Gemeente Hellendoorn

Beleidskader privacy 2024-2026

Gemeente Hellendoorn

Inhoudsopgave

1. Inleiding 3

1.1 Juridisch kader gemeentelijk privacy beleid 3
1.2 Bestuurlijke ambitie privacy 4
1.3 Speerpunten van beleid 4
1.4 Onderliggend beleid en richtlijnen 5

2. Uitgangspunten privacy beleid 6

2.1 Rechtmatigheid, behoorlijkheid en transparantie 6
2.2 Doelbinding 6
2.3 Minimale gegevensverwerking 7
2.4 Juistheid 7
2.5 Opslagbeperking 7
2.6 Integriteit en vertrouwelijkheid 7

3. Strategische invulling gemeentelijke verantwoordelijkheid 8

3.1 Verwerkingsgrondslagen AVG 8
3.2 Opstellen register van verwerkingsactiviteiten 8
3.3 Toegang tot privacygevoelige informatie 9
3.4 Aanstellen functionaris voor de gegevensbescherming (FG) 9
3.5 Meldplicht datalekken 9
3.6 Rechten van betrokkenen 10
3.7 Privacy by design en privacy by default 10
3.8 Uitvoering data protection impact assessment (dpia) 11
3.9 Inschakeling verwerkers, verwerkersovereenkomst 11
3.10 Beveiliging van persoonsgegevens 11
3.11 Veilig en vaardig werken: stimulering iBewustzijn 12
3.12 Verantwoordingsplicht (accountability) 12

4. Organisatie, taken en verantwoordelijkheden 13

4.1 Bestuurlijke organisatie 13
4.2 Management 13
4.3 Verantwoordelijkheid medewerkers 14

5. Tot besluit 14

Bijlagen 14

Documentnaam : Beleidskader privacy 2024-2026 Gemeente Hellendoorn
Datum : 12 december 2023
Status : Definitief

Definities en afkortingen

AVG	Algemene Verordening Gegevensbescherming. Dit is een Europese verordening (dus met rechtstreekse werking) die de regels voor de verwerking van persoonsgegevens door particuliere bedrijven en overheidsinstanties in de hele Europese Unie standaardiseert.
AP	Autoriteit Persoonsgegevens; de onafhankelijke Nederlandse toezichthouder op de naleving van de Europese en nationale regels voor de bescherming van persoonsgegevens.
Betrokkene	Individu van wie persoonsgegevens worden verwerkt, bijvoorbeeld de inwoner, leverancier of medewerker.
DPIA	Data protection impact assessment; een instrument om te kunnen aantonen dat de organisatie voldoet aan de verplichtingen uit de AVG. Wordt uitgevoerd bij een nieuwe verwerking of bij de wijziging van een bestaande verwerking die naar verwachting een hoog risico voor de rechten en vrijheden van betrokkene met zich meebrengt.
Persoonsgegevens	Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, bijvoorbeeld naam, adres, woonplaats, telefoonnummer, geboortedatum, mailadressen, financiële persoonsgegevens, bankrekeningnummers, paspoortkopieën, foto's, bijzondere persoonsgegevens zoals medische gegevens, strafrechtelijke persoonsgegevens en bij wet voorgeschreven identificatienummers (BSN).
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming; geeft invulling aan bepalingen die in de AVG niet (volledig) zijn uitgewerkt.
Verwerken	Elke handeling met betrekking tot persoonsgegevens valt onder het verwerken van persoonsgegevens, bijvoorbeeld het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op een andere manier beschikbaar stellen, samenbrengen, met elkaar in verband brengen, afschermen, wissen of vernietigen van gegevens.
Verwerker	De verwerker is de persoon of de organisatie die de persoonsgegevens verwerkt namens de verwerkingsverantwoordelijke.
Verwerkings-verantwoordelijke	De verwerkingsverantwoordelijke is een persoon of organisatie die het doel van en de middelen voor het verwerken van persoonsgegevens bepaalt.
Wpg	Wet politiegegevens; gebaseerd op een Europese verordening die de regels voor de verwerking van politiegegevens regelt. De Wpg geldt vanaf 2019 ook voor de buitengewoon opsporingsambtenaren (BOA's) van gemeenten.

1. Inleiding

Privacy is een fundamenteel recht dat essentieel is voor de vrijheid en autonomie van individuen. Dit recht beschermt niet alleen persoonsgegevens maar strekt zich ook uit tot fysieke ruimten, persoonlijke communicatie, en het familieleven. Het is een grondrecht dat met de grootste zorgvuldigheid dient te worden behandeld. In dit 'Beleidskader Privacy 2024-2026' ligt de focus op de bescherming van persoonsgegevens. Hierin wordt uiteengezet hoe de gemeente Hellendoorn omgaat met de verzameling, opslag en beveiliging van persoonsgegevens. Deze taak is van cruciaal belang, omdat de gemeente toegang heeft tot gevoelige informatie van zowel burgers als bedrijven. Deze moeten erop kunnen vertrouwen dat die informatie bij de gemeente in goede handen is.

De persoonsgegevens die de gemeente Hellendoorn verwerkt of laat verwerken, vallen onder de Algemene Verordening Gegevensbescherming (AVG) en de Uitvoeringswet Algemene Verordening Gegevensbescherming (UAVG). Dit beleid is een uitwerking van de uitgangspunten, regels en verplichtingen die afkomstig zijn uit deze wetgeving. Voor enkele werkprocessen binnen de gemeente gelden vaak aanvullende beveiligingseisen, die veel overeenkomsten vertonen met de eisen uit de AVG, maar in hun uitwerking soms net een stap verder gaan. Voor die onderdelen komen afzonderlijke beleidskaders, zodat duidelijk is hoe we hier als gemeente Hellendoorn invulling aan geven. Dit betreft bijvoorbeeld het sociaal domein, de basisregistratie personen en de verwerking van politiegegevens.

De gemeente Hellendoorn geeft met dit beleid duidelijk richting aan hoe de organisatie om moet gaan met privacy en laat zien dat zij de privacy waarborgt, beschermt en handhaaft. Dit beleid is van toepassing op de gehele organisatie en op alle processen, onderdelen, objecten en gegevensverzamelingen van de gemeente waarin persoonsgegevens worden verwerkt.

1.1 Juridisch kader gemeentelijk privacy beleid

Privacybescherming is een complexe materie die in diverse wetten en verdragen is vastgelegd. De belangrijkste regelgeving hierin is de Algemene Verordening Gegevensbescherming (AVG). Deze Europese wet is van toepassing op zowel particuliere bedrijven als overheidsinstellingen binnen de Europese Unie.

De AVG benadrukt de verantwoordelijkheid van organisaties om aan te tonen dat zij in overeenstemming met de wet handelen. Deze organisaties worden in de AVG aangeduid als 'verwerkingsverantwoordelijken'. Zij zijn degene die het doel en de middelen voor het verwerken van persoonsgegevens bepalen. Onder het 'verwerken van persoonsgegevens' valt een scala aan handelingen: van het verzamelen en opslaan tot het vernietigen van gegevens. Dit betekent in de dagelijkse praktijk dat de AVG bijna altijd van toepassing is zodra er met persoonsgegevens wordt gewerkt. Als dat door een rechtspersoon gebeurt, is deze rechtspersoon de verwerkingsverantwoordelijke, niet de individuele werknemer die de gegevens feitelijk verwerkt. De AVG is niet van toepassing op gegevens die worden gebruikt voor strafrechtelijke doeleinden. Hiervoor geldt de Europese Richtlijn gegevensverwerking opsporing en vervolging. In Nederland is de Wet politiegegevens (Wpg) hierop aangepast. De Wpg is sinds 2019 ook van toepassing op buitengewoon opsporingsambtenaren (boa's).

De Autoriteit Persoonsgegevens (AP) houdt toezicht op de naleving van deze wetten. Zij hebben de bevoegdheid om sancties op te leggen, die kunnen variëren van boetes tot 4% van de totale wereld-wijde jaaromzet of 20 miljoen euro, tot een last onder dwangsom en andere sancties.

1.2 Bestuurlijke ambitie privacy

Inwoners mogen van de gemeente Hellendoorn – zoals eerder aangegeven - verwachten dat ze zorgvuldig omgaat met persoonsgegevens en andere informatie. Daarnaast wil Hellendoorn een solide en betrouwbare partner zijn voor bedrijven, ketenpartners en derden vanuit haar verant-woordelijkheid voor gegevens die zij met ons delen. Dit betekent dat de gemeente er alles aan doet om de werkprocessen en informatiesystemen zodanig in te richten en te beheren dat veiligheid en privacy gewaarborgd zijn. De gemeente ziet dit niet als een eenmalige actie, maar als een continu proces, waarbij het beleid en de daarop gebaseerde wijze van werken voortdurend worden aangepast en afgestemd op nieuwe ontwikkelingen en ervaringen vanuit de dagelijkse praktijk.

De gemeente is daarnaast aantoonbaar 'in control' op privacy-gebied. Dit betekent dat de gemeente weet welke processen, gegevensstromen en bijbehorende informatie(systemen) zij in huis heeft, welke passende technische en organisatorische beveiligingsmaatregelen er al zijn en welke nog moeten worden ingericht. Ook betekent 'in control' dat de gemeente aan kan tonen dat de gegevensverwerking in overeenstemming met de geldende regelgeving wordt uitgevoerd en de beveiligingsmaatregelen toereikend en effectief zijn. Getroffen maatregelen dienen daarbij continu te worden geëvalueerd en indien nodig geactualiseerd. Door periodieke controle, organisatie brede planning én coördinatie wordt de kwaliteit van de gegevensverwerking verankerd binnen de gemeentelijke organisatie.

1.3 Speerpunten van beleid

De speerpunten die voor de uitvoering van de AVG de komende jaren hoog op de agenda van de gemeente staan zijn:

1. **Compliance:** borgen dat het interne beleid en de bedrijfsvoering in overeenstemming zijn met de vereisten van de AVG. Dit beleid moet kenbaar en vindbaar zijn voor de organisatie. De ambitie is om privacy naar een steeds hoger niveau te tillen.
2. **Privacy by design en default:** de gemeente zorgt dat de bescherming van persoonsgegevens altijd vanaf het begin bij vernieuwingen en veranderingen, zowel bij systemen als beleid en processen, meegenomen wordt.
3. **Bewust maken van verantwoordelijkheden:** de gemeente zorgt ervoor dat binnen de gehele gemeentelijke organisatie gehandeld wordt naar een verantwoordelijkheid voor de privacy-bescherming van de lijn met duidelijk ingevuld eigenaarschap.
4. **Aantoonbaar in control:** de gemeente verankert de bescherming van persoonsgegevens in de reguliere planning en control cyclus, en draagt zorg voor het periodiek uitvoeren van onafhankelijke onderzoeken en zelfevaluaties om het geheel voortdurend up-to-date te houden.

Eén en ander laat echter onverlet dat 100% beveiliging tegen cybercrime en andere vormen van misbruik van persoonsgegevens altijd een onmogelijke opgave zal blijven. Met het treffen van gerichte maatregelen – zowel technisch als organisatorisch – proberen we beveiligingsincidenten zoveel mogelijk te voorkomen en eventuele gevolgen te minimaliseren.

1.4 Onderliggend beleid en richtlijnen

Dit strategisch privacybeleid dient als algemene basis en dekt daarnaast voor een groot deel ook de beveiligingseisen uit specifieke wetgeving af. Voor bepaalde onderdelen met extra beveiligingseisen, zoals het sociaal domein, toezicht en handhaving en de basisregistratie personen, worden aanvullende beleidskaders opgesteld. Daarmee zorgen we voor duidelijkheid over de aanpak van de gemeente Hellendoorn. Deze kaders zijn verder uitgediept in gedragsregels, protocollen, procedures en werkinstructies. Goedkeuring voor (herzien) beleid moet altijd worden verkregen van het college van B&W. De uitvoering, inclusief het vaststellen van aanvullende regels en procedures, is gemandateerd aan het management en de algemeen directeur.

In het jaarlijkse privacy jaarplan, dat wordt vastgesteld door het managementteam, worden operationele aspecten van privacy en AVG verder uitgewerkt. Dit gebeurt op basis van input van teams, de interne organisatie rondom informatiebeveiliging en privacy, en nationale trends en ontwikkelingen. Hierbij worden ook wijzigingen in wet- en regelgeving en dreigingsbeelden van onder meer de Informatiebeveiligingsdienst (IBD) en het Nationaal Cyber Security Centrum (NCSC) meegenomen. Alle relevante wet- en regelgeving is toegankelijk via het gemeentelijke intranet.

Tot slot is dit beleid vastgesteld door het College van B&W voor de periode 2024 t/m 2026. Het is van toepassing op alle gemeentelijke processen en onderdelen waar de AVG relevant is. Het beleid wordt jaarlijks beoordeeld en indien nodig aangepast om te zorgen dat het blijft voldoen aan de vereisten voor een effectieve privacybescherming.

2. Uitgangspunten privacy beleid

De AVG noemt zes beginselen die organisaties moeten naleven tijdens het verwerken van persoonsgegevens. De verwerkingsverantwoordelijke – in gemeenten: het college van B&W – is verantwoordelijk voor het naleven van de beginselen en moet de naleving binnen de organisatie kunnen aantonen. Dit betekent dat passende technische en organisatorische maatregelen genomen moeten worden, zoals bijvoorbeeld het opstellen van beleidsregels, interne audits van verwerkingsactiviteiten en protocollen voor het omgaan met privacygevoelige informatie. Het betreft de volgende beginselen:

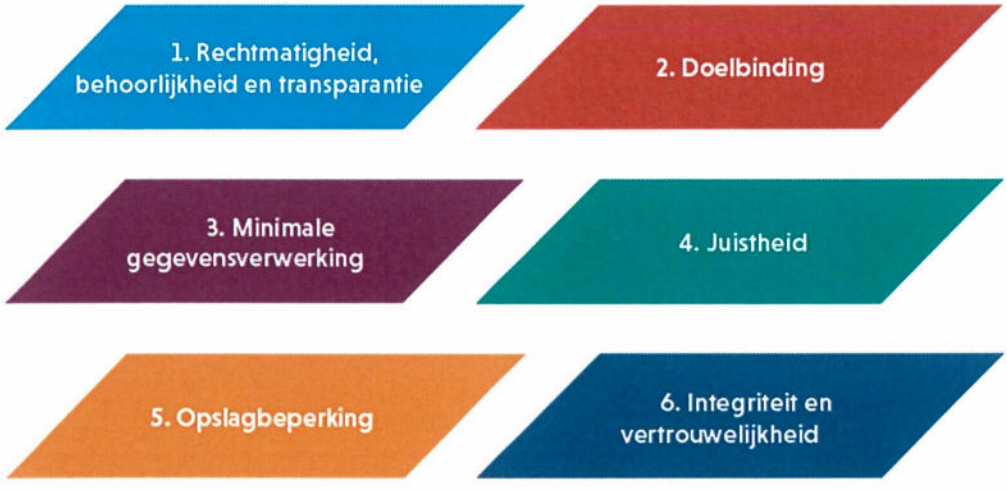
2.1 Rechtmatigheid, behoorlijkheid en transparantie

Organisaties moeten in de eerste plaats zorgen dat ze in overeenstemming met de relevante wet- en regelgeving werken en persoonsgegevens op behoorlijke, transparante en zorgvuldige wijze verwerken. Dit betekent dat er een grondslag moet zijn voor het verwerken van persoonsgegevens, dat we transparant zijn en op eigen initiatief communiceren naar betrokkenen over verwerkingen en daarbij aangeven welke risico's, regels, waarborgen en rechten er zijn voor betrokkenen. Dit doen we onder andere met een privacyverklaring op de website en het opnemen van al onze verwerkingen in een register van verwerkingsactiviteiten.

2.2 Doelbinding

Persoonsgegevens mogen vervolgens alleen worden verwerkt voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden die voorafgaand aan de verwerking zijn bepaald. Hierbij wordt een zorgvuldige afweging gemaakt overeenkomstig de eisen van proportionaliteit en subsidiariteit. Dit betekent dat de verwerking in relatie moet staan tot het doel en wanneer er sprake is van een inbreuk op de privacy, dit op de minst ingrijpende manier plaatsvindt. De persoonsgegevens worden alleen voor een ander doel gebruikt als dat verenigbaar is met de oorspronkelijke doeleinden. Het doel stelt daarmee de kaders waarbinnen we de gegevens mogen verwerken.

Uitgangspunten van het gemeentelijke privacy beleid



2.3 Minimale gegevensverwerking

Daarnaast mogen persoonsgegevens alleen worden verwerkt als dit strikt noodzakelijk is voor de doeleinden waarvoor ze worden gebruikt en als er redelijkerwijs geen andere (minder ingrijpende) manier is om het doel te realiseren. Ook mogen de persoonsgegevens niet langer worden bewaard dan nodig is. Bij de ontwikkeling van nieuwe producten en diensten wordt daarom zo vroeg mogelijk aandacht besteed aan het beschermen van de persoonsgegevens en zo ook aan de vraag of alle gegevens echt noodzakelijk zijn.

2.4 Juistheid

Als gemeente moeten we alle redelijke maatregelen nemen om ervoor te zorgen dat persoonsgegevens juist en actueel zijn. Dit doen we bijvoorbeeld door gebruik te maken van koppelingen met landelijke databases, zoals de BRP. Ook het gebruikmaken van standaard formulieren bij een intake en vaste sjablonen bij het opstellen van bijvoorbeeld brieven of rapporten helpen medewerkers om de juiste gegevens uit te vragen (en niet meer dan nodig). Als door ons verwerkte persoonsgegevens onjuist blijken te zijn, dan heeft de betrokkene het recht om deze gegevens te laten wijzigen of wissen. Als wij deze persoonsgegevens hebben gedeeld met andere organisaties, moeten we de wijzigingen zo snel mogelijk aan hen doorgeven.

2.5 Opslagbeperking

Het beginsel van opslagbeperking moet ervoor zorgen dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor de verwerking. De AVG geeft zelf geen concrete bewaartermijnen, maar verlangt wel dat we termijnen vaststellen voor het wissen van deze persoonsgegevens. De zogeheten selectielijst van de VNG vormt de basis voor het bewaren en vernietigen van archiefbescheiden bij gemeenten en intergemeentelijke organen. Daarnaast zijn er ook bewaartermijnen vastgelegd in specifieke wet- en regelgeving, zoals bijvoorbeeld de Wet politiegegevens. Als er een wettelijke plicht op de gemeente rust om de gegevens te bewaren, verwijdert de gemeente deze gegevens pas als de wettelijke bewaartermijn verlopen is.

2.6 Integriteit en vertrouwelijkheid

Tot slot moeten we als organisatie passende technische en organisatorische maatregelen nemen om persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging, verlies of wijziging, ongeautoriseerde openbaarmaking, misbruik of anderszins verwerking in strijd met de wet. Welke maatregelen we moeten nemen hangt af van de risico's die met een bepaalde verwerking gepaard gaan. Naarmate gegevens met een gevoeliger karakter worden verwerkt, worden zwaardere eisen gesteld aan de beveiliging. Meer informatie over de beveiliging van onze gegevens is vastgelegd in het informatiebeveiligingsbeleid.

3. Strategische invulling

Iedereen heeft recht op privacy. Gemeenten verzamelen en gebruiken veel persoonsgegevens. Deze gegevens zijn nodig voor het uitvoeren van de veelheid van taken waar de gemeente voor is. De gemeente is verantwoordelijk voor de bescherming van deze persoonsgegevens. Doel van dit privacy beleid is het beschrijven van kaders voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacy rechten van personen waarvan de gemeente Hellendoorn persoonsgegevens verwerkt. Met de maatregelen beschreven in dit hoofdstuk kunnen de doelstellingen worden gehaald en de risico's worden beperkt.

3.1 Verwerkingsgrondslagen AVG

Elke keer als persoonsgegevens worden verwerkt, is dat een inbreuk op de privacy van de mensen over wie het gaat. Als gemeente Hellendoorn verwerken we daarom alleen persoonsgegevens als het echt niet anders kan. Dus: als zonder deze gegevens het doel niet kan worden bereikt. De AVG noemt 6 grondslagen die we in dit verband kunnen hanteren:

1. **Toestemming:** toestemming kan gegeven worden door een vrije, specifieke, geïnformeerde en ondubbelzinnige wilsuiting. Stilzwijgende toestemming is niet voldoende.
2. **Uitvoering van een overeenkomst:** het gaat dan uiteraard om een overeenkomst waarbij de betrokkene partij is. Belangrijk is dat de overeenkomst niet uitgevoerd kan worden zonder die persoonsgegevens.
3. **Wettelijke verplichting:** zeker in gemeenteland bestaan er veel wettelijke verplichtingen op basis waarvan je persoonsgegevens moet verwerken. Ook worden daarin vaak eisen genoemd waaraan de verwerking moet voldoen.
4. **Vitaal belang:** vitaal wil zeggen dat het gaat om het leven van de persoon, waarbij de verwerking van persoonsgegevens nodig is om hem of haar te kunnen helpen.
5. **Algemeen belang:** hieronder vallen de gebruikelijke verwerkingen van, voor of namens de overheid (waar meestal ook al een wettelijke basis voor is).
6. **Gerechtvaardigd belang:** een verwerking moet aantoonbaar noodzakelijk zijn om bedrijfsactiviteiten te kunnen verrichten. Het vraagt een afweging tussen de belangen van de organisatie en de belangen van de betrokkenen.

Belangrijk is nog dat toestemming altijd vrij gegeven moet worden. In een overheidsorganisatie waarbij inwoners alleen bij hun eigen gemeente terecht kunnen is daarvan lang niet altijd sprake. Toestemming kan daarom alleen gebruikt worden voor optionele extra's.

3.2 Opstellen register van verwerkingsactiviteiten

Overeenkomstig de AVG leggen we al onze verwerkingsactiviteiten vast in een register. Het register geeft inzicht in wat er binnen de gemeente Hellendoorn is geregeld over de verwerking van persoonsgegevens. Denk bijvoorbeeld aan de verwerkingsdoeleinden, de aard van de verwerkte

gegevens, categorieën betrokken, bewaartermijnen en de getroffen beveiligingsmaatregelen. Het bijhouden van het register valt onder de verantwoordingsplicht, de 'privacyboekhouding' van de gemeente. Het is één van de zaken die we moeten inrichten om de naleving van de AVG aan te kunnen tonen. De privacy officer beheert het register van verwerkingsactiviteiten. Proceseigenaren zijn verantwoordelijk voor het (laten) opnemen van nieuwe verwerkingen in het register. Het register van verwerkingsactiviteiten wordt periodiek geactualiseerd.

3.3 Toegang tot privacygevoelige gegevens

Toegang tot applicaties, waarin gevoelige gegevens worden verwerkt, is binnen de gemeente Hellendoorn beperkt. Toegangsbeveiliging is ingericht, waardoor alleen aan die personen toegang tot informatie wordt verleend, die daarop recht hebben. Uitgangspunt daarbij is het principe "need to know": medewerkers moeten de informatie nodig hebben om hun functie goed te kunnen uitoefenen. Dit geldt zowel voor vaste medewerkers, als voor inhuur en leveranciers. Halfjaarlijks vindt evaluatie plaats van de rechten die uitgegeven zijn. Om de toegang goed te kunnen regelen, heeft de gemeente toegangsrichtlijnen en -protocollen opgesteld.

Daarnaast legt elke medewerker van de gemeente de eed of belofte af en overhandigt een Verklaring Omtrent Gedrag (VOG). Bij alle systemen waarin persoonsgegevens worden verwerkt vindt logging plaats, waarbij gebeurtenissen op de systemen worden vastgelegd. De logbestanden worden steek-proefsgewijs gecontroleerd op (on)rechtmatig gebruik. Net zoals bij alle andere verwerkingen van persoonsgegevens, moet bij de doorgifte van persoonsgegevens sprake zijn van een gerechtvaardigd doel. Belangrijk is vooral dat de doorgifte verenigbaar is met het doel waarvoor de persoonsgegevens zijn verkregen.

3.4 Aanstellen functionaris voor de gegevensbescherming (FG)

Op grond van de AVG is het aanstellen van een FG voor Hellendoorn verplicht. De FG is een onafhankelijke toezichthouder die gevraagd en ongevraagd advies geeft op het gebied van de AVG. De FG ziet er op toe dat de gemeente voldoet aan de wettelijke verplichtingen bij het verwerken van persoonsgegevens. Hij toetst onder andere de naleving van de wettelijke eisen, gemeentelijke richtlijnen op het gebied van privacy, het privacy beleid en het beveiligingsbeleid. De FG maakt jaarlijks een toezichtplan, voert dit uit en rapporteert zo nodig rechtstreeks aan het college en/of andere verwerkingsverantwoordelijken. De FG is contactpersoon voor de Autoriteit Persoons-gegevens (AP).

Binnen de gemeente is daarnaast een privacy officer (PO) aangesteld. De PO adviseert over c.q. vormt de vraagbaak binnen de gemeente voor AVG- en privacyvraagstukken, geeft advies omtrent de uitvoering van het privacy beleid en draagt bij aan de vergroting van privacy bewustzijn en -kennis. Ook kennen we bij de verschillende teams één of meer privacy ambassadeurs. Medewerkers, die naast hun directe taken net even iets meer weten over privacy en AVG. Op die wijze kunnen ze de naaste collega's en eigen manager gemakkelijk adviseren over privacy gerelateerde thema's.

3.5 Meldplicht datalekken

Transparant zijn betekent ook een open en eerlijke communicatie over zaken die onbedoeld anders lopen dan gepland. Als daarbij persoonsgegevens in het geding zijn, spreken we van een datalek. Het gaat bij een datalek om situaties waarbij een onrechtmatige verwerking van persoonsgegevens heeft

plaatsgevonden of kan plaatsvinden. Maar ook om situaties waarbij persoonsgegevens verloren zijn gegaan of waarin gegevens in handen kunnen komen of zijn gekomen van derden die geen toegang tot die gegevens mogen hebben.

Wanneer een datalek heeft plaatsgevonden en het waarschijnlijk is dat dit datalek leidt tot een risico voor de betrokkenen, dient dit binnen 72 uur te worden gemeld bij de toezichthouder, de AP. En – wanneer de risico's hoog worden geacht – ook aan de betrokkenen zelf. De gemeente Hellendoorn heeft een vastgestelde procedure datalekken waarin is beschreven op welke wijze datalekken binnen de gemeente worden afgehandeld. Tevens is er een intern register van datalekken waarin alle geconstateerde beveiligingsincidenten worden geregistreerd.

3.6 Rechten van betrokkenen

Betrokkenen van wie de gemeente persoonsgegevens verwerkt, hebben volgens de wet bepaalde rechten waarmee zij controle kunnen uitoefenen op de verwerking van hun gegevens. De gemeente Hellendoorn ondersteunt betrokkenen in het uitoefenen van hun rechten en draagt er zorg voor dat zij op een laagdrempelige manier aanspraak op hun rechten kunnen maken. Daarbij gaat het in de dagelijkse praktijk (vooral) om de volgende rechten:

- recht op inzage: dat is het recht van mensen om onder meer een kopie te ontvangen van de persoonsgegevens die van hen worden verwerkt;
- recht op vergetelheid: mensen hebben het recht om 'vergeten' te worden. Het wissen van gegevens is echter niet altijd mogelijk, bijvoorbeeld als wetgeving een minimale bewaartermijn verplicht stelt;
- recht op rectificatie en aanvulling: het recht om de persoonsgegevens die wij als gemeente verwerken te laten wijzigen;
- het recht om bezwaar te maken tegen de gegevensverwerking;
- recht op overdraagbaarheid van gegevens in een gestructureerde, gangbare en machine-leesbare vorm (wanneer dat praktisch mogelijk is);
- ten slotte hebben mensen recht op duidelijke informatie over wat er met hun persoonsgegevens wordt gedaan: waarvoor worden ze gebruikt, met wie worden ze gedeeld, etc.

Er is een procedure rechten van betrokkenen aanwezig waarin is beschreven op welke wijze verzoeken van betrokkenen binnen de gemeente Hellendoorn worden afgehandeld. De procedure waarborgt een tijdige afhandeling van de verzoeken. De gemeente heeft vanaf ontvangst van het verzoek 1 maand de tijd om het verzoek te behandelen, met de mogelijkheid dit te verlengen. Op de gemeentelijke website staat een aanvraagformulier.

3.7 Privacy by design en privacy by default

Bij de verwerking van persoonsgegevens worden de principes van 'privacy by design' en 'privacy by default' consequent toegepast. Privacy by design houdt in dat we bij de ontwikkeling van (nieuwe) producten en diensten zo vroeg mogelijk aandacht besteden aan het beschermen van persoonsgegevens. Hoe later in het proces nog dingen moeten worden ingepast, hoe lastiger (en duurder) het vaak wordt. Privacy by default houdt in dat de instellingen van een programma standaard worden ingesteld op de meest privacy vriendelijke manier. Op die manier zorgen we ervoor dat alleen de persoonsgegevens worden verzameld en verwerkt die écht noodzakelijk zijn, en laten we gebruikers zelf actief kiezen of ze gebruik willen maken van mogelijkheden die verder gaan dan dat.

3.8 Uitvoering data protection impact assessment (dpia)

Wanneer nodig voeren we een zogeheten data protection impact assessment (dpia) uit. Een dpia oftewel gegevensbeschermingseffectbeoordeling is een toetsing vooraf van nieuwe verwerkingen. Met een dpia worden de privacyrisico's in kaart gebracht en benoemen we maatregelen om die risico's te beheersen en te beperken. De dpia is verplicht als een verwerking – in het bijzonder een verwerking waarbij nieuwe technologieën worden gebruikt – een hoog risico inhoudt voor de rechten en vrijheden van de betrokkenen. De AP heeft inmiddels ook een lijst gepubliceerd voor verwerkingen waarbij een dpia altijd verplicht is.

De gemeente beschikt over een standaard model voor de uitvoering van een dpia. Proceseigenaren zijn verantwoordelijk voor de uitvoering van een dpia. De privacy officer en/of - ambassadeur ondersteunt en adviseert bij de uitvoering hiervan. De FG geeft advies over de uitgevoerde dpia. Zijn de risico's in kaart gebracht en komen we tot de conclusie dat er geen maatregelen zijn waarmee de risico's worden beperkt? Dan is overleg met de AP vereist voordat we met de verwerking mogen starten.

3.9 Inschakeling verwerkers, verwerkersovereenkomst

Gemeenten doen natuurlijk niet alles zelf. Maar al te vaak worden de verwerkingen uitgevoerd door derde partijen zoals andere overheidsorganisaties, semi-overheidsorganisaties en particuliere bedrijven. Steeds wanneer de gemeente het verwerken van persoonsgegevens 'uitbesteedt', zullen we goede afspraken moeten maken over de wijze waarop dit gebeurt en welke verplichtingen daarbij in acht genomen moeten worden. De gemeente schakelt enkel verwerkers in die afdoende garanties bieden voor een zorgvuldige verwerking overeenkomstig de AVG.

De afspraken worden schriftelijk vastgelegd in een verwerkersovereenkomst, onderlinge regeling of een gegevensuitwisselingsovereenkomst. We hanteren daarvoor de modellen van de VNG. In overleg met partijen kan een ander model worden gehanteerd, mits dit voldoet aan de eisen van de AVG. De gemaakte afspraken worden periodiek of steekproefsgewijs getoetst. Persoonsgegevens worden alleen doorgegeven aan een bedrijf of vestiging in een land buiten de Europese Economische Ruimte (EER), als deze doorgifte aantoonbaar rechtmatig is.

3.10 Beveiliging van persoonsgegevens

Voor de veilige verwerking van persoonsgegevens is een stevig IT fundament nodig. De AVG spreekt over "passende technische en organisatorische maatregelen, rekening houdend met de stand van de techniek". Beveiliging is dan ook altijd maatwerk. Hoe groter de privacyrisico's kunnen zijn, hoe beter de persoonsgegevens beveiligd moeten worden. Daarbij kijken we in ieder geval naar maatregelen die nodig zijn om:

- de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de gemeentelijke verwerkingssystemen en diensten te garanderen;
- bij een incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig te kunnen herstellen;
- met vaste regelmaat te testen of de genomen beveiligingsmaatregelen nog steeds effectief genoeg zijn, waarbij gebruik wordt gemaakt van een plan-do-check-act-cyclus.

Op grond van de AVG moeten we als gemeente kunnen aantonen dat we persoonsgegevens goed hebben beveiligd. Daarvoor is een actueel beveiligingsbeleid essentieel.

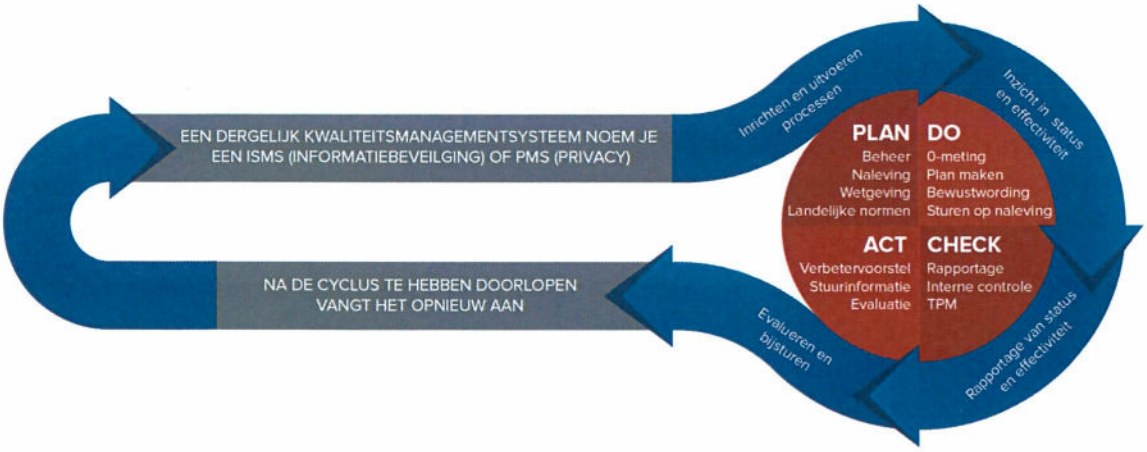
3.11 Veilig en vaardig werken: stimulering iBewustzijn

Privacybescherming en informatieveiligheid is veel meer dan ICT: het gaat in veel gevallen om de mens in de organisatie en de manier waarop deze met informatie(systemen) en de daaraan verbonden risico's omgaat. De mens is voor hackers nog altijd de makkelijkste, goedkoopste en snelste weg naar succes. Technologische ontwikkelingen zorgen er bovendien voor dat we op andere, vaak digitale, manieren omgaan met informatie. Zo werken we steeds meer tijd-, plaats- en apparaatonafhankelijk. Bij deze vrijheden horen ook nieuwe verantwoordelijkheden.

In onze informatiesamenleving wordt iBewustzijn en veilig en vaardig werken daarom steeds belangrijker. Het is noodzakelijk dat alle medewerkers de juiste instelling hebben ten aanzien van privacy en Informatieveiligheid. Houding en gedrag zullen daarom periodiek door middel van 'awareness'-campagnes en -trainingen beïnvloed moeten worden om medewerkers bewust te maken van het belang van privacy en informatieveiligheid, bekwaam te maken en om hun eigen rol daarin te kunnen vervullen. Nieuwe medewerkers krijgen binnen drie maanden een introductietraining.

3.12 Verantwoordingsplicht (accountability)

Een van de belangrijkste uitgangspunten van de AVG is het principe van accountability: organisaties die persoonsgegevens verwerken hebben een verantwoordingsplicht. Dit houdt in dat het enkel voldoen aan de privacywetgeving niet voldoende is; we zullen te allen tijde actief moeten kunnen aantonen dat wij compliant zijn en voldoen aan de privacywetgeving. Als gemeente zullen we dus zoveel mogelijk - zo niet alles - moeten documenteren. De gemeente moet daartoe een 'passend gegevensbeschermingsbeleid' opstellen met technische en organisatorische maatregelen om te waarborgen én aan te tonen dat de gegevensverwerking in overeenstemming met de geldende wet- en regelgeving wordt uitgevoerd. Getroffen maatregelen dienen continu te worden geëvalueerd en indien nodig geactualiseerd. Het implementeren van de informatiebeveiliging is dan ook geen eenmalige activiteit, maar een herhalend proces waarvoor structurele aandacht nodig is.



4. Organisatie, taken en verantwoordelijk-heden

Om het beleid op het gebied van privacybescherming gedegen vorm te kunnen geven en in de organisatie op zowel bestuurlijk als ambtelijk niveau te borgen heeft de gemeente een aantal rollen ingericht en verantwoordelijkheden belegd. Naast een aantal specifieke rollen, heeft iedere medewerker de verantwoordelijkheid om (privacy)gevoelige gegevens te beschermen en leidinggevenden om daarop te sturen en bewustzijn over privacy-aangelegenheden te creëren. Medewerkers, bestuur en management worden daarin ondersteund door de FG en de PO, waarbij op het gebied van informatieveiligheid nauw wordt samengewerkt met de gemeentelijke CISO.

4.1 Bestuurlijke organisatie

Het college van B&W van de gemeente Hellendoorn draagt als eigenaar van gemeentelijke informatieprocessen en -systemen de bestuurlijke verantwoordelijkheid voor een passend niveau van privacybescherming. De AVG spreekt in dit verband over verwerkingsverantwoordelijke. Voor alle gegevensverwerkende processen rond de uitgifte van waardedocumenten heeft de burgemeester daarnaast op basis van de Paspoortwet en het Reglement Rijbewijzen een eigen verantwoordelijkheid. Het college c.q. de burgemeester stelt de beleidskaders vast en stimuleert het management om alle noodzakelijke beschermingsmaatregelen te nemen.

Over de uitvoering van het beleid legt het college binnen de jaarlijkse P&C-cyclus verantwoording af aan de Gemeenteraad. Via het budgetrecht van de raad bepaalt de gemeenteraad bovendien de financiële kaders waarbinnen aan de privacy verplichtingen invulling gegeven moet worden. Daarnaast heeft de raad een specifieke verantwoordelijkheid rondom de eigen informatiehuishouding.

4.2 Management

Het bestuur is verantwoordelijk voor de kaderstelling; het management voor de sturing binnen deze bestuurlijke kaders. De ambtelijke organisatie werkt vanuit het principe van integraal management. Uitgangspunt daarbij is dat de manager verantwoordelijkheid draagt voor zowel de resultaten van het primaire proces als voor de ondersteunende processen, zoals Financiën, P&O, inkoop én informatieveiligheid en privacy. Het is de taak van de lijnmanager als procesverantwoordelijke om afwegingen te maken in hoeverre bepaalde risico's acceptabel zijn. Specialistische functies als FG, CISO en PO spelen een ondersteunende en adviserende rol als deskundige op het gebied van privacy en als coördinator van de centraal te treffen beschermingsmaatregelen.

In praktische zin betekent dit dat het management verantwoordelijk is voor de implementatie en het uitdragen van de maatregelen uit het privacybeleid binnen het eigen team. De manager beoordeelt op basis van een expliciete risicoafweging of voor specifieke informatiestromen aanvullende beveiligingsmaatregelen nodig zijn. Daarnaast stuurt het management op privacy-bewustzijn en de naleving van geldende wet- en (interne) regelgeving. En spreekt medewerkers waar nodig aan op geconstateerd onzorgvuldig gedrag. Management en medewerkers kunnen daarbij terugvallen op de eigen privacy ambassadeur(s).

4.3 Verantwoordelijkheid medewerkers

Onbewust menselijk handelen is de belangrijkste bedreiging voor de gemeentelijke informatie-voorziening. Ongewenste, onbewuste acties blijken een groter risico voor de privacy van burgers dan bewuste en gerichte aanvallen. De mens is daarmee een belangrijke schakel in het geheel van privacybescherming. Iedere medewerker binnen de gemeentelijke organisatie is verantwoordelijk voor alle aspecten van privacy en informatieveiligheid binnen de eigen invloedssfeer. Dat betekent onder andere de verplichting tot:

- het vertrouwelijk houden van informatie en wachtwoorden en andere vormen van toegangs-codes in het bijzonder;
- het raadplegen van (persoons) gegevens strikt te beperken tot hetgeen voor een juiste uitoefening van de eigen taken en verantwoordelijkheden noodzakelijk is;
- het op een veilige manier gebruiken van ICT middelen overeenkomstig de daarvoor geldende afspraken en procedures;
- het onmiddellijk doorgeven van elk vermoeden van het optreden van een datalek of ander privacy-incident aan de direct leidinggevende en de FG of CISO.

Informatie over privacy en informatieveiligheid is voor alle medewerkers toegankelijk via het gemeentelijke intranet.

5. Tot besluit

Dit privacy beleid dient door het lijnmanagement uitgewerkt te worden in specifiek uitvoeringsbeleid, nadere richtlijnen en/of werkinstructies. Minimaal één keer per jaar, of eerder indien daar aanleiding toe is, wordt dit privacy beleid geëvalueerd en indien nodig aangepast.

Hellendoorn, 19 december 2023.

Burgemeester en Wethouders van Hellendoorn:

de secretaris,

A.M. Ouwehand

de burgemeester

J. Eijbersen

De burgemeester van Hellendoorn:

J. Eijbersen

Bijlagen

Checklist 1: Wat zijn de plichten van de verwerkingsverantwoordelijke?

De AVG stelt dat elke verwerking van persoonsgegevens moet voldoen aan de volgende beginselen:

- de verwerking van persoonsgegevens moet rechtmatig, behoorlijk en transparant zijn;
- de verwerking moet gebonden zijn aan specifieke verzameldoelen ("doelbinding");
- de persoonsgegevens moeten toereikend zijn, ter zake dienend, en beperkt tot wat noodzakelijk is ("minimale gegevensverwerking");
- de gegevens moeten juist zijn;
- de gegevens mogen niet langer worden bewaard dan nodig ("opslagbeperking");
- gegevens moeten goed beveiligd zijn en vertrouwelijk blijven ("integriteit en vertrouwelijkheid").

De verwerkingsverantwoordelijke is verantwoordelijk voor de naleving van deze beginselen en moet dit ook kunnen aantonen. Concreet betekent dit dat de verwerkingsverantwoordelijke:

- een register van verwerkingsactiviteiten bij moet houden (de registerplicht);
- een functionaris voor de gegevensbescherming (FG) aan moet stellen;
- voorafgaande aan risicovolle verwerkingsactiviteiten een gegevensbeschermingseffectbeoordeling uit moet voeren;
- de Autoriteit Persoonsgegevens onder bepaalde omstandigheden voorafgaand aan een nieuwe risicovolle verwerkingsactiviteit moet raadplegen (de voorafgaande raadpleging);
- bij het inrichten van verwerkingen rekening dient te houden met het principe van privacy door ontwerp en standaardinstellingen (privacy by design & default);
- technische en organisatorische beveiligingsmaatregelen moet treffen die een passend beschermings-niveau bieden met het oog op het risico van de gegevensverwerking voor betrokkenen;
- in het geval van een (ernstig) datalek melding moet doen bij de Autoriteit Persoonsgegevens en onder bepaalde omstandigheden ook bij de betrokkenen;
- schriftelijke afspraken moet maken met verwerkers;
- medewerking moet verlenen aan de Autoriteit persoonsgegevens bij de uitvoering van diens taken.

Ten slotte dient de verwerkingsverantwoordelijke de rechten van de betrokkenen te respecteren en in te vullen.

Checklist 2: Wat zijn de plichten van de verwerker?

De belangrijkste verplichtingen uit de AVG voor de verwerker zijn:

- de verwerker mag voor de verwerking alleen handelen in opdracht van de verwerkingsverant-woordelijke en de overeengekomen schriftelijke afspraken over de verwerkingsactiviteiten naleven (met uitzondering van beslissingen over niet-essentiële middelen);
- de verwerker wordt verplicht een overzicht bij te houden van alle categorieën verwerkingsactiviteiten die hij in opdracht van de verwerkingsverantwoordelijke (heeft) verricht (registerplicht);
- de verwerker moet technische en organisatorische beveiligingsmaatregelen nemen die een passend beschermingsniveau bieden met het oog op het risico van de gegevensverwerking voor betrokkenen;
- de verwerker mag geen sub-verwerkers inschakelen zonder algemene of specifieke schriftelijke

toestemming van de verwerkingsverantwoordelijke;
- de verwerker moet de verwerkingsverantwoordelijke zonder onredelijke vertraging op de hoogte stellen van een datalek;
- de verwerker moet medewerking verlenen aan de Autoriteit persoonsgegevens bij de uitvoering van diens taken;
- de verwerker moet in bepaalde gevallen een functionaris voor de gegevensbescherming (FG) aanstellen.

Checklist 3: Welke informatie moeten we verstrekken aan betrokkenen?

Betrokkenen hebben recht op informatie. Organisaties dienen de informatie, zoals hieronder opgesomd, op een duidelijke manier te verstrekken aan betrokkenen. Dat kan bijvoorbeeld door het publiceren van een (online) privacyverklaring.

- de naam en contactgegevens van de organisatie;
- indien een functionaris voor de gegevensbescherming (FG) is aangesteld, de contactgegevens van deze functionaris;
- de specifieke doelen waarvoor persoonsgegevens worden verwerkt;
- de grondslag(en) waarop de verwerking is gebaseerd;
- wanneer de verwerking is gebaseerd op de grondslag 'gerechtvaardigd belang': aangeven wat het gerechtvaardigd belang is;
- wanneer de verwerking is gebaseerd op de grondslag 'wettelijke verplichting': aangeven of de betrokkene verplicht is die persoonsgegevens te verstrekken en wat de gevolgen zijn van het niet verstrekken van die persoonsgegevens voor de betrokkene;
- wanneer de verwerking is gebaseerd op de grondslag 'noodzakelijk is voor de uitvoering of het aangaan van een overeenkomst': aangeven of de betrokkene verplicht is die persoonsgegevens te verstrekken en wat de gevolgen zijn van het niet verstrekken van die persoonsgegevens voor de betrokkene;
- de eventuele ontvangers of categorieën ontvangers van de gegevens;
- in geval van doorgifte van persoonsgegevens aan landen buiten de EER:
    - of er een adequaatheidsbesluit van de Commissie bestaat,
    - of passende waarborgen zijn getroffen, welke dit zijn en of hier een kopie van kan worden verkregen, dan wel waar die waarborgen kunnen worden geraadpleegd;
- de bewaartermijn, of als dat niet mogelijk is de criteria voor het bepalen ervan;
- de rechten van de betrokkene;
- in het geval van toestemming, dat de betrokkene die toestemming altijd weer kan intrekken;
- dat de betrokkene het recht heeft een klacht in te dienen over de verwerking bij de AP

Verder moet alle andere informatie worden verstrekt die noodzakelijk is om tegenover de betrokkene een behoorlijke en transparante verwerking te waarborgen. Als een organisatie de persoonsgegevens voor andere doelen verder gaat verwerken, moet de betrokkene opnieuw worden geïnformeerd over dat nieuwe doel.

Checklist 4: Eisen aan de verwerkersovereenkomst

In een verwerkersovereenkomst dienen tenminste de volgende zaken te worden vermeld:

- het onderwerp en de duur van de verwerking;
- de aard en het doel van de verwerking;
- het soort persoonsgegevens en de categorieën van betrokkenen;
- de rechten en verplichtingen van de verwerkingsverantwoordelijke.

Verder dient in de overeenkomst te worden bepaald dat de verwerker:

- de persoonsgegevens alleen verwerkt onder de schriftelijke instructies van de verwerkingsverantwoordelijke, onder andere voor wat betref de doorgifte van persoonsgegevens aan een land buiten de EER of een internationale organisatie (tenzij de verwerker wettelijk verplicht is persoonsgegevens te verwerken);
- waarborgt dat de toegang tot die gegevens is beperkt tot gemachtigde personen. Deze personen moeten gebonden zijn aan geheimhouding op grond van een overeenkomst of een wettelijke verplichting;
- een passend niveau van beveiliging van de persoonsgegevens hanteert;
- de verwerkingsverantwoordelijke, voor zoveel mogelijk, door middel van technische en organisatorische maatregelen ondersteuning biedt bij het nakomen van diens verplichtingen met het oog op beantwoording van verzoeken rondom de rechten van betrokkenen;
- de verwerkingsverantwoordelijke, rekening houdende met de aard van de verwerking en de informatie waarover de verwerker beschikt, bijstaat bij het nakomen van diens verplichtingen op het gebied van de beveiliging van persoonsgegevens en de meldplicht datalekken;
- na beëindiging van de overeenkomst de in opdracht van de verwerkingsverantwoordelijke verwerkte persoonsgegevens wist of teruggeef, en bestaande kopieën verwijdert;
- de verwerkingsverantwoordelijke alle informatie ter beschikking stelt die nodig is om aantoonbaar te maken dat de verplichtingen op grond van de AVG rondom het inzetten van een verwerker worden nageleefd en die nodig is om audits mogelijk te maken;
- afspraken met betrekking tot sub-verwerkers maakt.