CVDR

Officiële uitgave van Haren.

Nr.
CVDR612214_1
9 januari
2019

Privacybeleid Gemeente Haren

Het college van burgemeester en wethouders van de gemeente Haren;
gelezen het voorstel van de Functionaris voor de Gegevensbescherming van 23 mei 2018;
besluit
vast te stellen het **Privacybeleid Gemeente Haren**.

1. Algemeen

De gemeente Haren verwerkt persoonsgegevens. Dat doet zij binnen de kaders van de Wet bescherming persoonsgegevens (Wbp) die per 25 mei 2018 wordt vervangen door de Algemene verordening gegevensbescherming (AVG) en de Nederlandse Uitvoeringswet AVG (UAVG). De AVG verplicht de gemeente Haren onder meer om persoonsgegevens te verwerken op een wijze die ten aanzien van de betrokkene rechtmatig, behoorlijk en transparant is, en voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Dit privacybeleid is een invulling van artikel 24 lid 2 van de AVG, dat van verwerkingsverantwoordelijken vereist om een passend gegevensbeschermingsbeleid uit te voeren. In dit privacybeleid werkt de gemeente Haren uit hoe zij persoonsgegevens verwerkt en op welke wijze zij waarborgt dat de gegevens conform de vereisten van de AVG en UAVG verwerkt worden
Dit beleid geldt voor alle medewerkers, tijdelijke inhuur en externe partijen. Het is voor alle medewerkers eenvoudig beschikbaar via een aantal media zoals intranet, internet en Scienta (ISMS).

1.1 Inleiding

Dit privacybeleid is vastgesteld door het college van burgemeester en wethouders van de gemeente Haren. Onderhoud van het privacybeleid en periodieke toetsen zijn noodzakelijk om het bereikte niveau te handhaven, te verhogen én voorbereid te zijn op de AVG. Om privacy zo concreet mogelijk te maken beperkt het beleid zich tot onderwerpen die binnen de gemeente Haren noodzakelijk zijn voor het waarborgen van een zorgvuldige omgang met persoonsgegevens, overwegingen bij keuzes en de concrete maatregelen. De concrete maatregelen worden indien nodig in de bijlagen toegevoegd. Zie hiervoor dus ook de beschikbare verordeningen, protocollen en procedures. Bij het opstellen van het beleid is zoveel mogelijk vermeden dat privacywetgeving wordt herhaald of niet concreet wordt. De volledige tekst van de AVG is onder meer te vinden op de website van de Autoriteit Persoonsgegevens. De verordening gegevensverstrekking basisregistratie personen en het reglement verwerking persoonsgegevens sociaal domein blijven onverkort van kracht.
Het beleid omvat het geheel van maatregelen die kaders en waarborgen scheppen voor de verwerking van persoonsgegevens. Het biedt een kader dat de organisatie helpt bij vragen en veranderingen: wat is ons beleid, doen we wat we in ons beleid hebben gezegd te doen en hoe kunnen we verbeteringen doorvoeren?

1.2 Reikwijdte en doelstelling van het beleid

Doelstelling van dit privacybeleid is:

- Compliant zijn met de Nederlandse en Europese wetgeving.
- Houvast bieden om nieuwe wetgeving zoals de AVG en de UAVG te implementeren.
- Een kader bieden om (toekomstige) verwerkingen van persoonsgegevens te toetsen aan een vastgesteld kader.
- Taken, bevoegdheden en verantwoordelijkheden die betrekking hebben op de verwerking van persoonsgegevens voor iedereen duidelijk te beleggen.
- Richtlijnen geven hoe om te gaan met persoonsgegevens en verwerkingen daarvan.
- Normen stellen met betrekking tot de bescherming van persoonsgegevens en privacywetgeving.

Dit beleid gaat alleen over de verwerking van persoonsgegevens van burgers/cliënten. De verwerking van gegevens van medewerkers uit hoofde van de werkgever-werknemersrelatie wordt niet in dit privacybeleid behandeld. Beleid hiervoor valt onder verantwoordelijkheid van de betreffende afdeling P&O.

1.3 Voor wie is dit beleid bedoeld?

Het beleid heeft drie doelen. Het is in eerste instantie bedoeld voor allen die betrokken zijn bij de verwerking van persoonsgegevens binnen de gemeente Haren. In feite wordt van alle personen die persoonsgegevens verwerken of beleid maken verwacht dat zij behoorlijk en zorgvuldig handelen. Ieder draagt een verantwoordelijkheid die past bij zijn niveau en rol. Zo wordt bijvoorbeeld van een ‘gewone’ medewerker niet verwacht dat deze beveiligingslekken opspoort en dicht. Wel mag van deze medewerker

worden verwacht dat hij signalen doorgeeft aan een afdelingsmanager of het Team ICT. Hierin worden de volgende categorieën onderscheiden:

- Directeur/gemeentesecretaris
- Afdelingsmanagers en teamcoördinatoren
- Medewerkers

In tweede instantie is het beleid bedoeld als uitgangspunt voor beleidsmakers en beslissers. Niet alleen gaat het om organisatorische keuzes, ook inkopers en ICT-medewerkers moeten in dit beleid kaders en handvatten vinden. Wanneer een nieuw systeem wordt aangekocht /geïmplementeerd of een afdeling een nieuwe dienst wil ontwikkelen, biedt dit beleid handvatten om privacy by design toe te passen en vanaf het begin te werken volgens de wet. Het beleid kan ook helpen bij het uitvoeren van Data Protection Impact Assessments (DPIA's).
Als derde, tot slot, vormt het beleid een vertrekpunt voor audits, periodieke onderzoeken en om aantoonbaar aan de toepasselijke wet- en regelgeving te voldoen.

2. Rollen en verantwoordelijkheden

2.1 Aantoonbaar AVG compliant met het privacybeleid als basis

Het college van burgemeester en wethouders van de gemeente Haren stelt gegevensbeschermingsbeleid op. Dit beleid omvat het voorliggende privacybeleid en verder alle documenten, processen, besluiten enz. die onderdeel maken van het geheel van passende en organisatorische maatregelen die waarborgen en waarmee aangetoond kan worden dat de verwerkingen in overeenstemming met de AVG worden uitgevoerd.
De AVG stelt in artikel 5 lid 2 dat de verwerkingsverantwoordelijke, in dit geval de gemeente, verantwoordelijk is voor de naleving van de in artikel 5 lid 1 AVG genoemde eisen, en tevens dat de verwerkingsverantwoordelijke dat kan aantonen. Artikel 24 lid 1 AVG bepaalt dat de verwerkingsverantwoordelijke passende technische en organisatorische maatregelen moet treffen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG wordt uitgevoerd. Deze maatregelen moeten worden geëvalueerd en indien nodig geactualiseerd.
Onderdeel van dergelijke maatregelen is het uitvoeren van een passend gegevensbeschermingsbeleid. De gemeente Haren voorziet in deze verplichting door het opzetten, inrichten en uitvoeren van het onderhavige privacybeleid.
Uitgangspunt voor alle verwerkingen van persoonsgegevens is dat de gemeente zich houdt aan de verplichtingen inzake dataminimalisatie en doelbinding en daarbij de beginselen van proportionaliteit en subsidiariteit in acht neemt.

2.2 Rollen en verantwoordelijkheden

Voor een goede toepassing van de AVG is het noodzakelijk om vast te stellen welke rol diverse, bij de verwerking van persoonsgegevens betrokken partijen innemen en welke verantwoordelijkheden daaruit voortvloeien. Hierbij zijn de definities uit de AVG bepalend.

Term AVG	Inhoud begrip
verwerkingsverantwoordelijke	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.
verwerker	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de verwerkingsverantwoordelijke persoonsgegevens verwerkt.
andere verwerker of subverwerker	Wanneer een verwerker een derde inschakelt om namens de verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten, wordt deze derde aangeduid als 'andere verwerker'. Deze 'andere verwerker' wordt ook vaak aangeduid als 'subverwerker'. Deze laatste term geeft aan dat een ketenverantwoordelijkheid met verschillende partijen kan ontstaan. De AVG spreekt over een 'andere verwerker'.
derde	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de betrokkene, noch de verwerkingsverantwoordelijke, noch de verwerker, noch de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of de verwerker gemachtigd zijn om de persoonsgegevens te verwerken.
ontvanger	Een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een derde, aan wie/waaraan de persoonsgegevens worden verstrekt
betrokkene	De geïdentificeerde of identificeerbare natuurlijke persoon naar wie de verwerkte persoonsgegevens te herleiden zijn.

Verwerkingsverantwoordelijke

Het college van burgemeester en wethouders van de gemeente Haren is 'verwerkingsverantwoordelijke' in de zin van de AVG omdat het college bepaalt voor welke doeleinden en met welke middelen persoonsgegevens worden verwerkt door de gemeente. Door de opzet en structuur van de gemeente Haren is sprake van delegatie van de uitvoering van de verwerking van persoonsgegevens aan verschillende afdelingen/personen binnen de gemeente.
De verwerkingsverantwoordelijke heeft ten aanzien van de verwerking van persoonsgegevens dus een bepalende rol en stelt het privacybeleid vast. Afdelingsmanagers, medewerkers en andere onderdelen

van de gemeente vallen met betrekking tot de privacy onder het gezag van de verwerkingsverantwoordelijke en zij opereren binnen de kaders die hen worden gesteld.

Verwerker

Voor zover de gemeente de verwerking van persoonsgegevens uitbesteedt aan een derde die in opdracht van en volgens de instructies van de gemeente opereert, is deze derde aan te merken als een verwerker. Een verwerker verwerkt persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke, zonder dat hij aan diens rechtstreekse gezag onderworpen is. De verwerking van persoonsgegevens moet wel de primaire opdracht zijn van de ingeschakelde derde. Met andere woorden, zijn dienstverlening moet gericht zijn op het verwerken van persoonsgegevens ten behoeve van de verwerkingsverantwoordelijke. Wanneer de verwerking van persoonsgegevens niet zijn primaire opdracht is, maar het een uitvloeisel is van een andere vorm van dienstverlening, dan is de betreffende derde als dienstverlener zélf de verwerkingsverantwoordelijke voor deze verwerking. Oftewel, het enkele feit dat een derde een opdracht krijgt van de verwerkingsverantwoordelijke is niet voldoende om te kunnen spreken van verwerkerschap; de opdracht moet gericht zijn op het verwerken van persoonsgegevens.

Een goed voorbeeld is een administratiekantoor dat namens een organisatie de salarisadministratie voert. De opdracht aan het administratiekantoor is het uitvoeren van de salarisadministratie, wat neerkomt op het verwerken van de persoonsgegevens van de medewerkers. In dit geval is het administratiekantoor verwerker. Een ander voorbeeld is een aanbieder van gegevensopslag in de cloud. Wanneer de dienst puur ziet op het opslaan van gegevens, dan is de cloudaanbieder een verwerker. Een handelsinformatiebureau dat bedrijven in staat stelt om de kredietwaardigheid van consumenten te beoordelen is daarentegen meestal géén verwerker. De opdracht is immers 'beoordeel voor mij de kredietwaardigheid van deze consument'. Hoewel bij de beoordeling van de kredietwaardigheid weliswaar persoonsgegevens worden gebruikt en het handelsinformatiebureau opdrachtnemer is, bepaalt het handelsinformatiebureau zelf hoe zij de opdracht uitvoert en welke gegevens zij daar eventueel voor aanwendt (doel en middelen). Het handelsinformatiebureau is daarmee zelf verwerkingsverantwoordelijke en niet verwerker. Een ander voorbeeld is het aanbieden van online diensten. Wanneer een cloudaanbieder bijvoorbeeld een fitness app aanbiedt aan bedrijven om medewerkers gezond en fit te houden en deze app verwerkt daartoe de gegevens van medewerkers, dan is de cloudaanbieder verwerkingsverantwoordelijke. Een laatste voorbeeld betreft zorgaanbieders die in opdracht van een gemeente zorg leveren. Zij doen dit weliswaar in opdracht van de gemeente, maar bepalen zelf doel en middelen voor de concrete invulling van hun zorgtaken. Een verwerker heeft geen zeggenschap over de verwerkingen en mag alleen handelen onder de verantwoordelijkheid van de verwerkingsverantwoordelijke en naar diens instructies. Op het moment dat de verwerker zelfstandig beslissingen gaat nemen over de doelen van de verwerking en de middelen, dan wordt deze zelf verantwoordelijk voor die (nieuwe) verwerkingen[1].

Subverwerker

Van subverwerkers is sprake wanneer de verwerker andere verwerkers inschakelt. Deze laatste term geeft aan dat een ketenverantwoordelijkheid met verschillende partijen kan ontstaan. De AVG spreekt over een 'andere verwerker' en stelt hier eisen aan in artikel 28 AVG.

Gedeelde verantwoordelijkheid binnen de organisatie

Onder de verantwoordelijkheid van de gemeente Haren kunnen ondersteunende of aanvullende werkmaatschappijen, serviceproviders of gemeenschappelijke regelingen vallen. De algemene bepalingen van dit privacybeleid zijn ook op hen van toepassing. Zij vallen direct onder de verantwoordelijkheid, alleen of in gezamenlijkheid, van de deelnemende partijen.

Het zorgvuldig en goed omgaan met persoonsgegevens is een verantwoordelijkheid van de verwerkingsverantwoordelijke. Hieronder valt ook het instrueren en informeren van medewerkers, het goed uitvoeren van getroffen maatregelen en het aanpassen van procedures. Vanuit hun gedeelde verantwoordelijkheid spreken de organisatieonderdelen elkaar aan wanneer door nalatigheid of onzorgvuldig handelen de kwaliteit van maatregelen lager wordt dan afgesproken.

Gezamenlijke verwerkingsverantwoordelijken

Wanneer de verwerkingsverantwoordelijke samen met anderen het doel en middelen van gegevensverwerkingen bepaalt, dan is er sprake van gezamenlijke verantwoordelijkheid. Dit is bijvoorbeeld het geval als de gemeente uit hoofde van een samenwerkingsconvenant samen met de andere bij dat convenant betrokken partijen bepaalt hoe en waarom er persoonsgegevens worden verwerkt.

Artikel 26 van de AVG bepaalt dat bij gezamenlijke verantwoordelijkheid de partijen onderling duidelijke afspraken moeten maken over wie invulling geeft aan de diverse rechten en plichten uit de AVG. Het is met name van belang dat de betrokkene weet waar hij terecht kan om zijn rechten uit te oefenen. Ongeacht de afspraken tussen de gezamenlijke verwerkingsverantwoordelijken blijven zij jegens betrokkenen hoofdelijk aansprakelijk voor de naleving van de AVG.

1) Tekst afkomstig uit Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming van het Ministerie van Justitie en Veiligheid, paragraaf 3.5.1.

2.3 Beleid inzake de interne organisatie

Het college van burgemeester en wethouders van de gemeente Haren heeft voor de verwerking van persoonsgegevens een intern beheerder aangesteld. Dit volgt de lijnen van de interne organisatie, waarbij iedere leidinggevende verantwoordelijkheden heeft op zijn eigen niveau. De verantwoordelijkheden en organisatie-inrichting volgen de lijnen van de procuratieregeling.

Privacy en personeel

Onder de term personeel worden diegenen bedoeld die door de gemeente Haren conform artikel 1 van de Ambtenarenwet zijn aangesteld als ambtenaar in algemene dienst. Zij zijn uit hoofde van hun functie reeds verplicht tot geheimhouding.

Onderdeel van organisatorische beveiligingsmaatregelen is het bewustzijn van personeel met betrekking tot de wet- en regelgeving inzake de bescherming van persoonsgegevens. Communicatie naar het personeel en het inzetten van bewustwordingsprogramma's op het gebied van privacybescherming is dan ook een belangrijk actiepunt met als doel te groeien naar een privacybewuste organisatiecultuur en het aantal datalekken vanuit menselijk handelen te minimaliseren. Specifieke aandacht aan het onderwerp wordt gegeven na incidenten, bij vragen die breed leven of zodra (intern) onderzoek laat zien dat bijscholing nodig is. Bewustwording is een doorlopend programma van lange adem en de inzet/effectiviteit met de benodigde middelen van dit instrument behoort jaarlijks te worden geëvalueerd. Voorts is een privacyprotocol nodig waarin gedragsregels staan hoe om te gaan met het verwerken van persoonsgegevens zoals het verstrekken van gevoelige gegevens aan collega's en derden. Dit protocol behoort kenbaar te worden gemaakt aan iedereen en persoonlijk te worden overhandigd bij elke nieuwe aanstelling of externe inhuur. Een belangrijk uitgangspunt voor dit protocol is het opnemen van een zekere terughoudendheid met het verstrekken van persoonsgegevens aan collega's en aan derden.

Relatie met anderen

De gemeente Haren werkt samen in regionaal verband. Zo kent de gemeente Haren onder andere samenwerkingen op het gebied van zorg en veiligheid. De gemeente Haren dient zorg te dragen dat zij afdoende afspraken maakt met deze samenwerkingspartners, die veelal samen met de gemeente als gezamenlijk verantwoordelijken kunnen worden aangemerkt, om de privacy te waarborgen.

2.4 Beleid inzake leveranciers en verwerkers

Algemeen beleid t.a.v. externe leveranciers

Wanneer een contractuele overeenkomst wordt aangegaan met externe leveranciers dan gelden de Algemene Inkoopvoorwaarden van de gemeente Haren. Deze zijn vastgesteld door de verwerkingsverantwoordelijke, i.c. het college van burgemeester en wethouders.

Overeenkomsten voor levering van ICT-diensten- en apparatuur

Wanneer sprake is van ICT-diensten en/of -apparatuur dan gelden aanvullende voorwaarden, te weten de meest recente versie van de Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT). Leveranciers zijn gehouden aan geheimhouding.

Overeenkomsten met verwerkers

Wanneer voor de uitvoer van een overeenkomst persoonsgegevens worden verwerkt dan geldt de externe leverancier als verwerker. De verwerking van persoonsgegevens moet wel tot de primaire opdracht van de leverancier behoren. In deze gevallen worden aanvullende bepalingen opgenomen in een verwerkersovereenkomst. Verwerkers verwerken persoonsgegevens in opdracht van de gemeente Haren. Alleen verwerkers die afdoende garanties bieden ten aanzien van de bescherming van persoonsgegevens worden ingehuurd. Met alle verwerkers wordt een verwerkersovereenkomst gesloten. In deze verwerkersovereenkomst maakt de gemeente Haren in ieder geval afspraken over:

- De aard, het doel en de duur van de uit te voeren verwerking van persoonsgegevens, met een nadere beschrijving van de soorten persoonsgegevens en de categorieën van betrokkenen;
- Afspraken over het door de verwerker inhuren van andere verwerkers (subverwerkers);
- Technische en organisatorische beveiligingsmaatregelen;
- Afspraken over geheimhouding en vertrouwelijkheid;
- Doorgifte van persoonsgegevens naar het buitenland;
- Verdeling van verantwoordelijkheden met de gemeente Haren als verwerkingsverantwoordelijke en de opdrachtnemer als verwerker;
- Wanneer en hoe persoonsgegevens vernietigd worden;
- Afspraken over het afhandelen van verzoeken aangaande de rechten van een betrokkene;
- Afspraken over heronderhandeling en beëindiging, inclusief de verplichting van de verwerker om bij een beëindiging van de overeenkomst de gegevens aan de gemeente terug te leveren.

Gebruik verwerkersovereenkomst van verwerker

Wanneer een verwerker een eigen voorstel voor een verwerkersovereenkomst heeft, kan besloten worden deze overeenkomst aan te houden. In deze gevallen wordt de overeenkomst getoetst op minimaal de volgende elementen. Afwijken van deze criteria kan alleen in overleg met de Functionaris

Gegevensbescherming (hierna: FG) en na toestemming van het college van burgemeester en wethouders van de gemeente Haren. Opgenomen zijn in ieder geval bepalingen:

- De gemeente Haren verwerkt bijzondere gegevens: de verwerker is zich hiervan bewust en treft maatregelen die passend zijn bij deze categorie persoonsgegevens.
- Het is verwerkers niet toegestaan gegevens te verwerken voor andere doelen dan is bepaald in de overeenkomst.
- De verwerker handelt alleen in opdracht van en conform de instructies van de gemeente Haren.
- De verwerker is aansprakelijk voor eventuele schade aan de gemeente Haren of aan personen van wie persoonsgegevens zijn verwerkt, voor zover ontstaan door zijn werkzaamheden of (nalaten van) handelen en die van de door hem ingeschakelde subverwerkers.
- De verwerker treft passende maatregelen en is bij voorkeur ISO 27001 gecertificeerd en kan een informatiebeveiligingsplan overleggen.
- De gemeente Haren heeft het recht ter plekke onderzoek uit te (laten) voeren door (externe) deskundigen.
- Bij datalekken meldt een verwerker deze datalekken direct, bij voorkeur binnen maximaal 24 uur na ontdekking, neemt actie om lekken te dichten en werkt samen met de gemeente Haren om gevolgen te beperken.
- Bij datalekken bij een verwerker worden toezichthouders en/of betrokkenen uitsluitend door de gemeente Haren geïnformeerd.
- Vastgesteld wordt of een verwerker subverwerkers (AVG: andere verwerkers) mag inschakelen. Subverwerkers mogen na schriftelijke toestemming worden ingeschakeld, zolang ze gevestigd zijn binnen de EU, de gegevens alleen binnen de EU verwerkt worden, deze derde partijen minimaal eenzelfde niveau van beveiliging hebben als de verwerker dient te treffen en ook overigens minimaal voldoen aan de verplichtingen die voor verwerker gelden uit hoofde van de met de gemeente Haren gesloten verwerkersovereenkomst.
- Persoonsgegevens worden niet buiten de EU opgeslagen. Dit geldt ook voor cloudopslag. Het college van burgemeester en wethouders van de gemeente Haren kan na advies van de FG een uitzondering toestaan.
- Wanneer een verwerker gevestigd is buiten de EU dan heeft de verwerker een vertegenwoordiger in de EU aangewezen.
- De verwerker houdt een overzicht bij van alle categorieën persoonsgegevens die in opdracht van het college van burgemeester en wethouders van de gemeente Haren worden verwerkt.
- Indien daartoe verplicht op grond van de AVG stelt de verwerker een FG aan en stelt hier het college van burgemeester en wethouders van de gemeente Haren van op de hoogte.

2.5 Beleid inzake derden

De gemeente Haren gaat zorgvuldig om met persoonsgegevens van ingezetenen/cliënten en overige betrokkenen, zoals bezoekers van de websites, deelnemers aan diensten waarbij persoonsgegevens bij de gemeente Haren terecht komen. Dit is onder andere beschreven in de privacyverklaring en de cookiebepaling welke op de website van de gemeente Haren zijn terug te vinden.
De gemeente Haren maakt voor wat betreft de beschermende maatregelen geen onderscheid tussen ingezetenen en niet-ingezetenen. Het (hoge) niveau van beschermende maatregelen wordt overal toegepast.

2.6 Functionaris voor gegevensbescherming

De gemeente Haren heeft conform de verplichting daartoe op grond van artikel 37 AVG een functionaris voor gegevensbescherming (FG) aangesteld.
De FG ziet toe op de volgende organisatieonderdelen en verwerkingsactiviteiten:

- De FG informeert en adviseert de gemeente over haar verplichtingen uit hoofde van de wet- en regelgeving.
- De FG ziet toe op de naleving van:
  - privacywet- en regelgeving.
  - het privacybeleid, speciaal de toewijzing van verantwoordelijkheden en audits.
- De FG is verplicht desgevraagd een advies over een privacy impact assessment (PIA) te geven en ziet toe op de uitvoering van zijn advies.
- De FG ziet toe op de bewustmaking en de opleiding van het bij de verwerking betrokken personeel.
- De FG kan verantwoordelijk zijn voor het beheren van documentatie en registers zoals:
  - het register van de verwerkingsactiviteiten.
  - het register datalekken.

De taken van de FG zijn, naast de wettelijke taken:

- Het ontwikkelen van Interne regelingen.
- Adviseren over technologie en beveiliging (privacy by design).
- Input leveren bij het opstellen of aanpassen van een gedragscode.
- Meldingen van gegevensverwerkingen bijhouden.
- Vragen en klachten van mensen binnen en buiten de organisatie afhandelen.

De FG stelt jaarlijks een jaarverslag op.

3 Beleid voor rechtmatig en zorgvuldige verwerking van persoonsgegevens

3.1 Inleiding uitgangnspunten van een rechtmatige verwerking

Uit de AVG vloeit een aantal verplichtingen voort voor de gemeente als verwerkingsverantwoordelijke. De voornaamste verplichtingen zijn nader beschreven in de thema's van dit hoofdstuk.

3.2 Verwerkingsregister

Melding bij de Autoriteit Persoonsgegevens vervangen door interne registerplicht

De verwerkingen van de gemeente Haren zijn gemeld bij de AP. Met de komst van de AVG is deze externe meldplicht vervangen door een interne registratieplicht. Artikel 30 AVG vereist namelijk dat de gemeente een register moet opstellen en bijhouden van alle verwerkingsactiviteiten die onder de verantwoordelijkheid van de gemeente plaatsvinden. Dit verwerkingsregister moet minimaal de volgende gegevens bevatten:

- De naam en contactgegevens van de verwerkingsverantwoordelijke en, eventuele gezamenlijke verwerkingsverantwoordelijken, alsmede van de functionaris voor de gegevensbescherming;
- De verwerkingsdoeleinden;
- Een beschrijving van de categorieën van betrokkenen (bijvoorbeeld burgers/ingezetenen of werknemers) en van de categorieën persoonsgegevens;
- Een beschrijving van de categorieën van ontvangers van de persoonsgegevens aan wie de persoonsgegevens zijn of zullen worden verstrekt;
- Indien van toepassing: een beschrijving van eventuele doorgifte van persoonsgegevens aan een derde land of internationale organisatie en eventueel documenten met betrekking tot passende waarborgen;
- Indien mogelijk, de beoogde termijnen waarbinnen de verschillende categorieën van persoonsgegevens moeten worden gewist;
- Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.

De gemeente geeft uitvoering aan deze verplichting door het bijhouden van een verwerkingsregister in vooralsnog een Excelsheet, maar zodra er deze beschikbaar is in Scienta.

Risicovolle verwerking soms voorafgaand melden

Vanaf 25 mei 2018 is de gemeente Haren verplicht een Data Protection Impact Assessment (DPIA) uit te voeren als een verwerking mogelijk een hoog risico inhoudt voor rechten en vrijheden van de betrokkenen. Als uit de DPIA blijkt dat de verwerking inderdaad een hoog risico oplevert en de gemeente Haren geen maatregelen neemt of kan nemen om dit risico te beperken, dan moet de verwerking voor toepassing eerst worden voorgelegd aan de AP (de zogeheten voorafgaande raadpleging zoals beschreven in artikel 36 AVG).

3.3 Transparantie

De gemeente Haren is transparant over hoe ze persoonsgegevens verwerkt. Hierdoor weten burgers en personen die benaderd worden wie de gemeente Haren is, dát ze persoonsgegevens verwerkt, waarom dit gebeurt en welke maatregelen de gemeente Haren treft om zorgvuldig met gegevens om te gaan.

De belangrijkste manieren om betrokkenen te informeren over de verwerking van persoonsgegevens zijn:

- algemene voorwaarden bij inschrijven;
- additionele informatie bij het aanvragen van specifieke diensten;
- alle websites geven, indien vereist, een cookie melding en hebben een privacyverklaring inclusief cookiebepaling;
- de gemeente Haren biedt laagdrempelige mogelijkheden om inzage te krijgen in de verwerking van persoonsgegevens. Zie hiervoor ook het kopje ‘

Betrokkenen worden in ieder geval geïnformeerd over:

- de identiteit en contactgegevens van de verantwoordelijke en van de FG;
- de doeleinden en rechtsgrond(en) van de gegevensverwerking;

- indien van toepassing: de ontvangers of categorieën ontvangers van de persoonsgegevens;
- indien van toepassing, nadere informatie met betrekking tot eventuele doorgifte van persoonsgegevens naar een derde land of internationale organisatie;
- informatie inzake bewaartermijnen;
- informatie over de rechten van betrokkenen.

Indien de gegevens niet van de betrokkenen zelf zijn verkregen, moet ook informatie gegeven worden over de categorieën van persoonsgegevens die verwerkt worden. Zie ook de informatie in hoofdstuk 3.7 over de rechten van betrokkenen.

3.4 Doelbinding

Met doelbinding wordt bedoeld dat gegevens alleen worden verwerkt voor het doel waarvoor ze verzameld zijn. En als gegevens toch voor andere doelen worden gebruikt, wordt beoordeeld of dit niet te ver afstaat van dat doel.
De gemeente Haren verwerkt alleen gegevens voor de doelen waarvoor ze van burgers gekregen zijn. In paragraaf 3.3 Transparantie is aangegeven hoe en wanneer personen op de hoogte worden gesteld van de verwerking van persoonsgegevens. De organisatie zorgt ervoor dat de persoonsgegevens alleen voor deze doelen worden verwerkt. Wanneer de wens ontstaat om persoonsgegevens voor andere doelen te verwerken wordt daar waar nodig een DPIA uitgevoerd, om de vraag te beantwoorden of de verwerking 'niet onverenigbaar is' met het oorspronkelijke doel. Dit vereiste volgt uit artikel 5 lid 1 sub b en artikel 6 lid 4 AVG.
De gemeente verwerkt alleen de persoonsgegevens die minimaal noodzakelijk zijn voor het vooraf bepaalde doel. De gemeente streeft naar minimale gegevensverwerking. Waar mogelijk worden minder of geen persoonsgegevens verwerkt.
Voor het bereiken van het doel waarvoor de persoonsgegevens worden verwerkt, wordt inbreuk op de persoonlijke levenssfeer van de betrokken burger zoveel mogelijk beperkt (subsidiariteit).
De gegevensverwerking is te allen tijde proportioneel. Dit houdt in dat de inbreuk op de persoonlijke levenssfeer van de betrokkene niet onevenredig is in verhouding met het door middel van de verwerking te bereiken doel.

3.5 Rechtmatige grondslag

De gemeente Haren mag alleen persoonsgegevens verwerken wanneer hier een grondslag voor bestaat. De gemeente Haren verwerkt gegevens van haar burgers, geïnteresseerden, en bezoekers van haar websites veelal op basis van wettelijke taken, in het kader van de vervulling van taken van algemeen belang en in het kader van de uitoefening van openbaar gezag. In sommige gevallen verwerkt zij gegevens ter uitvoering van een overeenkomst of op basis van toestemming. Zodra een persoon is ingeschreven worden de gegevens verwerkt conform de wettelijke bepalingen vanuit in de Basisregistratie Personen (BRP). Ook voor andere publiekrechtelijke taken is de gemeente verplicht de BRP te gebruiken. Ten aanzien van de onlineactiviteiten verwerkt de gemeente Haren persoonsgegevens ter uitvoering van wettelijke verplichtingen (informatievoorzieningen aan het publiek), of op basis van een 'gerechtvaardigd belang' en in sommige gevallen op basis van toestemming (bijvoorbeeld voor het plaatsen van toestemmingsplichtige cookies).
De gemeente Haren verwerkt vanuit haar wettelijke taken per definitie bijzondere persoonsgegevens. Dit is opgenomen in het register van de verwerkingsactiviteiten. De gemeente is tevens wettelijk verplicht om BSN te verwerken, onder meer uit hoofde van de Wet algemene bepalingen Burgerservicenummer (Wabb) en de Wet Basisregistratie Personen (Wet BRP). Dit is in overeenstemming met het bepaalde in artikel 87 AVG en artikel 46 UAVG. Verwerking van BSN dient wel altijd proportioneel te zijn.

3.6 Kwaliteit van gegevens

De gemeente Haren treft maatregelen om de kwaliteit van gegevens te borgen. Onder kwaliteit wordt verstaan dat gegevens juist, nauwkeurig en actueel zijn. Voordat gegevens worden verwerkt vinden (geautomatiseerde) controles plaats om onjuiste benadering van personen te voorkomen doordat gegevens niet juist zijn.
In ieder geval zijn de volgende maatregelen getroffen:
- Bij de invoer van gegevens vindt een kwaliteitscontrole plaats door het verifiëren van gegevens.
- ICT-systemen valideren gegevens door middel van invoercontroles en validaties.
- ICT-systemen zijn daar waar persoonsgegevens worden gebruikt direct of indirect gekoppeld aan de Basis Registratie Personen zodat altijd wordt beschikt over de actuele gegevens.
- Burgers/cliënten hebben de mogelijkheid gegevens in te zien en te corrigeren indien nodig.

3.7 Rechten van de betrokkene

Personen van wie er persoonsgegevens worden verwerkt hebben een aantal rechten. Deze rechten zijn geregeld in artikel 12 t/m 22 AVG. Voor een deel zijn dit nieuwe rechten en voor een deel zijn het rechten die ook al onder de Wbp bestonden die nu (veelal in strengere vorm) in de AVG terugkomen.

Het gaat om de volgende rechten, die hierna één voor één worden beschreven:

A. het recht op informatie
B. het recht op inzage
C. het recht op rectificatie
D. het recht op vergetelheid (het wissen van gegevens)
E. het recht op beperking van de verwerking
F. het recht op dataportabiliteit
G. het recht van bezwaar
H. het recht zich te verzetten tegen geautomatiseerde besluitvorming (inclusief geautomatiseerde besluitvorming op basis van profiling)

Betrokkenen worden gewezen op hun rechten in de privacyverklaring dat op de website is geplaatst en in de informatie die nieuwe ingezetenen/cliënten krijgen. Zij kunnen hun rechten uitoefenen waarbij het college van burgemeester en wethouders van de gemeente Haren waarborgt dat verzoeken correct en tijdig worden afgehandeld.

Algemene beperkingen voor rechten van betrokkenen

Naast beperkingen die per specifiek recht gelden (daarover hieronder meer), is er ook een aantal algemene beperkingen die van toepassing zijn op alle rechten van betrokkenen. Deze zijn te vinden in artikel 23 AVG en variëren van een beperking die noodzakelijk is vanwege nationale veiligheid en openbare orde, voorkoming en opsporing van strafbare feiten etc. tot de beperking 'ter bescherming van de betrokkene *of de rechten en vrijheden van anderen*'. Onder 'anderen' moet ook de verwerkingsverantwoordelijke worden begrepen. Een dergelijke beperking is nu ook in de Wbp opgenomen.

A. Het recht op informatie

Het recht van een betrokkene op informatie is een uitwerking van het transparantiebeginsel neergelegd in artikel 5 van de AVG. Persoonsgegevens moeten worden verwerkt op een wijze die ten aanzien van de betrokkene transparant is. De betrokkene moet dus informatie ontvangen omtrent hoe zijn persoonsgegevens worden verwerkt tenzij de betrokkene deze informatie al heeft. Aan deze verplichting wordt doorgaans voldaan doormiddel van een privacyverklaring die op een duidelijke plek op de website wordt gepubliceerd. Zo'n verklaring is echter niet verplicht, de informatie mag ook op een andere manier verstrekt worden. Op de privacyverklaring hoeft bovendien geen akkoord te worden gevraagd. Het betreft een plicht tot informeren.

Hoe moet de informatie verstrekt worden?

De AVG stelt een aantal algemene eisen aan de informatieverstrekking. Deze moet beknopt, transparant en begrijpelijk zijn. Het is dus niet de bedoeling dat dit een ellenlang technisch en/of juridisch document wordt. Het moet begrijpelijk zijn voor de lezer en het moet afgestemd zijn op de doelgroep, in het bijzonder wanneer de informatie voor een kind bestemd is.

Daarnaast moet deze gemakkelijk toegankelijk zijn en in duidelijke en eenvoudige taal zijn geschreven volgens de verordening. Het ligt voor de hand om vast te houden aan het Europees referentiekader voor de talen en de tekst te schrijven op bijvoorbeeld taalniveau B1.

Ten slotte moet de informatie zonder daarvoor kosten in rekening te brengen worden verstrekt.

Welke informatie moet verstrekt worden?

Het recht op informatie wordt door de AVG in twee verschillende situaties onderscheidden. Welke informatie verstrekt dient te worden verschilt naar gelang de persoonsgegevens bij de betrokkene zelf worden verzameld dan wel wanneer deze persoonsgegevens niet van de betrokkene zijn verkregen maar elders vandaan komen. In onderstaand overzicht is weergegeven welke informatie in de twee verschillende situaties moet worden verstrekt.

	Persoonsgegevens rechtstreeks verkregen van betrokkene (artikel 13 AVG)	Persoonsgegevens niet rechtstreeks verkregen van betrokkene (artikel 14 AVG)
De identiteit en contactgegevens van de verwerkingsverantwoordelijke, en wanneer van toepassing die van zijn vertegenwoordiger en functionaris voor gegevensbescherming.	x	x
Het doel van de verwerking en de rechtsgrond waar deze op gebaseerd is	x	x
De gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde wanneer van toepassing (indien de verwerking gebaseerd is op artikel 6 lid 1 onder f AVG)	x	x
De betrokken categorieën van persoonsgegevens		x
Indien van toepassing alle ontvangers of categorieën van ontvangers van persoonsgegevens	x	x
Indien gegevens worden doorgegeven naar buiten de EU, informatie hierover waaronder in het bijzonder: of en welke waarborgen er zijn en hoe hier een kopie van verkregen kan worden of waar deze geraadpleegd kunnen worden	x	x
De bewaartermijn van de persoonsgegevens of indien dit niet mogelijk is op voorhand te zeggen de criteria die gebruikt worden om deze termijn te bepalen.	x	x

Informatie over het recht van betrokkene op inzage, rectificatie, wissing of beperking, het recht tegen de verwerking bezwaar te maken en het recht op dataportabiliteit	x	x
Het recht om toestemming voor de verwerking in te trekken (wanneer van toepassing).	x	x
Het recht om een klacht in te dienen bij een toezichthoudende autoriteit.	x	x
De bron waar de persoonsgegevens vandaan komen en, indien van toepassing, of zij uit een openbare bron komen.		x
Of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten, en of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt.	x	
het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.	x	x

Met 'persoonsgegevens rechtstreeks verkregen van betrokkene' worden bijvoorbeeld bedoeld de gegevens die door een gebruiker worden verstrekt in een webformulier of bij inschrijving in de gemeente. Persoonsgegevens die niet rechtstreeks van de betrokkene verkregen worden zijn bijvoorbeeld gegevens die door een derde partij verzameld worden en aan de verwerker verstrekt worden. Waar precies de scheidslijn ligt tussen deze twee gevallen onder de AVG is nog onduidelijk maar te verwachten is dat deze niet anders is dan onder de oude wetgeving.
Onder de Wbp was het volgens de AP zo dat voor de eerste categorie de betrokkene zelf, actief zijn persoonsgegevens ter beschikking stelt dan wel een vertegenwoordiger dit namens hem doet. Maar let op: camerabeelden verkregen door kenbaar (niet-heimelijk) cameratoezicht vallen bijvoorbeeld ook onder de categorie persoonsgegevens rechtstreeks verkregen van betrokkene. Er is sprake van kenbaar cameratoezicht indien betrokkene op de hoogte is van dat toezicht en weet voor welk doel deze beelden gebruikt worden.
Wanneer moet de informatie verstrekt worden?
In het geval van de eerste categorie (persoonsgegevens worden rechtstreeks verkregen van de betrokkene) dient de informatie aan de betrokkene verstrekt te worden op het moment van verkrijging. In dit geval kan bijvoorbeeld op het formulier verwezen worden naar de privacyverklaring.
Indien de gegevens op een andere manier verkregen worden dient de informatie binnen een redelijke termijn, maar in ieder geval binnen een maand verstrekt te worden. Als de data gebruikt wordt om te communiceren met de betrokkene in ieder geval wanneer het eerste contact plaatsvindt en als men voornemens is de data door te sturen aan een andere ontvanger, dan in ieder op het moment wanneer deze data wordt verstrekt.
Op de informatieplicht is een belangrijke uitzondering, te weten: indien het verstrekken van de informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen. Het is denkbaar dat persoonsgegevens worden verwerkt die niet meteen herleidbaar zijn tot contactinformatie. Bijvoorbeeld IP-adressen of MAC-adressen. In een dergelijk geval zou het waarschijnlijk onevenredig veel inspanning vergen om contact om te nemen met de betrokkene. Uitgezocht zou immers moeten worden hoe de persoon achter een IP-adres bereikt kan worden. Een vrijwel onmogelijke taak indien er dagelijks duizenden van deze persoonsgegevens verwerkt worden. De AVG schrijft echter wel voor dat er in dit geval passende maatregelen worden getroffen om de rechten, vrijheden en gerechtvaardigde belangen van de betrokkene te waarborgen. In ieder geval zal de informatie openbaar gemaakt moeten worden en gepubliceerd moeten worden. De aangewezen plek lijkt hiervoor eveneens de privacyverklaring.

B. Het recht van inzage

Een betrokkene heeft het recht om van de verwerkingsverantwoordelijke antwoord te krijgen op de vraag of er hem betreffende persoonsgegevens verwerkt worden en zo ja, inzicht te krijgen in welke gegevens dit dan zijn. Hij heeft bovendien recht op enige aanvullende informatie.
Het recht van inzage past net als het recht op informatie in de doelstelling van transparantie van de AVG. Een betrokkene moet kunnen nagaan of hem betreffende persoonsgegevens worden verwerkt en of dit gebeurt in lijn met de plichten die uit de AVG voortvloeien. Met andere woorden: of deze verwerking rechtmatig plaatsvindt. Het recht op inzage is bovendien bedoeld om de uitoefening van de overige rechten (rectificatie, vergetelheid, beperking en portabiliteit) voortvloeiend uit de AVG mogelijk te maken dan wel te vergemakkelijken.
Welke gegevens moeten worden verstrekt?
Er moet allereerst antwoord gegeven worden op de vraag of er persoonsgegevens van de verzoeker verwerkt worden. Indien dit het geval is dient hij inzicht te krijgen in welke gegevens dit dan zijn. Hij heeft bovendien recht op enige aanvullende informatie:

- De verwerkingsdoeleinden;
- De betrokken categorieën;
- De ontvangers of categorieën van ontvangers aan wie de persoonsgegevens zijn of zullen worden verstrekt, met name ontvangers in derde landen of internationale organisaties;
- Indien mogelijk, de periode gedurende welke de persoonsgegevens naar verwachting zullen worden opgeslagen, of indien dat niet mogelijk is, de criteria om die termijn te bepalen;

- Dat de betrokkene het recht heeft de verwerkingsverantwoordelijke te verzoeken dat persoonsgegevens worden gerectificeerd of gewist, of dat de verwerking van hem betreffende persoonsgegevens wordt beperkt, alsmede het recht tegen die verwerking bezwaar te maken;
- Dat de betrokkene het recht heeft klacht in te dienen bij een toezichthoudende autoriteit;
- Wanneer de persoonsgegevens niet bij de betrokkene worden verzameld, alle beschikbare informatie over de bron van die gegevens;
- Het bestaan van geautomatiseerde besluitvorming, met inbegrip van profilering, en, ten minste in die gevallen, nuttige informatie over de onderliggende logica, alsmede het belang en de verwachte gevolgen van die verwerking voor de betrokkene.

Wanneer persoonsgegevens worden doorgegeven aan een land buiten de EU of een internationale organisatie, heeft de betrokkene bovendien het recht in kennis te worden gesteld van de passende waarborgen die overeenkomstig de AVG zijn genomen.

Hoe moeten deze gegevens verstrekt worden?

Het Europese Hof van Justitie heeft in 2014 uitgemaakt dat het recht van inzage niet zo ver gaat dat hele administraties integraal overlegd dienen te worden. Artikel 15 lid 3 AVG bepaalt echter dat de verwerkingsverantwoordelijke de betrokkenen een kopie dient te verstrekken van de persoonsgegevens die worden verwerkt. Het is dus twijfelachtig of kan worden volstaan met het verstrekken van een overzicht van de persoonsgegevens die verwerkt worden. Het is vaak ook makkelijker om de gegevens volledig aan de betrokkene te verstrekken. Aan het recht van inzage (en dat van wijziging, verwijdering en beperking) zou bijvoorbeeld kunnen worden voldaan door de betrokkene toegang te geven tot een beveiligd gedeelte op een website/portal waar hij (bijvoorbeeld via DigiD) zijn gegevens in kan zien en (indien van toepassing) kan aanpassen. Dit ligt bovendien in lijn met het beginsel van privacy by design. De informatie dient in een gangbare elektronische vorm te worden verstrekt, tenzij het verzoek op papier is gedaan of indien de betrokkene expliciet om een papieren kopie verzoekt. De informatie dient kosteloos te gebeuren tenzij de aanvrager om meerdere kopieën verzoekt. In dat geval mogen daarvoor redelijke administratiekosten worden gerekend.

Beperkingen

Zoals hierboven al vermeld, erkent de AVG dat rechten en vrijheden van anderen in het geding kunnen komen door een inzageverzoek. Het recht van privacy houdt op waar dat van een ander begint. In sommige gevallen zal het recht van inzage dus beperkt worden door de rechten van anderen. Denk hierbij bijvoorbeeld aan een inzageverzoek die tot onevenredige administratieve lasten leidt voor de verwerkingsverantwoordelijke. Of camerabeelden waar twee personen tegelijkertijd weergegeven worden. Deze beelden kunnen niet zonder meer verstrekt worden aan degene die het inzageverzoek doet. Een oplossing zou kunnen zijn om de tweede persoon onherkenbaar te maken.

C. Het recht op rectificatie

De betrokkene heeft onder de AVG het recht om van de verwerkingsverantwoordelijke onverwijld rectificatie van hem betreffende onjuiste persoonsgegevens te verkrijgen. Met inachtneming van de doeleinden van de verwerking heeft de betrokkene het recht 'vervollediging' van onvolledige persoonsgegevens te verkrijgen.

Een betrokkene moet het recht hebben om hem betreffende persoonsgegevens te laten rectificeren. Dit houdt in dat fouten of omissies hersteld zullen moeten worden zodat zij corresponderen met de werkelijkheid. Het betreft geen absoluut recht om elk gegeven in elk systeem naar wens aan te (laten) passen. Het kan gaan om een situatie dat persoonsgegevens in eerste instantie verkeerd zijn opgenomen: denk bijvoorbeeld aan een naam die verkeerd is ingevoerd. Of om gegevens die wijzigen: denk hierbij bijvoorbeeld aan iemand die zijn wettelijke naam wijzigt.

Doorgeven van de rectificatie

De verwerkingsverantwoordelijke stelt iedere ontvanger aan wie persoonsgegevens zijn verstrekt, in kennis van elke rectificatie van persoonsgegevens.

D. Recht op vergetelheid (het wissen van gegevens)

De betrokkene heeft het recht van de verwerkingsverantwoordelijke zonder onredelijke vertraging wissing van hem betreffende persoonsgegevens te verkrijgen.

De betrokkene heeft dus het recht om vergeten te worden. Dit recht om vergeten te worden wordt echter door de AVG wel begrensd en is slechts van toepassing is specifieke in de verordening omschreven gevallen. Er is dus geen absoluut en onvoorwaardelijk recht om vergeten te worden.

Gevallen waarin het recht van vergetelheid van toepassing is

- de persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt.
    - Deze grond voor verwijdering hangt nauw samen met het beginsel van opslagbeperking. Het is op grond van de AVG de bedoeling dat gegevens verwijderd worden wanneer zij niet meer bewaard hoeven te worden voor de doeleinden waarvoor zij zijn verkregen

- de betrokkene trekt de toestemming waarop de verwerking berust (indien de rechtsgrond voor verwerking toestemming is) in, en er is geen andere rechtsgrond voor de verwerking;

- Indien er bijvoorbeeld (inmiddels) een gerechtvaardigd belang is of een wettelijke plicht is om de gegevens te verwerken zullen de gegevens niet gewist hoeven te worden.

- de betrokkene maakt bezwaar tegen de verwerking op grond van een overheidstaak of het eigen gerechtvaardigd belang, en er zijn geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking, of de betrokkene maakt bezwaar tegen de verwerking in geval van direct marketing.
  - Let er op dat in het geval de persoonsgegevens worden gebruikt voor direct marketing zij altijd gewist moeten worden in geval er bezwaar wordt gemaakt.

- de persoonsgegevens zijn onrechtmatig verwerkt.
  - Indien er op de een of andere manier in strijd gehandeld wordt met de AVG. Bijvoorbeeld indien er niet is voldaan aan de algemene informatieverplichtingen uit artikel 12, 13 en 14 AVG.

- de persoonsgegevens moeten worden gewist om te voldoen aan een in Europees of nationaal recht neergelegde wettelijke verplichting die op de verwerkingsverantwoordelijke rust;
  - Wanneer er op de verwerker een andere wettelijke plicht rust om de gegevens te verwijderen en dit is niet gebeurd dan moet dit alsnog gebeuren op verzoek van de betrokkene.

- de persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij aan een kind.
  - De AVG stelt extra eisen aan de verwerking van persoonsgegevens wanneer dit de persoonsgegevens van een kind betreffen. Dit omdat zij minder bekend zijn met de risico's en consequenties van het verstrekken van hun data. Met een dienst van de informatiemaatschappij wordt elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten wordt verricht.

Notificatieplicht
Indien de verwerkingsverantwoordelijke de persoonsgegevens openbaar heeft gemaakt moet hij, rekening houdend met de beschikbare technologie en de kosten die er mee gemoeid zijn, redelijke maatregelen treffen om anderen die deze gegevens verwerken ervan op de hoogte te stellen dat de betrokkene de verwerkingsverantwoordelijken heeft verzocht om de gegevens te wissen.
De verwerkingsverantwoordelijke zal dus actief anderen op de hoogte moeten brengen van het feit dat hij deze gegevens moet verwijderen zodat zij hetzelfde kunnen doen. Een voorbeeld: Een groot sociaal netwerk krijgt een verwijderverzoek met betrekking tot alle persoonsgegevens van een gebruiker. Zij zullen niet enkel het profiel van de gebruiker moeten verwijderen, maar ook Google op de hoogte moeten brengen van dit verwijderverzoek indien deze persoonsgegevens ook voorkomen in de zoekresultaten van Google.
Weigering van het verzoek van de betrokkene
In een aantal gevallen kan geweigerd worden te voldoen aan een verzoek van de betrokkene om gegevens te verwijderen. Dit is het geval indien de verwerking nodig is voor één van de volgende redenen:
- voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie;
- voor het nakomen van een in Europees of nationaal recht neergelegde wettelijke verwerkingsverplichting;
- voor het vervullen van een taak van algemeen belang of het uitoefenen van het openbaar gezag dat aan de verwerkingsverantwoordelijke is verleend;
- om redenen van algemeen belang op het gebied van volksgezondheid;
- met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden;
- voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

E. Recht op beperking van de verwerking
Het recht op beperking van de verwerking is een recht dat we nog niet kenden onder de Wbp. Indien een betrokkene vraagt om beperking van de verwerking van de persoonsgegevens, dan mag de verantwoordelijke de data nog wel bewaren, maar hij mag het niet meer verwerken/gebruiken. Het is wat dat betreft dus minder ver strekkend dan het recht op vergetelheid. Niet aan elk verzoek hoeft te worden voldaan. Er moet voldaan zijn aan één van de in de AVG genoemde criteria.

- de juistheid van de persoonsgegevens wordt betwist door de betrokkene. In dit geval is een beperking voor de betrokkene wenselijk zodat zijn gegevens niet verwerkt worden gedurende de periode waarin zij nog niet gecorrigeerd zijn.

- de verwerking is onrechtmatig en de betrokkene verzet zich tegen het wissen van de persoonsgegevens en verzoekt in de plaats daarvan om beperking van het gebruik ervan.
- de verwerkingsverantwoordelijke heeft de persoonsgegevens niet meer nodig voor de verwerkingsdoeleinden, maar de betrokkene heeft deze nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

Het uitgangspunt van de AVG is dat gegevens niet langer bewaard worden dan nodig. Indien een betrokkene er echter in het kader van een juridische procedure belang bij heeft dat deze gegevens niet verwerkt (wissen is een verwerking) worden.

- de betrokkene heeft bezwaar gemaakt (zie hierna) tegen de verwerking en er is nog geen antwoord/beslissing geweest op dit bezwaar.

In afwachting van de behandeling van zijn bezwaar kan een betrokkene beperking van verwerking verlangen.

Uitzonderingen voor de verwerkingsverantwoordelijke
Wanneer een betrokkene zijn recht op beperking uitoefent is dit niet absoluut. De gegevens mogen nog wel opgeslagen (ook een vorm van verwerking) worden, immers zou het anders niet verschillen van het recht van gegevenswissing. Ook kan er (deels) weer verwerking plaatsvinden indien hier specifiek toestemming voor wordt gegeven door de betrokkene. Ten slotte mogen de gegevens nog verwerkt worden voor de instelling, uitoefening of onderbouwing van een rechtsvordering of ter bescherming van de rechten van een andere natuurlijke persoon of rechtspersoon of om gewichtige redenen van algemeen belang voor de Unie of voor een lidstaat.

Informeren van de betrokkene
Indien een verwerkingsverantwoordelijke de beperking opheft, bijvoorbeeld omdat inmiddels duidelijk is dat de gegevens waarvan de juistheid werd betwist toch juist bleken of, moet de verantwoordelijke de betrokkene hiervan op de hoogte stellen.

F. Het recht op dataportabiliteit
Ook het recht op dataportabiliteit of overdraagbaarheid van gegevens is een nieuw recht onder de AVG. In de Wbp is geen soortgelijk recht te vinden. Het recht op dataportabiliteit houdt in dat een betrokkene de mogelijkheid krijgt om zijn persoonsgegevens te 'hergebruiken' bij verschillende diensten. Het geeft de betrokkene het recht een kopie te eisen die bruikbaar is bij een andere dienstverlener.

Een voorbeeld: een betrokkene houdt zijn hardlooppresta ties bij via de app Runkeeper. Hij heeft het recht zijn gegevens bij Runkeeper op te vragen in een gemakkelijk te porteren format zodat hij deze kan gebruiken bij concurrent Strava.

Beperkingen
Ook aan het recht op dataportabiliteit wordt een aantal eisen en beperkingen gesteld.

Er is slechts een recht op dataportabiliteit als aan alle hiernavolgende criteria is voldaan:

i) *Het moet gaan om persoonsgegevens rechtstreeks verkregen van betrokkene*
Dit criterium moet breed worden geïnterpreteerd. Het betreft niet slechts data die door de betrokkene wordt verstrekt in enge zin, bijvoorbeeld in een formulier. Het kan ook geen om gegevens die bij de betrokkene worden gemeten. Denk bijvoorbeeld aan data van een hartslagmeter. Ook bijvoorbeeld data die de browser van een gebruiker verstuurt valt hier waarschijnlijk onder.

ii) *De verwerking vindt plaats op grond van toestemming of op grond van de uitvoering van een overeenkomst*
Slechts indien de gegevensverwerking op één van deze twee grondslagen berust is het recht van dataportabiliteit van toepassing

iii) *De verwerking wordt verricht via automatische procedés.*
Het recht is slechts van toepassing in het geval van digitale gegevens. Gegevens op papier vallen niet onder het recht van overdraagbaarheid.

Deze vereisten zijn cumulatief. Aan alle criteria moet dus zijn voldaan voordat een recht op portabiliteit ontstaat. Dit zal vrijwel nooit het geval zijn bij verwerkingen door de gemeente Haren.
Ook is expliciet bepaald dat het recht van dataportabiliteit geen afbreuk mag doen aan de rechten van derden. Videobeelden waarin meerdere personen zijn opgenomen vallen dus niet zonder beperking onder het recht van dataportabiliteit. Ook is denkbaar dat er bijvoorbeeld een inbreuk zou worden

gemaakt op het intellectuele eigendom van een ander met een onbeperkt recht op dataportabiliteit. Er zal dus altijd kritisch gekeken moeten worden voordat gegevens verstrekt worden of de rechten van derden wellicht in het geding zijn.
Het verstrekken van de gegevens
De persoonsgegevens moeten in een gestructureerde, gangbare en machine-leesbare vorm aangeleverd worden. Denk hierbij bijvoorbeeld aan het CSV formaat. Met machine-leesbaar wordt voornamelijk bedoeld dat het informatie op een dusdanige manier is gestructureerd dat een computer specifieke elementen uit het bestand kan lezen en verwerken. Het uitgangspunt dat in het achterhoofd gehouden moet worden is dat een andere organisatie zonder onevenredig veel moeite te hoeven doen de gegevens in hun systeem kan importeren zodat de betrokkene gemakkelijk kan overstappen naar deze dienst.
De AVG stelt bovendien de eis dat deze informatie kosteloos moet worden verstrekt. Voor deze aanvullende dienst mogen dus geen kosten in rekening gebracht worden.
Indien de betrokkene het verzoekt is het in sommige gevallen zo dat de data rechtstreeks naar een andere gegevensverantwoordelijke gestuurd moet worden. Dit is het geval indien dit technisch mogelijk is. De AVG roept echter expliciet niet de plicht in het leven voor verwerkingsverantwoordelijken om te zorgen dat hun systemen compatible zijn met die van andere (concurrerende) dienstverleners. Hoe ver deze plicht dus precies reikt zal in de toekomst moeten blijken.

G. Het recht van bezwaar

Een betrokkene kan vanwege redenen die verband houden met zijn specifieke situatie gebruik maken van dit recht van bezwaar tegen de verwerking van hem betreffende persoonsgegevens, als voldaan is aan de in de AVG genoemde eisen.
Als een betrokkene bezwaar maakt moet de verwerkingsverantwoordelijke de verwerking staken, tenzij dwingende gerechtvaardigde gronden anders bepalen.
Betrokkenen hebben te allen tijde het recht om bezwaar te maken tegen de verwerking van hun persoonsgegevens in verband met de totstandbrenging of de instandhouding van een directe relatie tussen de verwerkingsverantwoordelijke of een derde en de betrokkene met het oog op werving voor commerciële of charitatieve doelen. Dit zijn uitingen van direct marketing. Denk hierbij aan mailings over acties, nieuwsbrieven of het onder de aandacht brengen van diensten van de gemeente Haren. Het overgrote deel van deze uitingen vindt via de digitale weg plaats. Het verzet zal vaak voorkomen in de vorm van het uittekenen of opt-out. Alle digitale uitingen bieden de mogelijkheid zich uit te schrijven van de uiting (opt-out).
Bezwaar ook online
Voorts vermeld dat de AVG dat in het geval van online diensten er ook een online mogelijkheid zal moeten zijn om bezwaar in te dienen. Niet volstaan kan worden met een postadres en het verzoek een brief te sturen.

H. Het recht zich te verzetten tegen geautomatiseerde individuele besluitvorming, waaronder profiling

De AVG biedt een aantal waarborgen voor personen tegen het risico dat een potentieel beschadigend besluit wordt genomen zonder menselijke tussenkomst. De betrokkene heeft op grond van artikel 22 AVG het recht om niet onderworpen te worden aan een uitsluitend geautomatiseerd besluit (waaronder geautomatiseerde besluitvorming op basis van profilering) indien hier voor hem rechtsgevolgen aan zijn verbonden of dit hem anderszins in aanmerkelijke mate treft.
Onder profiling onder de AVG wordt het volgende verstaan:
"elke vorm van geautomatiseerde verwerking van persoonsgegevens waarbij aan de hand van persoonsgegevens bepaalde persoonlijke aspecten van een natuurlijke persoon worden geëvalueerd, met name met de bedoeling zijn beroepsprestaties, economische situatie, gezondheid, persoonlijke voorkeuren, interesses, betrouwbaarheid, gedrag, locatie of verplaatsingen te analyseren of te voorspellen;"
Het recht zich te verzetten tegen geautomatiseerde besluitvorming
Er moet dus sprake zijn van:
1. een besluit dat uitsluitend is gebaseerd op geautomatiseerde verwerking waaronder besluitvorming op basis van profiling; en
2. er moeten voor de betrokkene rechtsgevolgen aan zijn verbonden of het besluit moet hem in aanmerkelijke mate treffen.

Denk hierbij bijvoorbeeld aan de situatie dat op basis van postcode en huisnummer iemand wel of niet in aanmerking komt voor een bepaalde levensverzekering, vergunning of lening.

Indien aan beide voorwaarden wordt voldaan, heeft de betrokkene in beginsel het recht om zich tegen de betreffende besluitvorming te verzetten.

Beperkingen
Het recht van verzet tegen geautomatiseerde besluitvorming is niet van toepassing wanneer het besluit:
1. Is toegestaan bij wet (en bovendien waarborgen biedt ter bescherming van rechten en vrijheden van individuen)

2. Nodig is voor de totstandkoming van een overeenkomst tussen de betrokkene en een verwerkingsverantwoordelijke
3. Berust op uitdrukkelijke toestemming van de betrokkene.

Deze laatste twee uitzonderingen zijn slechts van toepassing indien maatregelen worden getroffen door de verantwoordelijke ter bescherming van de rechten en vrijheden van betrokkene. Deze zouden ten minste moten bestaan uit: i) een recht op menselijke tussenkomst, ii) de mogelijkheid voor betrokkene om zijn standpunt kenbaar te maken en iii) het recht om het besluit aan te vechten.

Op de volgende manieren kan een betrokkene inzage krijgen in de gegevens die door de gemeente Haren worden verwerkt:
- door inzage te vragen bij Inzageverstrekker, via een van de kanalen die de gemeente Haren aanbiedt.

Afhandeling verzoeken
Wanneer iemand om inzage vraagt krijgt deze zo snel mogelijk zijn gegevens. Er moet onverwijld en in ieder geval binnen één maand na ontvangst daarvan gereageerd worden op een verzoek van een betrokkene uit hoofde van een van zijn rechten zoals hierboven opgesomd. Onder de huidige Wbp is dat vier weken.
Afhankelijk van de complexiteit van de verzoeken en van het aantal verzoeken is de initiële termijn onder de AVG indien nodig te verlengen met nog eens twee maanden. Een dergelijke verlenging dient wel binnen één maand na ontvangst van het verzoek te worden medegedeeld. Indien er geen gevolg wordt gegeven aan een verzoek dient dat uiterlijk binnen één maand te worden medegedeeld.
De gemeente Haren streeft naar beantwoording binnen 30 dagen. Eventueel wordt contact opgenomen met de betrokkene om te zien welke informatie gewenst is.
Identiteit vrager vaststellen
De identiteit van de vrager wordt vastgesteld via de procedure Identiteit vaststellen en machtigen zoals deze in het handboek Informatiebeveiliging Haren is vastgelegd. De gemeente verstrekt telefonisch geen informatie over personen.
Minderjarigheid
Verzoeken tot uitoefening van de rechten als bedoeld in artikel 15 – 22 AVG ten behoeve van een minderjarige jonger dan 16 jaar kunnen alleen door, of met toestemming van, een persoon met ouderlijk gezag worden gedaan.
Bijdrage
De gemeente Haren voldoet kosteloos aan verzoeken van betrokkenen uit hoofde van de uitoefening van hun rechten. Slechts indien verzoeken van een betrokkene kennelijk ongegrond of buitensporig zijn, met name vanwege hun repetitieve karakter, mag de gemeente Haren ofwel een redelijke vergoeding in rekening brengen in het licht van de administratieve kosten waarmee het verstrekken van de gevraagde informatie of communicatie of het treffen van de gevraagde maatregelen gepaard gaan, ofwel weigeren gevolg te geven aan

Artikel 3.8 Informatiebeveiliging

Om zorgvuldig met persoonsgegevens om te kunnen gaan moeten passende beschermende maatregelen worden getroffen. Deze maatregelen moeten de geheimhouding en beveiliging borgen. De maatregelen gelden voor allen die onder verantwoordelijkheid van het college van burgemeester en wethouders van de gemeente Haren werken: interne medewerkers, verwerkers en subverwerkers. De maatregelen gelden ook voor diensten en goederen die onderdeel zijn van de beveiliging, zoals beveiliging van het pand, de schoonmaak of leveranciers van hardware. Dit thema is een uitwerking van de artikelen 5 lid 1 sub f en 32 AVG. Uit hoofde van de meldplicht datalekken (artikel 33 AVG) zal het college van burgemeester en wethouders van de gemeente Haren een beveiligingsincident moeten melden bij de AP tenzij het niet waarschijnlijk is dat de inbreuk op de beveiliging een privacyrisico inhoudt. Dit is verder uitgewerkt in een separaat document getiteld Protocol Datalekken gemeente Haren.
Deze paragraaf werkt de volgende onderwerpen uit:
- Geheimhouding
- Informatiebeveiliging (standaardnorm)
- Informatiebeveiliging

De gemeente Haren draagt zorg voor informatiebeveiligingsmaatregelen en maatregelen die persoonsgegevens beschermen. Het betreft ook maatregelen rondom informatiebeveiliging, zoals beveiliging van het pand en een goede afvoer van vertrouwelijk materiaal.
Het Team ICT is verantwoordelijk voor de algemene informatiebeveiliging van het netwerk, basissystemen en het ICT-platform.
Geheimhouding
Dit onderdeel over geheimhouding richt zich op alle personen die onder het gezag van het college van burgemeester en wethouders van de gemeente Haren gegevens verwerken. Dit zijn de medewerkers

van de interne organisatie maar ook verwerkers en gedetacheerden. Niemand werkt voor de gemeente Haren zonder uitdrukkelijk tot geheimhouding verplicht te zijn, als onderdeel van de zorgvuldige verwerking.

Werknemers

Iedere werknemer tekent een geheimhoudingsverklaring of legt de eed/ gelofte af bij indiensttreding als onderdeel van de arbeidsovereenkomst.
Daarnaast worden medewerkers in een aantal documenten gewezen op hun geheimhoudingsplicht. Naast de geheimhoudingsplicht worden medewerkers gewezen op het belang van zorgvuldige omgang met gegevens. Dit is breder dan de omgang met persoonsgegevens, want deze gaat ook over andere uitingen.

Telewerken

De gemeente Haren biedt de mogelijkheid tot plaats-onafhankelijk werken. Hiervoor biedt ze instrumenten zoals werken via een cloudoplossing of beveiligde laptops waardoor veilig werken mogelijk wordt. Voor thuiswerken gelden dezelfde uitgangspunten als die gelden voor werken op een kantoorlocatie. De procedure is vastgelegd in de Gedragscode Telewerken (met BRP).

Geheimhouding voor specifieke rollen

Bij enkele bedrijfsfuncties worden medewerkers specifiek op hun geheimhoudingsplicht gewezen zoals bij het gebruik van Suwinet en BRP.

Leveranciers, verwerkers en andere derden

Ook verwerkers vallen onder de geheimhoudingsplicht (art. 28 lid 3 sub b AVG). Verwerkers en externen worden door middel van verwerkersovereenkomsten en contracten verplicht tot geheimhouding. Deze plicht is opgenomen in de standaard verwerkersovereenkomst. Bij alle contracten met leveranciers, verwerkers en overige externen die toegang krijgen tot het pand of de systemen, is in de contracten een bepaling over geheimhouding opgenomen.
In de standaardovereenkomst, die ook wordt gebruikt bij leveranciers, is een vergelijkbare geheimhoudingsverklaring opgenomen zoals bij verwerkers.

Informatiebeveiliging

Voor informatiebeveiliging wordt de Baseline Informatiebeveiliging voor Nederlandse Gemeenten (BIG) gebruikt. Dit is een algemeen geaccepteerde standaard voor beheer van informatiebeveiliging en te treffen maatregelen binnen gemeenten. De informatiebeveiligingsmaatregelen zullen worden opgenomen in het informatiebeveiligingsbeleid.

3.9 Beleid t.a.v. bewustwording en training

Medewerkers van de gemeente Haren worden periodiek herinnerd aan een goede en zorgvuldige omgang met persoonsgegevens. Er wordt periodiek beoordeeld en vastgesteld welke informatiebehoefte de medewerkers hebben ten aanzien van hun basisbewustzijn over de zorgvuldige omgang met persoonsgegevens en specifieke thema's. De informatie hierover kan komen uit de periodieke beoordelingen, signalen of vragen bij leidinggevenden.

3.10 Beleid inzake controle en naleving

Onder de AVG is de gemeente Haren verplicht een FG aan te stellen. Onderdeel van de taken van de FG is het toezien op de naleving door de gemeente van de verplichtingen met betrekking tot de bescherming van persoonsgegevens.
De naleving van dit beleid is de gedelegeerde verantwoordelijkheid van eenieder op zijn eigen niveau. Het college van burgemeester en wethouders van de gemeente Haren blijft eindverantwoordelijk voor alle handelingen die onder zijn verantwoordelijkheid worden uitgevoerd.

3.11 Jaarverslag

Jaarlijks wordt een privacyjaarverslag opgesteld. Hierin staan in ieder geval:

- (indien nodig) voorafgaande raadplegingen inzake verwerkingen van persoonsgegevens aan de AP conform artikel 36 AVG en verhouding van deze tot de praktijk;
- toevoegingen en aanpassingen van het privacybeleid en aanverwante documenten (zoals de privacyverklaring en de cookiebepaling), aan de hand van vigerende wet- en regelgeving;
- een overzicht van toezicht, incidenten en controles op de naleving van genomen maatregelen;
- ondernomen acties en adviezen ten aanzien van DPIA's;
- ondernomen activiteiten ten aanzien van opleidingen en awareness van medewerkers;
- een overzicht van uitgevoerde activiteiten, inclusief die van externe partijen, die naleving en kwaliteit van privacybescherming borgen en verbeteren;
- een beschrijving van de kwaliteit van naleving van privacywetgeving volgens de FG;
- alle overige relevante zaken die voor het college van burgemeester en wethouders van de gemeente Haren nodig zijn om het gevoerde beleid te kunnen beoordelen op effectiviteit en kwaliteit, en om hierop aanvullend waar nodig aanvullende of corrigerende maatregelen te kunnen treffen.

3.12 Gegevensverkeer met landen buiten de EU

Inleiding

Wanneer gegevens verwerkt worden in een land buiten de EU zijn de AVG artikelen 44 en verder van toepassing. Alle landen van de EU werken onder dezelfde verordening waarmee een zorgvuldige verwerking verondersteld wordt. Wanneer gegevens naar een land buiten de EU worden doorgegeven om daar verwerkt te worden, zal het college van burgemeester en wethouders van de gemeente Haren ook in deze situaties de wet moeten naleven en een zorgvuldige verwerking moeten borgen. Dat kan op een aantal manieren. Bijvoorbeeld doordat gegevens alleen naar een land worden doorgegeven dat een passend niveau van beveiliging kent. Een overzicht is te vinden op de site van de Europese Commissie. Vervolgens moet duidelijk zijn dat de betreffende organisatie voldoende maatregelen heeft getroffen om de persoonsgegevens te beschermen. Wanneer het betreffende land niet op de lijst voorkomt, bestaan andere mogelijkheden alsnog persoonsgegevens door te geven. Deze mogelijkheden zijn opgenomen in de betreffende AVG-artikelen. Het is de bedoeling alleen met verwerkers samen te werken die voldoende maatregelen hebben getroffen om een zorgvuldige omgang te waarborgen.

Verwerkers

Van verwerkers is bekend waar zij gegevens opslaan. Gegevens worden alleen buiten de EU opgeslagen wanneer daarover in de verwerkersovereenkomst een afspraak is gemaakt. De algemene inkoopvoorwaarden en de aanvullende GIBIT voorwaarden vormen een verplicht onderdeel in de contractuele afspraken. De locatie van de verwerking van gegevens wordt bijgehouden door de verantwoordelijke afdeling.

Cloud

Wanneer cloudopslag of cloudverwerkingen worden gebruikt wordt in alleen gekozen voor cloudservers binnen de EU.

Analytische cookies van derden

Op websites wordt gebruik gemaakt van analytische cookies. Via de afname van deze diensten kan informatie over gebruikers van de site verwerkt worden buiten de EU. Ook deze verwerking valt onder het beleid (zie boven). Hoe wordt om gegaan met de cookies wordt opgenomen in de cookiebepaling van de privacyverklaring dat op iedere Harense website benaderbaar is.

4 Beleid rondom incidenten (datalekken)

4.1 Datalekken en beveiligingsincidenten

Per 1 januari 2016 is de meldplicht datalekken van kracht (artikel 34a Wbp). In de AVG is dit opgenomen in de artikelen 33 en 34. Wanneer beveiligingsmaatregelen niet afdoende zijn gebleken en persoonsgegevens (mogelijk) zijn gelekt of verloren zijn gegaan, kan sprake zijn van een datalek. Binnen de gemeente Haren is het Protocol Datalekken Gemeente Haren van kracht. In dit proces is beschreven hoe de organisatie reageert op datalekken.

In het kort is de procedure als volgt:

1. Is sprake van een beveiligingsincident en zijn er (mogelijk) persoonsgegevens gelekt? Dan meldt een medewerker dit bij een verantwoordelijke bestuurder, of via het calamiteitennummer bij ICT of via datalek@haren.nl. Incidenten die direct worden gemeld zijn:
   - elk incident met een informatiedrager;
   - elk vermoeden dat er met de beveiliging van gegevens iets mis is.

Bij het doen van een melding moet contact tussen de personen zijn geweest. Alleen een mailtje naar de ICT-helpdesk is absoluut onvoldoende. Het moet duidelijk zijn dat de melding is ontvangen.

2. Activeer de Datalekken Commissie;

De verantwoordelijk bestuurder en manager Bedrijfsvoering overleggen en bepalen of de datalekprocedure wordt gevolgd. Zo ja, dan wordt een datalekteam geactiveerd.
In het datalekteam zitten in ieder geval de betreffende verantwoordelijk bestuurder, manager Bedrijfsvoering, de manager de afdeling waar het lek heeft plaatsgevonden, aangevuld met een communicatieadviseur en Verantwoordelijke Informatiebeveiliging.

3. Bestrijd het datalek en voer het meldingsproces uit. Meld het lek bij de AP en, na beoordeling, bij de betrokkene(n);
4. Binnen 72 uur moet een (voor-)melding bij de AP zijn gedaan;
5. Documenteer proces voor verantwoording en feedback. Gebruik hiervoor het register datalekken.

Wanneer sprake is van een datalek bij een verwerker, dan is in de verwerkersovereenkomst opgenomen dat deze de gemeente Haren zo snel mogelijk van het datalek op de hoogte stelt. Het informeren van getroffen personen wordt door de gemeente Haren uitgevoerd.

4.2 Taken verantwoordelijkheden en bevoegdheden van de functionaris voor gegevensbescherming (FG)

Deze bijlage bevat een overzicht van taken, verantwoordelijkheden en informatie over de positionering van de functionaris voor gegevensbescherming (FG).

Algemeen

Een functionaris voor gegevensbescherming (FG) is geen verlengstuk van de toezichthouder. De FG heeft bijvoorbeeld geen corrigerende bevoegdheden zoals de toezichthouder die heeft. De FG heeft een adviserende taak, ook als het gaat over het beoordelen van naleving van de Wet bescherming persoonsgegevens (Wbp) en de Algemene Verordening Gegevensbescherming (AVG). De verantwoordelijkheid voor de verwerking van persoonsgegevens conform de Wbp/AVG blijft liggen bij de verwerkingsverantwoordelijke. Wel kunnen interne afspraken en bevoegdheden worden toegekend aan een FG.

Onder de Wbp is de FG niet verplicht. Onder de AVG wordt de FG wel verplicht voor gemeenten.

Wetgeving

- Wbp: art. 62 – 64 Wbp
- AVG: art. 37 – 39 AVG

De organisatie en de positie van de FG

Hierbij gaat het om taken, verantwoordelijkheden en bevoegdheden van de verwerkingsverantwoordelijke ten opzichte van de FG.

Aanstelling en positionering

- De verantwoordelijke wijst een FG aan en positioneert deze in de organisatie:
  - de FG is een natuurlijk persoon;
  - een FG kan aangesteld worden voor een hele overheidsorganisatie. Hieronder kunnen ook samenwerkende gemeenten vallen;
  - een FG kan een personeelslid zijn;
  - een FG rol kan voltijds maar ook in deeltijd worden ingevuld
  - de rol van FG kan door een externe partij op grond van een dienstverleningsovereenkomst worden ingevuld;
  - let op: Gemeenten hebben al een privacybeheerder in dienst voor de gegevensverwerkingen op grond van de Wet basisregistratie personen (BRP). De positie van een privacybeheerder BRP zal bepaald moeten worden ten opzichte van de FG. De VNG adviseert de privacybeheerder BRP als actiehouder voor het BRP-domein te positioneren.
- Als een FG ook andere rollen en taken vervult voorkomt de verantwoordelijke belangenconflicten tussen taken en plichten.
- De verantwoordelijke wijst een FG aan op grond van zijn professionele kwaliteiten. De verantwoordelijke beoordeelt deze professionele kwaliteiten.
- De verantwoordelijke maakt de contactgegevens van de FG bekend:
  - bij contactgegevens in privacyverklaringen;
  - bij het register van de verwerkingsactiviteiten;
  - aan de Autoriteit Persoonsgegevens (AP)
  - aan de AP wanneer een voorafgaand onderzoek wordt ingesteld.
- De verantwoordelijke meldt de aanstelling van een FG aan de AP

Uitvoeren van taken

- De verantwoordelijke betrekt de FG naar behoren en tijdig bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.
- De verantwoordelijke vraagt de FG om advies bij de uitvoer van PIA's.
- De verantwoordelijke stelt benodigde middelen ter beschikking zodat de FG zijn taak naar behoren kan vervullen:
  - toegang tot persoonsgegevens;
  - toegang tot verwerkingsactiviteiten;
  - zie verder algemene auditbevoegdheden.
- De verantwoordelijke waarborgt dat het verslag van de FG direct aan de verantwoordelijke word uitgebracht.
- De verantwoordelijke stelt de benodigde middelen ter beschikking om de deskundigheid van de FG op peil te houden.
- De verantwoordelijke biedt aan betrokkenen de mogelijkheid om contact op te nemen met de FG:
  - bij vragen over de verwerking van gegevens;
  - bij het uitoefenen van hun rechten.

Beperkingen en kaders
- De verantwoordelijke voorkomt dat de FG-instructies krijgt met betrekking tot de uitvoering van taken door de FG.
- De verantwoordelijke mag de FG niet ontslaan of straffen voor de uitvoeren van zijn taken.

4.3 Taken, verantwoordelijkheden en bevoegdheden van de FG

Aanstelling en positionering
- De FG brengt rechtstreeks verslag uit aan de hoogst leidinggevende.
- De FG is gehouden aan geheimhouding en vertrouwelijkheid.
- De FG is het contactpunt van, overlegt met en werkt samen met de AP.

Uitvoeren van taken
- De FG informeert en adviseert de verantwoordelijke over zijn verplichtingen uit hoofde van de wet- en regelgeving.
- De FG ziet toe op de naleving van:
  - privacywet- en regelgeving
  - het privacybeleid, speciaal de toewijzing van verantwoordelijkheden en audit.
- De FG is verplicht desgevraagd een advies over een privacy impact assessment (PIA) te geven en ziet toe op de uitvoering van zijn advies.
- De FG ziet toe op de bewustmaking en de opleiding van het bij de verwerking betrokken personeel.
- De FG kan verantwoordelijk zijn voor het beheren van documentatie en registers zoals:
  - het register van verwerkingen;
  - het register datalekken.
- Een FG kan overwegen lid te worden van brancheorganisaties zoals het Nederlands Genootschap voor Functionarissen voor de Gegevensbescherming (NGFG).
- Een FG kan overwegen zich te laten certificeren.

Aanvullende informatie
AP en Artikel-29 werkgroep
- Themapagina FG
- Richtlijnen functionaris voor gegevensbescherming (FG)

Brancheorganisaties
- Nederlands genootschap voor functionarissen voor gegevensbescherming (NGFG)
- VNG Themapagina
- Handreiking rol en taken FG
- Handreiking positionering FG

Artikel 4.4 Positionering van de functionaris voor gegevensbescherming

Deze paragraaf maakt onderdeel uit van het privacy management systeem (PMS) van de gemeente Haren. Het bevat best practices en aandachtspunten voor de positionering van de functionaris voor gegevensbescherming (FG).

Positie moet onafhankelijke uitvoer van taken waarborgen

De FG dient in alle onafhankelijkheid zijn werkzaamheden te kunnen uitvoeren en ontvangt daarbij geen instructies vanuit de gemeente en verwerkers. Het gaat dan om instructies over bijvoorbeeld:
- het te bereiken resultaat
- de opdracht een klacht te onderzoeken
- de opdracht een toezichthouder te raadplegen.

Verder mag de FG geen instructies ontvangen om:
- een bepaald standpunt in te nemen over een gegevensbeschermingskwestie, bijvoorbeeld over een wettelijke interpretatie.

Om belangenverstrengeling te voorkomen, is af te raden dat de FG ook een functie binnen de organisatie heeft waarin hij het doel en de middelen van een gegevensverwerking bepaalt. Dit kan bijvoorbeeld zo zijn als de FG een managementpositie vervult, zoals hoofd financiën, strategie, marketing, IT of HRM. Aan te raden is om vast te stellen over welke organisatieonderdelen het toezicht van de functionaris gegevensbescherming zich zal uitstrekken. Denk hierbij ook aan de relatie met de privacybeheerder BRP.

Positionering FG en CISO

De AVG draagt een verwerkingsverantwoordelijke op om een passend niveau van beschermende maatregelen te treffen. In zijn algemeenheid maken persoonsgegevens onderdeel uit van de gegevens waarvoor een organisatie informatiebeveiligingsmaatregelen dient te treffen. Het domein informatiebeveiliging heeft dan ook een duidelijke overlap met privacy. Hetzelfde zal gelden voor de functionarissen, de FG en de Chief Information Security Officer (CISO).

- bepaal of de FG en de CISO functies door een of meerdere personen uitgevoerd zullen worden;
- vul, indien mogelijk, beide functies onafhankelijk van elkaar in;
- let bij de inrichting van de functies op overlap in taken en verantwoordelijkheden;
- overweeg, wanneer de CISO en FG een gecombineerde rol is, bepaalde taken zoals taken met betrekking tot verslaggeving, meldingenregister en klachtbehandeling bij een andere functionaris te beleggen;
- tref waarborgen voor afdoende overleg en afstemming tussen beide functies;
- tref waarborgen dat een FG zowel organisatiebreed en strategisch/tactisch advies kan geven naast betrokkenheid bij individuele casuïstiek in PIA's en klachten.

Best practices inzake omgang met belangenconflicten en de FG
Combineren van rollen
Wanneer een FG zijn taken combineert met een andere rol, zoals die van Security Officer (CISO) of beleidsadviseur, is aan te raden de functies en rollen expliciet te scheiden, zodat voor iedereen meteen duidelijk is wanneer de persoon welke functie op welk moment vervult.
Voorkomen van belangenconflicten
Om belangenconflicten voorkomen wordt aangeraden om, afhankelijk van de activiteiten, grootte en structuur van de organisatie, de volgende best practices toe te passen:

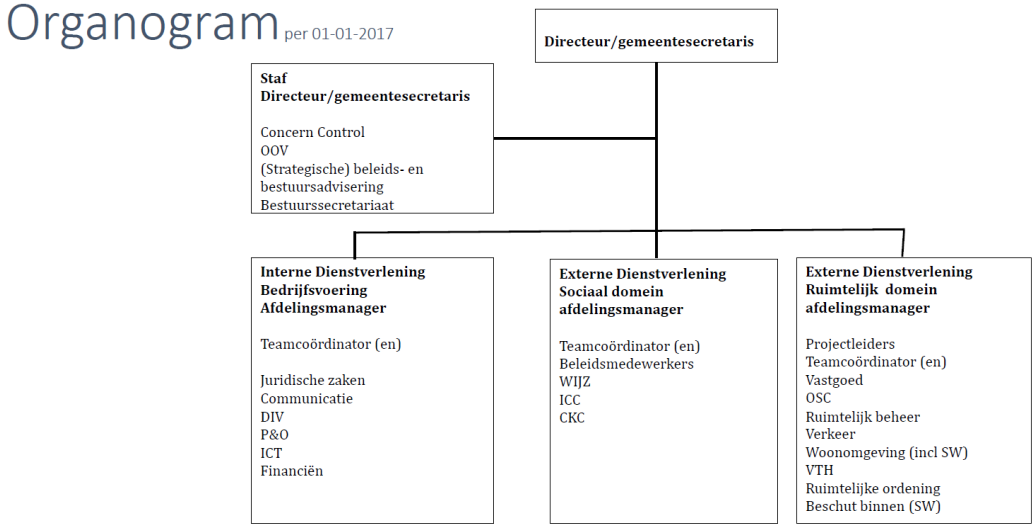
- bepaal vooraf welke posities niet verenigbaar zijn met de functie van FG;
- stel interne regels op om belangenconflicten te vermijden;
- geef meer algemene uitleg over belangenconflicten en wanneer ze kunnen optreden;
- verklaar dat een FG geen belangenconflict mag hebben en zorg ervoor dat iedereen zich hiervan bewust is;
- zorg voor waarborgen in de interne regels van de organisatie en zie erop toe dat de vacature voor de positie van FG of een servicecontract met een andere partij specifiek en gedetailleerd genoeg is om belangenconflicten te voorkomen.

Meer informatie

- Richtlijnen voor functionarissen voor de gegevensbescherming (FG's)

Artikel 4.5 Verantwoordelijkheden ten aanzien van het privacybeleid

Deze toelichting op taken en verantwoordelijkheden maakt deel uit van Handboek Informatiebeveiliging van de gemeente Haren. Het bevat verantwoordelijkheden en activiteiten met betrekking tot informatiebeveiliging die uitgevoerd moeten worden op basis van de AVG en Wbp.



Bijlage Toelichting op de rechten van de betrokkene

Inleiding

Personen hebben het recht te weten welke informatie door de gemeente Haren wordt verwerkt. Als deze informatie onjuist blijkt te zijn, mag deze gecorrigeerd of verwijderd worden. Deze rechten zijn in de AVG opgenomen in hoofdstuk III onder de artikelen 12 t/m 22 (Rechten van de betrokkene). In de praktijk zullen vooral artikel 15 t/m 18 (inzage, correctie en beperking en verwijdering van gegevens) en artikel 21 (Recht van bezwaar) van de AVG van toepassing zijn.

Deze rechten gelden voor alle personen van wie de gemeente Haren persoonsgegevens verwerkt.

Het artikel rechten betrokkene bevat informatie over hoe de gemeente Haren omgaat met de verzoeken van personen. Ondanks dit proces, staat het een betrokkene vrij de vorm en het kanaal te kiezen voor een verzoek. In voorkomende gevallen zullen verzoeken intern doorgeleid moeten worden.

Om welke rechten gaat het?

- Recht op informatie. Een persoon wordt geïnformeerd dat de gemeente Haren gegevens over hem opslaat. Dit gebeurt bij wanneer gegevens van een persoon worden verzameld of wanneer een persoon een website bezoekt (via de cookie melding).
- Recht op inzage. Een persoon mag weten welke gegevens door de gemeente Haren over hem zijn opgeslagen en worden verwerkt.
- Recht op correctie en verwijdering. Wanneer gegevens verkeerd blijken te zijn kan een persoon vragen deze aan te passen of te verwijderen. Ook kunnen gegevens afgeschermd worden als ze nog nodig zijn, bijvoorbeeld in een gerechtelijke procedure.
- Recht van verzet. Een persoon mag de gemeente Haren vragen zijn persoonsgegevens niet meer te verwerken. Dit is niet altijd mogelijk, omdat bepaalde gegevens verwerkt moeten worden om wettelijke taken te kunnen uitvoeren. Het recht van verzet, zoals hier wordt bedoeld, gaat over specifieke situaties van een betrokkene en zaken als direct marketing, marktonderzoeken, post- en onlineverwerkingen (waaronder elektronische nieuwsbrieven).
- Bij klachten over het gebruik van persoonsgegevens (ook bijvoorbeeld een foto van de persoon) geldt de bestaande klachtenregeling.
- (AVG) Met de introductie van het recht op dataportabiliteit kan een persoon verzoeken zijn gegevens in een leesbaar formaat te ontvangen of over te hevelen naar een andere organisatie.

Wat mag een betrokkene inzien?

De betrokkene heeft het recht om alles in te zien. Hier zullen alle medewerkers rekening mee moeten houden bij het inrichten en samenstellen van informatie en dossiers. Wel gelden enkele uitzonderingen.

- Persoonlijke werkaantekeningen vallen buiten het inzagerecht. Het moet dan wel gaan om persoonlijke aantekeningen. Wanneer aantekeningen bedoeld zijn om te delen met collega's, uit te werken of toegankelijk zijn voor anderen zijn het geen persoonlijke aantekeningen meer.
- Inzage mag geweigerd worden als dat noodzakelijk is voor:
  - de veiligheid van de staat;
  - het voorkomen, opsporen en vervolgen van strafbare feiten;
  - zwaarwegende economische en financiële belangen van de staat en andere openbare lichamen;
  - het toezicht op de naleving van wettelijke voorschriften die zijn gesteld om de onder 2 en 3 genoemde belangen te beschermen;
  - bescherming van uw rechten en vrijheden of die van anderen. Hier kan ook een onevenredige (administratieve) belasting van de organisatie onder vallen.

Let op:

Omdat de gemeente Haren een bestuursorgaan is, dan geldt dat een reactie op een verzoek van een betrokkene wordt gezien als een besluit in de zin van de Algemene wet bestuursrecht (Awb). Op grond van deze wet kan een betrokkene (of diens vertegenwoordiger) bezwaar maken tegen het besluit. Ook geldt de dwangsomregeling inzake niet tijdig beslissen uit hoofde van de Awb.

Links:

Website Autoriteit Persoonsgegevens

Naslag wetsartikelen (Wet bescherming persoonsgegevens)

Hoofdstuk 6 Rechten van de betrokkene

- Artikel 35: Informatieplicht en inzage
- Artikel 36: Verbetering, aanvulling, verwijdering of afscherming
- Artikel 37: Vorm, identiteit en minderjarigheid

- Artikel 38: Informeren van derden
- Artikel 39: Vergoeding;
- Artikel 40: Verzet tegen verwerking
- Artikel 41: Verzet tegen verwerking
- Artikel 42: Automatische verwerking

Hoofdstuk 7 Uitzonderingen en beperkingen
- Artikel 43: Uitzonderingen

Naslag wetsartikelen (Algemene verordening gegevensbescherming)
Hoofdstuk III Rechten van de betrokkene

- Artikel 12. Transparante informatie, communicatie en nadere regels voor de uitoefening van de rechten van de betrokkene
- Artikel 13. Te verstrekken informatie wanneer persoonsgegevens bij de betrokkene worden verzameld
- Artikel 14. Te verstrekken informatie wanneer de persoonsgegevens niet van de betrokkene zijn verkregen
- Artikel 15. Recht van inzage van de betrokkene
- Artikel 16. Recht op rectificatie
- Artikel 17. Recht op gegevenswissing
- Artikel 18. Recht op beperking van de verwerking
- Artikel 19. Kennisgevingsplicht inzake rectificatie, wissing of beperking
- Artikel 20. Recht op overdraagbaarheid van gegevens
- Artikel 21. Recht van bezwaar
- Artikel 22. Geautomatiseerde individuele besluitvorming, waaronder profilering

Haren, 12 juni 2018
M.P. de Wilde
secretaris

P. van Veen
burgemeester