit kan reden zijn om het beleid aan te passen. Omdat daarnaast nog niet geheel duidelijk is hoe de toezichthouder, de Autoriteit Persoonsgegevens zijn taak zal opvatten, is het daarom noodzakelijk om het privacybeleid periodiek - in ieder geval éénmaal per jaar - te evalueren. Er is immers sprake van nieuwe wetgeving, die volop in beweging is.

Dit beleid is van toepassing op de gehele organisatie, alle processen, onderdelen, objecten en gegevensverzamelingen van HHSK.

1.1 Relatie informatiebeveiligingsbeleid - Privacybeleid

Informatiebeveiligingsbeleid en privacybeleid zijn termen die soms door elkaar worden gebruikt. Informatiebeveiliging en privacybescherming zijn echter niet hetzelfde. Ze hebben een gemeenschappelijk raakvlak, en beiden ook een eigen domein daarbuiten.

Een goed informatiebeveiligingsbeleid is een voorwaarde voor de privacyregelgeving, en dat wordt ook zo benoemd in de AVG. Dan gaat het met name om de verwerking van persoonsgegevens. Ieder datalek is ook een (informatie)beveiligingsincident.

Informatiebeveiliging heeft echter een veel bredere scope dan alleen persoonsgegevens. Het gaat om de bescherming van alle data tegen aantasting van integriteit, vertrouwelijkheid en beschikbaarheid.

Privacybescherming gaat niet alleen over de beveiliging van persoonsgegevens tegen inbreuken, maar ook om het beperken van het verzamelen en gebruiken van persoonsgegevens tot het minimaal noodzakelijke.

1.2 Leeswijzer

In hoofdstuk 2 wordt beschreven wat persoonsgegevens zijn en welke maatregelen wij allemaal treffen of getroffen hebben om te kunnen voldoen aan de verantwoordingsplicht van HHSK. In de daarop volgende hoofdstukken leggen we uit aan de hand van welke principes dat gebeurt en van welke rechten burgers en medewerkers gebruik kunnen maken. In hoofdstuk 6 wordt de meldplicht datalekken behandeld.

Deze beleidsnota is te beschouwen als een levend document, dat regelmatig aangevuld en/of gewijzigd zal worden.

2. Belangrijkste definities en maatregelen uit de verordening verklaard

2.1 Wat zijn persoonsgegevens?

Een persoonsgegeven is een essentieel begrip in de AVG. Onder een persoonsgegeven wordt verstaan: '*elk gegeven over een geïdentificeerd of identificeerbaar natuurlijk persoon'*. Dit betekent dat de informatie direct over een persoon gaat of naar een bepaald persoon te herleiden is. Gegevens van overleden personen of organisaties zijn geen persoonsgegevens.,

In Tabel 1 worden verschillende soorten persoonsgegevens met een aantal voorbeelden weergegeven.

Soort persoonsgegevens	***Voorbeeld***
Geen persoonsgegevens	*- Bedrijfsnaam en adres* *- Vervuilingswaarde eenheden per huishouden*
Persoonsgegevens	*- Naam, adres en woonplaats* *- IP-adres* *- Geboortedatum*
Bijzondere/ gevoelige persoonsgegevens	*- Personeelsdossier* *- Kopie paspoort* *- Financiële gegevens* *- Telefoongegevens* *- Ras of etnische afkomst* *- IBAN* *- Strafrechtelijke gegevens* *- Genetische en biometrische gegevens* *- Politieke voorkeur* *- Digitale kaartgegevens*

Ook al wordt het onder de AVG geen bijzonder persoonsgegeven genoemd, voor het Burgerservicenummer (BSN) blijft gelden dat het enkel gebruikt mag worden wanneer het door de wet is voorgeschreven, en enkel voor die doeleinden gebruikt mag worden die die wet bepaalt. Nederland gaat hier dus verder dan de AVG, en heeft gebruik gemaakt van de beleidsvrijheid die de AVG biedt.

Tabel 1 - Overzicht persoonsgegevens

2.2 Wanneer worden persoonsgegevens "verwerkt"?

Het verwerken van persoonsgegevens is binnen de AVG ruim omschreven en omvat elke handeling vanaf het raadplegen en verzamelen tot aan het vernietigen van persoonsgegevens. Het maakt daarbij niet uit of deze persoonsgegevens in een computersysteem zijn opgeslagen, op papier zijn afgedrukt, op een USB-stick staan of via e-mail worden verzonden. Het bekijken van een persoonsgegeven valt al onder het begrip "verwerken".

> ***Definitie "verwerking":***
>
> *Een bewerking of een geheel van bewerkingen met betrekking tot persoonsgegevens of een geheel van persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens;*
>
> *Artikel 4, Algemene Verordening Gegevensbescherming*

Om persoonsgegevens te mogen verwerken, moeten we voldoen aan de in de AVG genoemde eisen. Deze eisen zijn terug te brengen tot een aantal principes. Deze moeten in acht genomen worden bij het verwerken van persoonsgegevens. De principes worden in paragraaf 2.7 verder uitgewerkt.

Er is voor het verwerken van persoonsgegevens een leidraad beschikbaar in **Bijlage A: Checklist voor het werken met persoonsgegevens**. Deze kan in geval van twijfel bij iedere (intentie tot) verwerking weer worden geraadpleegd.

2.2.1 Verwerkingenregister

Alle verwerkingen van persoonsgegevens worden per werkproces geregistreerd en bijgehouden in een verwerkingenregister. HHSK is verplicht verantwoording af te leggen over alle gegevensverwerkingen wanneer de Autoriteit Persoonsgegevens daar om vraagt. Om te kunnen voldoen aan deze verantwoordingsplicht vereist de AVG dat HHSK een register bijhoudt van alle verwerkingen binnen de organisatie. Hierin moet ook staan welk doel en welke grondslag voor de verwerkingen worden gebruikt en wie verantwoordelijk is voor het proces waarbinnen de verwerking plaatsvindt. Daarnaast moet het register vermelden hoe lang de gegevens bewaard blijven. Dit register zal, eenmaal ingevuld, jaarlijks worden geëvalueerd op initiatief van de Functionaris Gegevensbescherming (hierna: "FG") en worden bijgehouden.

2.3 De betrokkene

De betrokkene is de persoon van wie het betreffende persoonsgegeven is. Bijvoorbeeld de burger van wie er bij HHSK betalingsgegevens bekend zijn voor het innen van huurgelden of gegevens die HHSK ontvangt bij een vergunningaanvraag of bezwaarschrift. Hieronder valt ook een medewerker van HHSK van wie gegevens worden verwerkt vanwege het personeelsbeleid. Onder de AVG heeft de betrokkene een aantal rechten, waaronder het recht op inzage, op rectificatie en op vergetelheid. Deze rechten worden in hoofdstuk 5 verder toegelicht.

HHSK helpt de betrokkene in de uitoefening van zijn rechten. Via de website wordt de betrokkene via een privacystatement (privacyverklaring) in heldere taal geïnformeerd over zijn rechten en de manier waarop hij deze rechten kan inroepen.

2.4 De verwerkingsverantwoordelijke

De verwerkingsverantwoordelijke stelt vast welke persoonsgegevens verwerkt (mogen) worden en wat het doel is van die verwerking. De verwerkingsverantwoordelijke neemt het initiatief voor de verzameling van persoonsgegevens en is daar ook verantwoordelijk voor. De verwerkingsverantwoordelijke is daarnaast verantwoordelijk voor het afhandelen en, indien nodig, melden van datalekken.

HHSK is in beginsel de verantwoordelijke voor de verwerking van persoonsgegevens. Binnen HHSK heeft het waterschapsbestuur diverse taken en bevoegdheden overgedragen aan de ambtelijke organisatie. Het dagelijks bestuur is echter eindverantwoordelijk en de verwerkingsverantwoordelijke in de zin van de AVG.

2.5 De verwerker

De verwerker of bewerker (verder verwerker genoemd) is de partij (of persoon) die persoonsgegevens verwerkt in opdracht van de verantwoordelijke (vaak dus HHSK). De verwerker valt niet onder de aansturing van de verantwoordelijke.

2.6 De verwerkersovereenkomst

In een zogenaamde verwerkersovereenkomst wordt vastgelegd dat de verwerker een beveiligingsniveau voor de bescherming van persoonsgegevens hanteert conform de Baseline Informatiebeveiliging Waterschappen (BIWA) en dit Privacybeleid. Hierin zijn ook andere afspraken gemaakt, zoals het melden van datalekken door de verwerker aan de verantwoordelijke en de aansprakelijkheid van partijen.

HHSK kan ook verwerker zijn voor andere partijen. Daarbij verwerkt HHSK persoonsgegevens in opdracht van een derde (die dan de verantwoordelijke is) op basis van afspraken die in een verwerkersovereenkomst zijn vastgelegd.

> ***Voorbeeld van HHSK als verwerker:***
>
> *Dit kan voorkomen als HHSK een samenwerkingsovereenkomst aangaat met bijvoorbeeld een gemeente. Onlangs is met de gemeente Lansingerland een samenwerkingsovereenkomst gesloten voor onderhoud. Als HHSK voor het uitvoeren van onderhoud persoonsgegevens van de gemeente nodig heeft, dan treedt HHSK op als verwerker van die persoonsgegevens en de gemeente als verwerkingsverantwoordelijke.*

Een verwerkersovereenkomst bestaat altijd naast een contract voor een product en/of dienstverlening.

2.6.1 Verspreiden naar derden

HHSK kan taken en processen uitbesteden aan externe verwerkers, die daarvoor de beschikking krijgen over persoonsgegevens waarvoor HHSK verantwoordelijk is. Denk bijvoorbeeld aan een callcenter dat in opdracht van HHSK klantvragen afhandelt, of een communicatiebureau dat in opdracht van HHSK een nieuwsbrief verspreidt. De verwerker is daarbij niet direct aan het gezag van de verantwoordelijke onderworpen, maar verwerkt de gegevens voor de verantwoordelijke. Met deze verwerkers worden afspraken gemaakt over de privacy en informatiebeveiliging conform de AVG en de BIWA.

2.6.2 Verwerken binnen en buiten de EU

Persoonsgegevens mogen in principe alleen binnen de EU verwerkt worden, aangezien de verordening van toepassing is in de hele EU. Het verwerken van persoonsgegevens buiten de EU mag alleen in specifieke gevallen. Dit zal ook vermeld worden als onderdeel van de gegevensbeschermingseffectbeoordeling, die bij verwerkingen buiten de EU altijd moet worden uitgevoerd. Daarvoor dient advies gevraagd te worden aan de privacy-juristen voordat het verwerken wordt uitgevoerd. Dit geldt ook als een verwerker een derde wenst in te schakelen om persoonsgegevens verder te verwerken.

2.6.3 Verschil geheimhouding en verwerkersovereenkomst

Het verschil tussen een overeenkomst waarin geheimhouding geregeld wordt versus een verwerkersovereenkomst zit primair in de belofte. De eerste is een passieve belofte “ik zal niets (actief) verder vertellen”. Bij de verwerkersovereenkomst is de belofte “ik zal de persoonsgegevens beschermen”. Dit vereist een (pro-)actieve houding.

2.7 Privacy-principes

De AVG gaat uit van een aantal beginselen waar elke verwerking van persoonsgegevens aan moet voldoen, de zogenaamde “privacy-principes”. Deze principes vormen het normatieve hart van de AVG en de verwerkingsverantwoordelijke is verantwoordelijk voor de naleving hiervan.

De principes luiden als volgt:

1. **De verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn**
   Persoonsgegevens mogen alleen verwerkt worden als de verwerking noodzakelijk is met het oog op het bereiken van een specifiek, in de AVG genoemd, doel of als er toestemming is verkregen van degene wiens gegevens worden verwerkt. De verwerking moet vervolgens netjes en verantwoord gebeuren. Tenslotte moet duidelijk zijn voor welke doelen de persoonsgegevens worden verwerkt en hoe dat gebeurt.
2. **De verwerking moet gebonden zijn aan specifieke verzameldoelen (doelbinding)**
   Persoonsgegevens mogen alleen worden verzameld en verwerkt voor vooraf bepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Wanneer de gegevens later voor een ander doel worden gebruikt, dan moet dat nieuwe doel verenigbaar zijn met het oorspronkelijke verzameldoel.
3. **De gegevens moeten toereikend, ter zake dienend en beperkt tot het noodzakelijke zijn (minimale gegevensverwerking)**
   Wanneer persoonsgegevens worden verwerkt, dan moeten zij voor het doel toereikend en slechts daaraan dienend zijn. Verder mogen er niet méér persoonsgegevens worden verwerkt dan strikt noodzakelijk voor het bepaalde doel.
4. **De gegevens moeten juist zijn**
   De verwerkingsverantwoordelijke (HHSK) moet alle redelijke maatregelen nemen om ervoor te zorgen dat de gegevens correct en actueel zijn. Gegevens die dat niet (meer) zijn, moeten worden gewist of gecorrigeerd.
5. **De gegevens mogen niet langer worden bewaard dan nodig**
   Persoonsgegevens mogen niet langer worden bewaard dan noodzakelijk voor het doel van de verwerking. Wanneer de bewaartermijn verstreken is, moeten persoonsgegevens dan ook worden vernietigd of gewist.
   De bewaartermijn is geheel afhankelijk van het doel waarvoor gegevens verzameld zijn. Het is aan de eigenaar van de gegevens om aan te geven hoe lang het noodzakelijk is de persoonsgegevens te bewaren. Er dient hierbij ook rekening gehouden te worden met wettelijke bewaarplichten zoals de archiefwet en de belastingwet.
6. **De gegevens moeten goed beveiligd zijn en vertrouwelijk blijven**
   Persoonsgegevens moeten worden beschermd tegen ongeoorloofde of onrechtmatige verwerking en tegen verlies, vernietiging of beschadiging. Voor de inrichting van informatiebeveiliging steunt HHSK op de Baseline Informatiebeveiliging Waterschappen (BIWA) en het informatiebeveiligingsbeleid van HHSK en HHR.

Voor HHSK is het belangrijk dat het privacybeleid helder is voor zowel de burgers als voor werknemers. HHSK moet transparant zijn over de verwerking van persoonsgegevens. Het moet voor betrokkenen duidelijk zijn in hoeverre en op welke manier er persoonsgegevens worden verwerkt. Alle communicatie richting betrokkene moet begrijpelijk zijn, ook met betrekking tot de rechten van betrokkenen. De gedachte hierachter is dat de betrokkene beter in staat is om in te schatten wat er met zijn gegevens gebeurt en eventueel actie kan ondernemen.

Een uitwerking hiervan is dat HHSK op zijn website een privacyverklaring heeft gepubliceerd.

2.8 Voorwaarden (grondslagen) voor verwerken

Persoonsgegevens mogen enkel worden verwerkt als er voldaan is aan minimaal één van de volgende voorwaarden (grondslagen):

- De betrokkende heeft voor de verwerking expliciet **toestemming** verleend (deze toestemming wordt te allen tijde geregistreerd)
- De verwerking is noodzakelijk voor de uitvoering van een **overeenkomst**
- De verwerking is noodzakelijk om een **wettelijke verplichting** na te komen
- De verwerking is noodzakelijk ter vrijwaring van een **vitaal belang** van de betrokkenen (bijvoorbeeld in geval van medische noodzaak als de betrokkene niet in staat is zelf toestemming te verlenen)
- De verwerking is noodzakelijk voor de goede vervulling van een **publiekrechtelijke taak**. Op grond van de AVG kan aan deze voorwaarde alleen worden voldaan als het gaat om een publiekrechtelijke taak, die op grond van de wet aan de verantwoordelijke is toegewezen.
- De verwerking is noodzakelijk voor de behartiging van een **gerechtvaardigd belang**. Deze grondslag geldt onder de AVG niet voor verwerkingen door overheidsinstanties in het kader van de uitoefening van hun publiekrechtelijke taken. Die vallen namelijk onder de voorgaande grondslag. Deze grondslag kan voor overheden echter wel van toepassing zijn in het kader van hun bedrijfsvoering.

Als er niet voldaan kan worden aan tenminste één van de genoemde voorwaarden (grondslagen) dan mogen de persoonsgegevens niet worden verwerkt.

Enkele voorbeelden van situaties waarin verwerking niet is toegestaan:

- *Kan het vastgestelde doel op een andere manier worden bereikt? Dan is het niet noodzakelijk om persoonsgegevens te verwerken en dus niet toegestaan.*
- *Als er te weinig persoonsgegevens worden verwerkt om het doel te kunnen bereiken, dan is die verwerking geen geschikt middel om het doel te bereiken en daarom niet toegestaan.*
- *Er mag niet begonnen worden met het verzamelen van gegevens, voordat het doel daarvan is vastgesteld.*
- *Als het doel van de verwerking tussentijds verandert, dan moet de verwerking stoppen. Nadat een gegevensbeschermingseffectbeoordeling is uitgevoerd, zou de verwerking opnieuw gestart kunnen worden.*

2.9 Privacy door ontwerp (privacy by design)

Privacy door ontwerp wil zeggen dat bij de ontwikkeling van producten al wordt nagedacht hoe de privacy van gebruikers zo optimaal mogelijk kan worden beschermd. Denk bijvoorbeeld aan het implementeren van

versleuteling van gegevens. Mocht de server worden gehackt, dan kan de hacker niets met die gegevens zonder daar een “sleutel” voor te hebben. Een voorbeeld van versleuteling is pseudonimisering. De persoonsgegevens worden dan vervangen door een pseudoniem. In het product kan een bepaald algoritme worden geïmplementeerd, dat berekent door welk pseudoniem de gegevens moeten worden vervangen. Natuurlijk blijft het mogelijk om door middel van hetzelfde algoritme de persoonsgegevens weer op te halen.

Andere voorbeelden van ‘privacy door ontwerp’ zijn: anonimisering, firewalls en twee-staps authenticatie. Anonimisering wil zeggen dat alle persoonlijke kenmerken uit gegevens worden verwijderd, waardoor het voor zowel ongewenste personen als de verwerker zelf niet mogelijk is om de gegevens te herleiden naar een persoon.. Een firewall is een soort filter die het inkomende en uitgaande internetverkeer controleert. Indien ongewenst verkeer wordt herkend, kan de firewall dit tegenhouden. Twee-staps authenticatie tot slot betekent dat er niet alleen een wachtwoord ingevoerd moet worden om in te kunnen loggen, maar daarnaast nog een extra handeling moet worden verricht. Denk bijvoorbeeld aan het intypen van een code die per sms wordt verstuurd, of het accepteren van een pop-up op de telefoon.

2.10 Privacy als standaard (privacy by default)

Privacy door standaardinstellingen houdt in dat maatregelen worden genomen om standaard alleen persoonsgegevens te verwerken, die noodzakelijk zijn voor het doel van de verwerking. Dit gebeurt bij HHSK bijvoorbeeld door de webformulieren zo aan te passen dat de burger zelf mag kiezen welke persoonsgegevens hij invult en wij slechts de strikt noodzakelijke gegevens verplicht stellen om in te vullen. Daarnaast dient de burger zelf actief toestemming te verlenen voor het ontvangen van een nieuwsbrief of een terugkoppeling op een melding.

3. Data Protection Impact Assessment (risicoanalyse)

Een Data Protection Impact Assessment (risicoanalyse), hierna te noemen “DPIA” is een methode om in een vroeg stadium van een gewenste verwerking op een gestructureerde manier privacyrisico’s in beeld te brengen. Een DPIA wordt in het kader van de AVG ook wel een Gegevensbeschermingseffectbeoordeling (GEB) genoemd.

Er wordt in geval van nieuwe informatiesystemen, applicaties of risicovolle projecten waar veel en/of gevoelige persoonsgegevens worden verwerkt altijd een DPIA gedaan; de diepgang hiervan is echter afhankelijk van de specifieke situatie. Een DPIA moet daarnaast ook worden uitgevoerd als er sprake is van de wijziging van het doel en de grondslag voor de verwerking van de gegevens of als het werkproces wijzigt waarbinnen de persoonsgegevens worden verzameld.

3.1 DPIA bij verwerkingen

Een DPIA is altijd verplicht als de verwerking waarschijnlijk een hoog privacyrisico oplevert voor de betrokkenen. Dat is in ieder geval aan de orde bij:

- het systematisch en uitvoerig evalueren van persoonlijke aspecten, waaronder profiling[1];
- het op grote schaal verwerken van bijzondere persoonsgegevens; en / of
- het op grote schaal systematisch volgen van mensen in een publiek toegankelijk gebied (bijvoorbeeld met cameratoezicht bij een gemaal of in de openbare ruimtes van HHSK).

3.2 DPIA bij veranderingen

Voor grootschalige wijzigingen in IT- systemen is vooraf advies nodig van de privacy-desk en de security-officer.. Deze medewerkers zullen samen de wijziging analyseren om vervolgens vast te stellen of het hier gaat om een wijziging in de verwerking van persoonsgegevens. Vervolgens zullen zij adviseren of nader juridisch advies nodig is of dat er een DPIA moet worden uitgevoerd om de risico’s beter in kaart te brengen.

[1] Bij profiling wordt er data verzameld met als doel een profiel op te bouwen rondom een medewerker of een burger, bijvoorbeeld om vast te stellen of iemand structureel wanbetaler is of regelmatig bij grote projecten klachten indient.

4. Rechten van betrokkenen

4.1 De verschillende rechten van betrokkenen

Alle betrokkenen (burgers en werknemers) hebben op grond van de AVG diverse rechten met betrekking tot hun persoonsgegevens. Van deze rechten kunnen zij gebruikmaken door middel van een verzoek bij HHSK. Dat zijn de volgende rechten:

- **Informatie**:
  Recht om te weten wat er met de persoonsgegevens gebeurt en waarom.
- **Inzage**
  Recht om inzage te krijgen in de persoonsgegevens die HHSK verzamelt en gebruikt.
- **Rectificatie**
  HHSK dient te zorgen dat de gegevens accuraat zijn en blijven. De betrokkene heeft het recht om correctie van persoonsgegevens te vragen. Ook heeft hij het recht om gegevens aan te laten vullen wanneer deze incompleet zijn.
- **Verwijdering en recht om vergeten te worden**
  Betrokkene heeft het recht op verwijdering van persoonsgegevens als verwerking van deze persoonsgegevens onrechtmatig is. Daarnaast heeft hij het recht om een eenmaal gegeven toestemming voor het verwerken van de gegevens in te trekken. Ook bestaat in sommige gevallen het recht om vergeten te worden. Dit is bijvoorbeeld het geval als de wettelijk bepaalde bewaartermijn is verstreken.
- **Beperking**
  In bepaalde gevallen bestaat het recht dat HHSK de gegevens tijdelijk niet gebruikt. Dit recht bestaat in de volgende situaties:
  - in afwachting van een beoordeling van een verbetering van de persoonsgegevens
  - in afwachting van de beoordeling van een bezwaar
  - indien de gegevens eigenlijk verwijderd zouden moeten worden, maar betrokkene dit niet wenst
  - indien het hoogheemraadschap de gegevens niet langer nodig heeft, maar betrokkene nog wel, bijvoorbeeld voor een rechtszaak
- **Verzet**
  Recht om HHSK te vragen om persoonsgegevens niet meer te gebruiken. Dit is echter niet mogelijk als HHSK persoonsgegevens heeft verzameld om te voldoen aan een wettelijke verplichting of voor de bescherming van vitale belangen.
- **Overdraagbaarheid van gegevens**
  Recht om de gegevens die aan HHSK zijn verstrekt, (terug) te ontvangen in een gangbaar bestandsformaat. Deze gegevens kunnen vervolgens worden overgedragen aan een andere organisatie.
- **Niet onderworpen te worden aan geautomatiseerde besluiten**
  Recht om niet onderworpen te worden aan een volledig geautomatiseerde verwerking, zonder menselijke tussenkomst, als dit:
  - Rechtsgevolgen voor de betrokkene heeft, bijvoorbeeld de weigering of toekenning van huur- of kinderbijslag
  - Het besluit de betrokkene in aanzienlijke mate treft, bijvoorbeeld het wel of niet verstrekt krijgen van een krediet

- **Klachtrecht**
  Recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens (AP) over hoe HHSK omgaat met persoonsgegevens.

4.2 Privacy-verzoeken van betrokkenen

Als verzoeken in relatie tot bovenstaande rechten binnenkomen, worden deze doorgezet naar de privacy-desk. De privacy-juristen zullen samen met de verwerkingsverantwoordelijke en medewerkers van de vakafdelingen de aanpak bepalen en uitvoeren.

4.3 Rechtsbescherming

De besluiten die HHSK neemt in het kader van een ingeroepen recht van een betrokkene, worden conform artikel 34 van de Uitvoeringswet AVG aangemerkt als een besluit in de zin van de Algemene wet bestuursrecht (Awb) en zijn daarom vatbaar voor bezwaar en beroep.

Hiervoor worden de bestaande procedures voor de afhandeling van bezwaar en beroep gebruikt.

5. Protocol “Meldplicht Datalekken” en Incident Response Team

5.1 Wat is een datalek?

Een inbreuk in verband met persoonsgegevens, beter bekend als een datalek, is een inbreuk op de beveiliging die leidt tot de vernietiging, het verlies, de wijziging, de ongeoorloofde verstrekking of de ongeoorloofde toegang tot doorgezonden, opgeslagen of op andere wijze verwerkte persoonsgegevens.

Voor de kwalificatie als “datalek” is het niet relevant dat er opzet in het spel is. Hoewel een hack van de systemen waarbij persoonsgegevens worden buitgemaakt een schoolvoorbeeld is van een datalek, kunnen ook gegevens die op een verloren laptop staan, een verkeerde verstuurde mail of een afgesloten website met persoonsgegevens die per ongeluk open staat, ook kwalificeren als een datalek.

5.2 Meldplicht en Incident Response Team

HHSK heeft bij een datalek een mogelijke meldplicht naar de Autoriteit Persoonsgegevens. Deze meldplicht houdt in dat HHSK binnen 72 uur een melding moet doen bij de Autoriteit Persoonsgegevens zodra HHSK een ernstig datalek constateert. Als het datalek negatieve gevolgen heeft of kan hebben voor de betrokkene (bijvoorbeeld financiële fraude of identiteitsfraude), meldt HHSK het datalek ook “onverwijld” aan de betrokkenen (de personen van wie de persoonsgegevens zijn gelekt).

HHSK heeft een protocol voor de afhandeling van datalekken, het “Incident Response Plan”, hierna te noemen “IRP”. In het IRP staan de stappen, taken en verantwoordelijkheden beschreven bij het melden van een datalek. Een speciaal Incident Response Team (IRT) komt bij het bekend worden van een datalek onmiddellijk bijeen en bepaalt de strategie aan de hand van het IRP. De FG zit het IRT (indien mogelijk) voor.

Bijlage A: Checklist voor het werken met persoonsgegevens

Uitgangspunten bij het werken met persoonsgegevens.	
1	**Doel** Heb ik vooraf een doel voor de verwerking van persoonsgegevens vastgesteld?
2	**Doelbinding** Worden de persoonsgegevens alleen gebruikt voor het doel dat ik heb vastgelegd?
3	**Grondslag** Is er minimaal een wettelijke grondslag voor de verwerking? • Ik heb aantoonbare toestemming van de burgers of werknemers • De gegevens zijn nodig voor de uitvoering van een overeenkomst • Het verwerken van deze gegevens is wettelijk verplicht • De verwerking van gegevens is nodig voor het uitvoeren van onze publiekrechtelijke taak • Er is een gerechtvaardigd belang, alleen voor interne bedrijfsprocessen,
4	**Kwaliteit** Zijn de te gebruiken gegevens: • actueel • nauwkeurig • juist
5	**Dataminimalisatie** • Gebruik ik alleen die gegevens die noodzakelijk zijn om het vastgestelde doel te verwezenlijken? • Bewaar ik deze gegevens niet langer dan nodig?
6	**Transparantie** • Heb ik de burgers of werknemers vooraf geïnformeerd over het doel van de gegevensverwerking? • Heb ik uitgelegd welke gegevens worden gebruikt en met wie deze worden gedeeld?
7	**Geheimhoudingsplicht** • Ben ik mij ervan bewust dat ik bij het gebruik van persoonsgegevens een geheimhoudingsplicht heb van de gegevens en de afleidbare informatie? • Heb ik een verwerkersovereenkomst gesloten met degene die de persoonsgegevens voor mij verwerkt (indien van toepassing)?
8	**Meldplicht Beveiligingsincidenten** Bij verlies of diefstal van de persoonsgegevens of als ik een vermoeden heb van een datalek weet ik dat ik dit moet melden bij de privacy-desk.