GEMEENTE HEERENVEEN

GEMEENTEBLAD

Officiële uitgave van de gemeente Heerenveen

Nr. 66791

4 maart

2021

Privacyreglement Gemeente Heerenveen

Het college van burgemeester en wethouders;

De burgemeester en;

De raad van de gemeente Heerenveen;

Ieder voor zover het hun eigen bevoegdheden betreft,

gelet op de AVG en de UAVG,

overwegende dat het wenselijk is om beleid vast te stellen voor de wijze waarop de raad bij de uitoefening van haar bevoegdheden omgaat met de verwerking van persoonsgegevens,

hebben op respectievelijk 27 oktober 2020, 27 oktober 2020 en 28 januari 2021, ieder voor zover het zijn eigen bevoegdheden betreft, besloten het volgende vast te stellen:

Privacyreglement Gemeente Heerenveen

1. Inleiding

1.1 Algemeen
De gemeente Heerenveen hecht veel waarde aan de bescherming van de privacy bij het verwerken van persoonsgegevens. Binnen de gemeente Heerenveen wordt voortdurend gewerkt met persoonsgegevens van burgers, medewerkers en (keten)partners. Persoonsgegevens worden voornamelijk verzameld bij de burgers voor het goed uitvoeren van de gemeentelijke wettelijke taken. De burgers moeten erop kunnen vertrouwen dat de gemeente zorgvuldig en veilig met de persoonsgegevens omgaat. Het is dus belangrijk om hier transparant over te zijn en te laten zien op welke manier de gemeente deze persoonsgegevens verwerkt. Vanuit respect voor de privacy van burgers is hierbij een goede afweging tussen het goed uitvoeren van de taken van de gemeente en het waarborgen van de privacy van belang.

Vooral in het Sociaal Domein en als het gaat om openbare orde en veiligheid, waar het noodzakelijk is om met bijzondere persoonsgegevens te werken, is dit belangrijk. Naast het belang van de individuele burger, is er het algemeen belang en zijn er belangen van burgers ten opzichte van elkaar. Dit vraagt om een aantoonbare zorgvuldige afweging waar betrokkenen in meegenomen worden.

In deze tijd gaat ook de gemeente mee met nieuwe ontwikkelingen. Nieuwe technologische ontwikkelingen, innovatieve voorzieningen, globalisering en een steeds meer digitale overheid stellen andere eisen aan de bescherming van gegevens en privacy. De gemeente is zich hier van bewust en zorgt dat de privacy gewaarborgd blijft, onder andere door maatregelen op het gebied van informatiebeveiliging, dataminimalisatie, transparantie en gebruikerscontrole.

Iedereen heeft recht op correcte, veilige en betrouwbare informatieverwerking en moet erop kunnen vertrouwen dat de gemeente zorgvuldig met deze gegevens omgaat.

1.2 Reikwijdte en afbakening privacyreglement
Het privacyreglement is van toepassing op:
- Alle processen binnen de gehele organisatie waarbinnen persoonsgegevens worden verwerkt;
- Digitale oplossingen waarin persoonsgegevens worden verwerkt, waarvoor de gemeente (intern en extern) verantwoordelijk is;
- Alle ruimten en digitale oplossingen die door bestuurders en medewerkers intern en extern worden gebruikt waar(op) persoonsgegevens worden verwerkt;
- Alle geldende normen en regels op het gebied van privacy.

Voor het grootste deel van de verwerkingen is het college de verantwoordelijke. Daar waar een specifieke taak is toebedeeld aan een ander bestuursorgaan, is dit bestuursorgaan ook de verantwoordelijke voor de verwerking van de persoonsgegevens.
Het privacyreglement heeft betrekking op de persoonsgegevens van personen van wie de gemeente gegevens verwerkt (of laat verwerken).

Informatiebeveiliging en de bescherming van persoonsgegevens zijn onlosmakelijk met elkaar verbonden. Informatiebeveiliging is een randvoorwaarde voor de borging van privacy bij de verwerking van persoonsgegevens. Het is het geheel aan maatregelen, procedures en processen die de beschikbaarheid, integriteit en vertrouwelijkheid van alle vormen van informatie binnen een organisatie garanderen.

Onder persoonsgegevens verstaan we alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon ("de betrokkene"). Dit betekent dat informatie direct over iemand gaat of naar deze persoon te herleiden is.

De verwerking van persoonsgegevens is elke handeling of elk geheel van handelingen met persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde processen. In de AVG valt onder een verwerking:
- Verzamelen, vastleggen en ordenen
- Bewaren, bijwerken en wijzigen
- Opvragen, raadplegen, gebruiken
- Verstrekken door middel van doorzending
- Verspreiding of enige andere vorm van ter beschikkingstellen
- Samenbrengen, met elkaar in verband brengen
- Afschermen, uitwissen of vernietigen van gegevens

Uit deze opsomming blijkt dat alles wat met een persoonsgegeven wordt gedaan een verwerking is.

Verdere definities met betrekking tot de verwerking van persoonsgegevens zijn opgenomen in de Algemene Verordening Gegevensbescherming (AVG).

1.3 Opbouw privacyreglement

Het privacyreglement geldt als algemeen kader voor de gehele organisatie. In hoofdstuk 2 staat het algemene beleid. De organisatie van verantwoordelijkheden, functies en rollen waarmee de gegevensbescherming bij de gemeente wordt geborgd, is opgenomen in hoofdstuk 3. In hoofdstuk 4 worden de risico's en maatregelen beschreven, om te voldoen aan de wet- en regelgeving. Rechten van betrokkenen worden beschreven in hoofdstuk 5 en in hoofdstuk 6 is een toelichting op de geautomatiseerde besluitvorming te vinden.

Voor bepaalde domeinen zal de gemeente aanvullend specifiek privacybeleid vaststellen en deze publiceren.

1.4 Wetten en regels

De juridische grondslag voor privacy is terug te vinden in wet- en regelgeving. De bescherming van de privacy bij de verwerking van persoonsgegevens is een grondrecht. Dit is geregeld in:
- Grondwet (artikel 10 Grondwet)
- Handvest van de grondrechten van de Europese Unie (EHRM)
- Europees Verdrag voor de Rechten van de Mens (EVRM)
- Internationaal Kinderrechtenverdrag (IVRK)

De bescherming van de privacy wordt ingevuld door wetten, namelijk:
- de Europese Algemene Verordening Gegevensbescherming
- Uitvoeringswet Algemene Verordening Gegevensbescherming

Verder is ook in specifieke regelgeving invulling gegeven aan de bescherming van de privacy bij de verwerking van persoonsgegevens zoals:
- Wet maatschappelijke ondersteuning (Wmo 2015)
- Jeugdwet
- Wet Basisregistratie Personen (Wet Brp)
- Participatiewet
- Wet algemene bepalingen Burgerservicenummer

2. Privacyreglement

2.1 Doelstelling

Doel van dit privacyreglement is het beschrijven van kaders voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacyrechten van personen waarvan de gemeente persoonsgegevens verwerkt.

Het privacyreglement omvat de gehele datacyclus van het genereren of verzamelen van gegevens, het dagelijks gebruik ervan en de gegevensopslag tot en met de archivering en vernietiging ervan. Er wordt geen onderscheid gemaakt tussen papieren of digitale informatieverwerking.

Het privacyreglement draagt bij aan:
- het beschermen van de privacy van personen van wie de gemeente gegevens verwerkt of laat verwerken;
- het maatschappelijk vertrouwen en draagvlak;
- het beheersen van afbreuk- en aansprakelijkheidsrisico's;
- het verantwoording af kunnen leggen aan het college/de burgemeester/raad, waar nodig de Autoriteit Persoonsgegevens (AP) of de rechter;
- het in kunnen spelen op wettelijke en technologische ontwikkelingen.

2.2. Uitgangspunten
De gemeente gaat op een veilige manier met persoonsgegevens om en respecteert de privacy van betrokkenen. Iedereen werkzaam binnen de organisatie is verantwoordelijk voor het verantwoord omgaan met persoonsgegevens en het waarborgen van de privacyrechten van personen.

Het is belangrijk om persoonsgegevens rechtmatig, behoorlijk en transparant te verwerken:
- rechtmatig: de hoofdregel is dat de verwerking van persoonsgegevens alleen toegestaan is in overeenstemming met de wet en op een zorgvuldige wijze;
- behoorlijk: persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. De gemeente zorgt ervoor dat de persoonsgegevens kloppen en volledig zijn voordat ze verwerkt worden;
- transparant: de gemeente is transparant over de manier waarop de gemeente met persoonsgegevens omgaat. De gemeente praat niet over de betrokkenen maar met de betrokkenen. De betrokkenen worden op de hoogte gesteld van de manier waarop met hun persoonsgegevens om wordt gegaan.

De gemeente houdt zich hierbij aan de volgende uitgangspunten:

Dataminimalisatie
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.

Grondslag en doelbinding
- De gemeente zorgt ervoor dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen worden verzameld en verwerkt.
- De gemeente verwerkt alleen persoonsgegevens als dit noodzakelijk is:
  - voor de uitvoering van een taak in het algemeen belang of voor de uitoefening van het openbaar gezag (deze grondslag is het meest voorkomend i.v.m. uitvoeren publiekrechtelijke taken);
  - om te voldoen aan een wettelijke verplichting (ook deze grondslag wordt veel gebruikt door de gemeente. Hierbij staat de verplichting om persoonsgegevens te verwerken letterlijk in de landelijke wetgeving, bijvoorbeeld de Participatiewet);
  - voor de uitvoering van een overeenkomst met de betrokkene (bijvoorbeeld het verwerken van persoonsgegevens in de administratie bij een koopovereenkomst);
  - bij uitzondering: ter bescherming van vitale belangen (situaties van leven of dood);
  - bij uitzondering: betrokkene heeft toestemming gegeven voor de verwerking (let op: betrokkene moet een vrije keuze hebben en dus ook kunnen weigeren. Daarom kan toestemming in het publiekrecht bijna nooit worden gebruikt als grondslag.)

De gemeente werkt hierbij vanuit de bedoeling. Dit betekent dat als er onduidelijkheid is over het wel of niet mogen verwerken zoals het delen van persoonsgegevens, het doel waarvoor gegevens worden verwerkt doorslaggevend is. De gemeente zorgt ervoor dat de motivatie of de belangenafweging hiervan schriftelijk wordt vastgelegd.

Bewaartermijn
Persoonsgegevens worden niet langer bewaard dan nodig is. De gemeente gaat hierbij uit van de Archiefwet en de daarop gebaseerde selectielijsten. Als registratie van de persoonsgegevens niet meer noodzakelijk is voor het doel, dan moeten de persoonsgegevens worden verwijderd of geanonimiseerd.

Integriteit en vertrouwelijkheid
De gemeente gaat zorgvuldig om met persoonsgegevens en behandelt deze vertrouwelijk. Zo worden persoonsgegevens alleen verwerkt door personen met een geheimhoudingsplicht en voor het doel

waarvoor deze gegevens zijn verzameld. De persoonsgegevens zijn overeenkomstig het classificatieniveau beveiligd door middel van passende technische en organisatorische maatregelen.

Delen met derden
In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt de gemeente afspraken over de eisen waar gegevensuitwisseling aan moet voldoen. Deze afspraken voldoen aan de wet. De gemeente maakt afspraken over de controle hierop.

Subsidiariteit
De verwerking van persoonsgegevens is alleen toegestaan wanneer het doel niet op een andere manier kan worden bereikt.

Proportionaliteit
De persoonsgegevens mogen alleen verwerkt worden als dit in verhouding staat tot het doel. Als dit doel ook bereikt kan worden met geen of minder (belastende) persoonsgegevens dan wordt daar voor gekozen.

Rechten van betrokkenen
De gemeente honoreert zover mogelijk alle rechten van betrokkenen. Om gebruik te maken van zijn/haar rechten kan de betrokkene een verzoek indienen. Dit verzoek kan zowel schriftelijk als via een webformulier ingediend worden. Binnen vier weken zal de gemeente laten weten wat er met het verzoek gaat gebeuren. Aan de hand van een verzoek kan de gemeente aanvullende informatie opvragen om zeker te zijn van de identiteit van de betrokkene.

De gemeente is verantwoordelijk voor het naleven van deze uitgangspunten en moet dit kunnen aantonen.

2.3 Risico's
Bij schending van de privacywet- en regelgeving is de gemeente wettelijk aansprakelijk. Het verwijtbaar onvoldoende beschermen van persoonsgegevens en het niet naleven van privacywet- en regelgeving kan leiden tot:
- het betalen van schadevergoeding. Elke benadeelde heeft hier recht op;
- reputatieschade en herstelkosten. Deze kunnen fors zijn en leiden tot verlies van vertrouwen in de overheid;
- onderzoeken, dwangmaatregelen en hoge bestuurlijke boetes. Bij overtreding van de AVG kan de AP als landelijk toezichthouder, een boete opleggen. Onder de AVG kunnen de (zeer) forse boetes oplopen tot maximaal € 20 miljoen.

Binnen bepaalde domeinen worden bijzondere persoonsgegevens, zoals medische gegevens of strafrechtelijke gegevens verwerkt. Voorbeelden zijn het sociaal domein en de openbare orde en veiligheidstaken. Aan de verwerking van deze persoonsgegevens zijn aanvullende voorwaarden gesteld (artikel 9 en 10 AVG), omdat er sprake is van (zeer) gevoelige informatie over personen.
De risico's van schending van de privacy voor personen variëren van ongemak, stigmatisering, uitsluiting en tot identiteitsfraude of chantage.

Om de risico's te beperken moeten maatregelen worden getroffen. Deze maatregelen zijn beschreven in hoofdstuk 4 van dit reglement. Leidend daarbij is dat privacy-eisen zoveel mogelijk worden geïntegreerd in regulier en/of al bestaand beleid en vertaald naar processtappen die worden geïntegreerd in het reguliere werkproces.

3. Taken en verantwoordelijkheden

3.1. Verantwoordelijken
De afzonderlijke bestuursorganen zijn ieder verantwoordelijk voor een zorgvuldige gegevensverwerking bij de uitvoering van zijn of haar taken. Het college is in de meeste gevallen eindverantwoordelijke voor de bescherming van de privacy van betrokkenen.

3.2 Het college
Het college:
- is eindverantwoordelijk om te waarborgen dat persoonsgegevens worden beschermd op een manier die in overeenstemming is met de geldende wet- en regelgeving en de zorgvuldigheidsvereisten. Er is een directe relatie met de beginselen van behoorlijk bestuur;
- stelt kaders voor de bescherming van de privacy op basis van wet- en regelgeving;
- rapporteert aan de raad over de uitvoering van het beleid.

3.2.1 Verantwoording aan de raad
Net zoals het college verantwoording moet afleggen over de gemeentelijk uitgaven, wordt ook verantwoording afgelegd over de realisatie van beleid. Dit geldt ook voor het privacyreglement en de toepassing daarvan. Het privacyreglement wordt om die reden onderdeel van de Planning & Control cyclus en opgenomen in de jaarrekening.

3.3 De directie
De directie is verantwoordelijk voor kaderstelling en sturing. De directie zorgt ervoor:
- dat er gestuurd wordt op concern risico's;
- dat er gecontroleerd wordt of de getroffen maatregelen voldoende bescherming bieden om de privacy van betrokkene(n) te beschermen;
- dat de FG, de CISO en de Privacy Officer (PO) naar behoren en tijdig worden betrokken bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

3.4 De afdelingshoofden
Het afdelingshoofd is verantwoordelijk voor een zorgvuldige verwerking van persoonsgegevens die binnen zijn of haar afdeling plaatsvindt. Dit betekent onder meer:
- het verwerkingsregister;
- verwerkersovereenkomsten;
- datalekken;
- continue aandacht voor informatieveiligheid en privacy bij de medewerkers;
- DPIA's;
- inhoudelijke behandeling van privacy klachten;
- inhoudelijke behandeling van verzoeken van rechten van betrokkenen.

3.5 De Functionaris Gegevensbescherming (FG)
De FG is de interne toezichthouder op de verwerking van persoonsgegevens binnen de organisatie. De FG houdt binnen de organisatie toezicht op de toepassing en naleving van de privacywetgeving. De wettelijke taken en bevoegdheden van de FG geven deze functionaris een onafhankelijke positie in de organisatie. De FG heeft in ieder geval de volgende verantwoordelijkheden:
- Het informeren en adviseren van de gemeente en de verwerkers die namens de gemeente persoonsgegevens verwerken over hun verplichtingen uit hoofde van de AVG en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming;
- Het toezien op naleving van de AVG, en andere EU wet- en regelgeving en nationale bepalingen omtrent gegevensbescherming;
- Het toezien op naleving van het gemeentelijke beleid en of de verwerker met betrekking tot de bescherming van persoonsgegevens;
- Het toezien op toewijzing van verantwoordelijkheden, bewustmaking en opleiding van het bij de verwerking betrokken personeel en de betreffende audits;
- Het geven van advies met betrekking tot de gegevensbeschermingseffect-beoordeling (DPIA) en het toezien of de uitvoering daarvan in overeenstemming is met de AVG;
- Het samenwerken met de AP;
- Het optreden als contactpunt voor de AP;
- In samenspraak met de CISO adviseren over digitale oplossingen en de informatiebeveiliging van gegevensverwerking;
- Toezien op het verwerkingsregister;
- Controleren van verwerkersovereenkomsten;
- Bij inbreuk persoonsgegevens (meldplicht datalekken) adviseren over de ernst en omvang ervan;
- Adviseren zodat privacy klachten tot een goed einde gebracht worden;
- Adviseren over de afhandeling van verzoeken van betrokkenen met betrekking tot de verwerking van hun gegevens en het uitoefenen van hun rechten (zoals o.a. recht op inzage).

3.6 Chief Information Security Officer (CISO)
De CISO is op organisatieniveau verantwoordelijk voor:
- het adviseren over informatieveiligheidsbeleid;
- het coördineren van de uitvoering van het beleid;
- het adviseren over informatiebeveiliging;
- het beheersen van risico's;
- het opstellen van rapportages met betrekking tot informatieveiligheid.

3.7 De Privacy Officer (PO)
De PO werkt nauw samen met de FG en de CISO en:
- Bevordert en adviseert de organisatie over de bescherming van persoonsgegevens (inclusief scholing);

- Stelt algemeen privacybeleid (inclusief procedures) op;
- Ondersteunt de afdeling bij het opstellen van afdelingsspecifiek privacybeleid;
- Adviseert over de juridische aspecten in de verwerkersovereenkomsten;
- Heeft een coördinerende en adviserende rol bij het verwerkingsregister;
- Adviseert bij klachtprocedures;
- Heeft een ondersteunende adviserende rol bij veiligheidsincidenten en datalekken;
- Heeft een ondersteunende en adviserende rol bij verzoeken van betrokkenen die gebruik maken van hun rechten;
- Ondersteunt en adviseert de afdelingen bij het uitvoeren van DPIA's;
- Ondersteunt en adviseert de privacy adviseurs op de afdelingen bij privacyvraagstukken.

3.8 De medewerkers
Alle medewerkers (inclusief inhuur/externen) zijn verantwoordelijk voor de bescherming van de privacy van betrokkene(n) bij de uitvoering van zijn of haar werkzaamheden. Dat betekent dat iedereen zorgt voor een veilige, rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens. De medewerkers kunnen hiervoor gebruik maken van het stroomschema die bijgevoegd is als bijlage.

4. Maatregelen
Persoonsgegevens worden alleen in overeenstemming met de wet en op behoorlijke en zorgvuldige wijze verwerkt. Dit gebeurt in overeenstemming met de in de AVG voorgeschreven doelbinding en proportionaliteit. Dit houdt in dat persoonsgegevens alleen voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen mogen worden verzameld, dat er niet meer persoonsgegevens worden verwerkt dan voor het doel nodig is en dat er waar mogelijk minder of geen persoonsgegevens worden verwerkt. De gemeente moet aantonen dat ze voldoet aan de AVG. Dit doet de gemeente aan de hand van onderstaande maatregelen.

4.1 Bij aanvang van de gegevensverwerking

4.1.1 Transparantie en informatieplicht
De hoofdregel van de verwerking van persoonsgegevens is dat het alleen toegestaan is in overeenstemming met de wet, en op een zorgvuldige wijze. Persoonsgegevens worden zoveel mogelijk verzameld bij de betrokkene zelf. De gemeente zorgt ervoor dat de persoonsgegevens kloppen en volledig zijn voordat ze verwerkt worden. De gemeente is transparant over de manier waarop de gemeente met persoonsgegevens omgaat. De gemeente praat niet over de betrokkenen, maar met de betrokkenen. De gemeente informeert de betrokkene over het verwerken van persoonsgegevens. Wanneer betrokkenen gegevens aan de gemeente geven, worden zij op de hoogte gesteld van de manier waarop de gemeente met persoonsgegevens om zal gaan. Dit kan bijvoorbeeld via een formulier gebeuren. De betrokkene wordt niet nogmaals geïnformeerd als hij/zij al weet dat de gemeente persoonsgegevens van hem/haar verzamelt en verwerkt, en weet waarom en voor welk doel dat gebeurt.
Wanneer de gegevens via een andere weg verkregen worden, dus buiten de betrokkene om, wordt de betrokkene geïnformeerd op het moment dat deze voor de eerste keer worden verwerkt.

Via de Wet openbaarheid van bestuur (Wob) kan men een verzoek om openbaarmaking van bestuurlijke informatie indienen bij de gemeente. De Wet hergebruik van overheidsinformatie (Who) regelt het op verzoek verstrekken van overheidsinformatie voor hergebruik. Bij deze verzoeken bekijkt de gemeente altijd of het antwoord geen inbreuk maakt op de persoonlijke levenssfeer van betrokkenen. In principe worden geen persoonsgegevens verstrekt.

4.1.2. Bewust omgaan met persoonsgegevens
Voor het borgen van privacy is het vooral van belang dat er bewust met persoonsgegevens wordt omgegaan. Het is noodzakelijk om het bewustzijn voortdurend aan te scherpen, zodat kennis van risico's wordt verhoogd en (veilig en verantwoord) gedrag wordt aangemoedigd. De gemeente zorgt ervoor dat hier voortdurend aandacht voor is.

4.1.3 Privacy by design of privacy by default
De gemeente zorgt ervoor dat er vanaf het ontwerpen van een nieuw of aangepast proces, product, dienst of informatiesysteem wordt nagedacht over:
- het rechtmatig, behoorlijk en transparant verwerken van persoonsgegevens;
- de maatregelen die hiervoor nodig zijn.

In systemen worden de standaard instellingen zodanig ingesteld dat de privacy bescherming maximaal wordt geborgd. De AVG noemt dit 'Gegevensbescherming door ontwerp en standaardinstellingen'.

4.1.4. Data Protection Impact Assessment
Bij de invoering van nieuw beleid of regelgeving wordt de bescherming van de persoonlijke levenssfeer meegewogen. Eén van de instrumenten om dit te doen, is de uitvoering van een Data Protection Impact Assessment (hierna: DPIA). De gemeente beoordeelt de noodzaak daartoe van geval tot geval aan de hand van een DPIA-checklist en de lijst van de Autoriteit Persoonsgegevens.
De volgende indicatoren worden daarbij als toetsingskader gehanteerd:
- een nieuwe of veranderde gemeentelijke taak,
- aanleg van een groot databestand,
- verwerking van bijzondere persoonsgegevens,
- aanschaf van een nieuw informatiesysteem,
- systematische gegevensuitwisseling met een derde.

Met een DPIA worden systematisch verwerkingen van persoonsgegevens, doeleinden, risico's en (voorgenomen) maatregelen beschreven om zo de impact van de verwerking op de bescherming van persoonsgegevens in kaart te brengen.
Voor het uitvoeren van een DPIA wordt gebruik gemaakt van de model DPIA van de IBD en de basis hiervoor het DEDA-model van CNIL.

4.1.5. Register van verwerkingen
De gemeente houdt een register van de verwerkingsactiviteiten bij. Het register bevat onder andere:
- De naam en contactgegevens van de verwerkingsverantwoordelijke en, mogelijk, de gezamenlijke verwerkingsverantwoordelijke;
- De doelen van de verwerking;
- Een beschrijving van de soort persoonsgegevens en de daarbij horende betrokkenen;
- Een beschrijving van de ontvangers van de persoonsgegevens;
- Indien van toepassing: een beschrijving van het delen van persoonsgegevens aan een derde land of internationale organisatie;
- De termijnen waarin de verschillende persoonsgegevens moeten worden gewist;
- Een algemene beschrijving van de beveiligingsmaatregelen.

De gemeente heeft het register openbaar gemaakt via de gemeentelijke website.

4.2 Informatiebeveiligingsbeleid
De gemeente Heerenveen neemt de privacy van haar klanten en de informatieveiligheid serieus. Burgers en bedrijven moeten er op kunnen vertrouwen dat de gemeente zorgvuldig en controleerbaar met informatie omgaat en deze goed beveiligt. De gemeente Heerenveen maakt daarom gebruik van de Baseline Informatiebeveiliging Overheid (BIO) en het daarbij horende niveau van informatiebeveiliging. Dit privacyreglement hangt daarom samen met het Informatiebeveiligingsbeleid. Het Informatiebeveiligingsbeleid is vastgesteld door de directie en ter kennisname verzonden aan het college van burgemeester en wethouders. Het informatiebeveiligingsbeleid wordt periodiek geëvalueerd. In het Informatiebeveiligingsbeleid zijn vertrekpunten m.b.t. informatiebeveiliging opgenomen welke integraal gelden voor de gehele organisatie.

4.2.1 Controle gegevensverwerking
Als onderdeel van de implementatie van de BIO (Baseline Informatiebeveiliging Overheid) wordt bij een aantal applicaties dat persoonsgegevens verwerkt, gewerkt met logging van de verwerkingen. In deze logging staat vermeld welke gebruiker, op welk moment, welke gegevens heeft verwerkt. Deze logging wordt gebruikt als er twijfel is over juist gebruik.

4.2.2. Dataclassificatie
De maatregelen die getroffen moeten worden om de gegevensbescherming te kunnen borgen, zijn niet voor elk proces en informatiesysteem hetzelfde. Er wordt daarom voor alle informatiesystemen een dataclassificatie uitgevoerd. Dataclassificatie heeft als doel om mate de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens aan te geven. Het maakt inzichtelijk welke maatregelen genomen moeten worden om de gegevens passend te beveiligingen.

4.2.3. Verwerkersovereenkomst met derden
Bij veel gemeentelijke processen worden gegevens verwerkt door derden. Denk hierbij aan uitbestede werkzaamheden of samenwerkingsverbanden. Het college blijft verantwoordelijk voor de verwerking van de gegevens. Zij moet er daarom op toezien dat gegevens juist verwerkt en beveiligd worden.

In het geval van samenwerking met externe partijen, waarbij sprake is van gegevensverwerking van persoonsgegevens, maakt de gemeente afspraken over de eisen waar gegevensverwerking en -uitwisseling aan moet voldoen.
Er worden bijvoorbeeld afspraken gemaakt over:

- de doeleinden waarvoor de gegevens mogen worden verwerkt;
- hoe de verwerker met de persoonsgegevens moet omgaan;
- welke beveiligingsmaatregelen moeten worden genomen;
- melden van een datalek aan de verantwoordelijke;
- welke vormen van toezicht de verantwoordelijke mag uitoefenen;
- de geheimhoudingsplicht;
- inschakeling van derden en onderaannemers door de verwerkers;
- locatie van de data;
- aansprakelijkheid in geval van schade door het niet naleven van regelgeving.

Als voor deze afspraken een verwerkersovereenkomst wordt afgesloten gebruikt de gemeente de standaard van de IBD/VNG.

Het afdelingshoofd die een dergelijke uitbesteding, samenwerking of uitwisseling aangaat, ziet toe op de totstandkoming van deze afspraken. De Privacy officer en de CISO worden bij de totstandkoming betrokken.

De gemeente geeft geen persoonsgegevens door aan (organisaties in) een land dat buiten de Europese Economische Ruimte ligt of internationale organisaties. Als zij dit gaat doen, dan zal dit alleen in overeenstemming met de voorwaarden uit de AVG zijn.

4.3. Meldplicht datalekken

Een datalek is een inbreuk op de beveiliging, waarbij een kans bestaat dat dit ernstige gevolgen dan wel ernstige nadelige gevolgen heeft voor de bescherming van de persoonsgegevens. De gemeente doet er alles aan om een datalekken te voorkomen en heeft hier ook afspraken over gemaakt met derden die werkzaamheden voor de gemeente uitvoeren.

Vast staat dat er wel datalekken gaan plaatsvinden. Een mail naar de verkeerde persoon sturen, stukken in de verkeerde envelop of een hack door een externen zijn dingen die niet 100% uit te sluiten zijn. Als dit zich voordoet, dan doet de gemeente zijn uiterste best de schending van de privacy zo snel mogelijk op te lossen of de negatieve gevolgen daarvan zo veel mogelijk te beperken. Van alle datalekken wordt een registratie bijgehouden. Van de datalekken met een hoog risico wordt melding gemaakt bij de AP/toezichthouder.

4.4. Bewaren van gegevens

Uitgangspunt van de AVG is dat persoonsgegevens niet langer worden bewaard dan noodzakelijk is voor het doel waarvoor ze zijn verwerkt. De bewaartermijnen van persoonsgegevens lopen hierdoor uiteen. In diverse wetten zijn minimale en maximale bewaartermijnen opgenomen. Deze komen ook terug in de vastgestelde selectielijsten die voortvloeien uit de Archiefwet, welke aangeven hoe lang informatie bewaard moet worden.

Het doel van de Archiefwet is het bewaren van belangrijke informatie. De AVG is gericht op bescherming van persoonsgegevens. Hierbij is dataminimalisatie een belangrijk uitgangspunt. Dit houdt in dat alleen díe persoonsgegevens mogen worden verwerkt die echt noodzakelijk zijn. De Archiefwet en de AVG hebben dus verschillende uitgangspunten. Hierdoor moet in de praktijk soms het belang van archivering worden afgewogen tegen het belang van bescherming van persoonsgegevens.

5. Rechten van betrokkene

De AVG is voor een heel groot deel gericht op het verbeteren van de privacy rechten van de betrokkenen. Dit betekent dat er meer aandacht is voor de rechten van betrokkenen en dat een procedure daarvoor van groot belang is. Daarom worden de rechten van betrokkenen en hoe de gemeente verzoeken op grond van deze rechten behandelt, hierna beschreven.

5.1 Welke rechten hebben betrokkenen

5.1.1 Recht op informatie

De gemeente moet de betrokkene, op het moment dat de verwerking van persoonsgegevens plaatsvindt, hierover informeren. Dit recht vangt aan bij het vragen van persoonsgegevens (aan betrokkene) of bij de eerste verwerking van de persoonsgegevens (bij gegevens verkregen van anderen). Het informeren van de betrokkene kan op individueel niveau plaatsvinden, maar ook in de vorm van een algemene informatievoorziening door bijvoorbeeld het verwerkingsregister deels openbaar te maken en beschikbaar te houden voor betrokkenen. Op zijn/haar verzoek verstrekt de gemeente informatie aan de betrokkene.

5.1.2 Recht op inzage
Betrokkenen hebben de mogelijkheid om te controleren of, en op welke manier, zijn/haar gegevens worden verwerkt. En wanneer gegevens verwerkt worden, hebben zij het recht om inzage te verkrijgen in de persoonsgegevens die verwerkt worden.

5.1.3 Recht op rectificatie
Als duidelijk wordt dat de gegevens niet kloppen, kan de betrokkene een verzoek indienen bij de gemeente om dit te corrigeren. Deze wijziging moet meteen plaatsvinden. Met inachtneming van de doeleinden van de verwerking heeft de betrokkene het recht onvolledige persoonsgegevens aan te vullen.

5.1.4 Recht op gegevenswissing (vergetelheid)
In gevallen waar de betrokkene toestemming heeft gegeven om gegevens te verwerken, heeft de betrokkene het recht om de persoonsgegevens te laten verwijderen.

5.1.5 Recht van verzet
Betrokkenen hebben het recht aan de gemeente te vragen om hun persoonsgegevens niet meer te gebruiken. De persoonsgegevens moeten wel bij de gemeente opgeslagen blijven.

5.1.6 Recht op overdraagbaarheid (dataportabiliteit)
Betrokkenen kunnen op basis van de AVG gegevens die hem/haar zelf betreffen opvragen in gestructureerde, gangbare en digitaal leesbare vorm. Ook heeft hij/zij het recht deze gegevens aan een andere verwerkingsverantwoordelijke over te dragen of rechtstreeks te laten overdragen, zonder daarbij te worden gehinderd tenzij dit afbreuk doet aan rechten en vrijheden van anderen.

Dit recht kan alleen uitgeoefend worden ten aanzien van digitale gegevens en als de gegevensverwerking heeft plaatsgevonden op basis van een overeenkomst of door toestemming. Dit komt bij de gemeente niet tot zeer weinig voor. Het recht op dataportabiliteit bij de gemeente is daarom sterk beperkt.

5.1.7 Recht van bezwaar (verzet)
Betrokkenen hebben het recht om bezwaar te maken tegen de verwerking van zijn/haar persoonsgegevens als gegevensverwerking plaatsvindt op grond van een algemeen belang of een gerechtvaardigd belang. De gemeente zal de verwerking van de gegevens dan staken, tenzij er gerechtvaardigde gronden zijn voor de verwerking.

Betrokkenen wordt vooraf op dit recht gewezen, dat wil zeggen uiterlijk op het moment van het eerste contact. Wanneer een beroep wordt gedaan op het recht van bezwaar is er automatisch, gedurende de periode die nodig is om een besluit te nemen, sprake van een beperking van de verwerking van de persoonsgegevens. Het recht op bezwaar zoals hier genoemd is niet hetzelfde als het indienen van bezwaar op grond van de Algemene wet bestuursrecht.

5.2 Hoe oefenen betrokkenen hun rechten uit

5.2.1 Controle identiteit
Na ontvangst van een verzoek tot uitoefening van bovenstaande rechten, stuurt de gemeente een bevestigingsbrief. Hierin wordt de betrokkene verzocht zich te identificeren. Voordat de gemeente het verzoek namelijk in behandeling kan nemen, wordt de identiteit van de betrokkene altijd gecontroleerd. De betrokkene kan hiervoor een afspraak maken en zich identificeren bij Burgerzaken. Indien het verzoek gaat over een kind onder de 16 jaar, dan is het noodzakelijk dat de verzoeker ouderlijk gezag heeft. De gemeente controleert dat via de rechtbank in het gezagsregister.

5.2.2 Behandeling van het verzoek
De gemeente handelt het verzoek binnen vier weken af. Als het verzoek complex is of als veel verzoeken tegelijkertijd behandeld moeten worden, dan kan de termijn verlengd worden tot drie maanden nadat de gemeente het verzoek heeft ontvangen.

Ook kan de gemeente als het verzoek om veel gegevens gaat, de betrokkene verzoeken om zijn/haar verzoek te specificeren.

5.2.3 Beslissing op verzoek
In de beslissing laat de gemeente weten of en hoe aan het verzoek zal worden voldaan. Indien verlenging van de beslistermijn noodzakelijk is, dan zal binnen de beslistermijn dit worden bericht aan de betrokkene.

In het geval de gemeente niet – of gedeeltelijk – aan het verzoek voldoet, wordt dit altijd gemotiveerd in het besluit. Het kan bijvoorbeeld zijn dat bepaalde gegevens vanwege de openbare orde of veiligheid niet gedeeld mogen worden. Ook is het niet toegestaan om gegevens van andere personen in te zien.

6. Geautomatiseerde besluitvorming

6.1 Profilering

Profilering vindt plaats wanneer er een geautomatiseerde verwerking van persoonsgegevens plaatsvindt waarbij aan de hand van persoonsgegevens naar bepaalde persoonlijke aspecten van een persoon wordt gekeken om deze persoon te categoriseren en te analyseren, of om zaken te kunnen voorspellen. Voorbeelden van persoonlijke aspecten kunnen zijn; financiële situatie, interesses, gedrag of locatie.

Om profilering wat duidelijker te maken, gebruiken we het volgende voorbeeld: Wanneer een bezoeker op de gemeentelijke website naar een bepaalde dienst kijkt, mag de gemeente geen actie ondernemen om de dienst aan te bieden. Gemeenten mogen wel bekijken hoe vaak een bepaalde dienst bekeken is, maar dus niet specifiek gericht adverteren. Daarnaast geeft de wet aan dat er geen besluit mag worden genomen op basis van profilering. De gemeente maakt geen gebruik van profilering. Als zij dit gaat doen, dan zal dit alleen in overeenstemming met de voorwaarden uit de AVG zijn.

6.2 Big data en tracking

Door middel van Big data onderzoek en tracking mogen alleen gegevens verwerkt worden wanneer deze niet herleidbaar zijn tot een natuurlijk persoon. Daarnaast worden ze alleen verzameld voor onderzoek dat door, of namens, de gemeente wordt uitgevoerd. De verzamelde gegevens door Big data onderzoek en tracking zijn alleen de gegevens die door geautoriseerde personen zijn verzameld. Wanneer de gegevens worden omgezet in een dataset zal dataminimalisatie worden toegepast. Dit betekent dat alleen de data die echt nodig is voor het behalen van het doel gebruikt zullen worden. Daarnaast kunnen persoonsgegevens gepseudonimiseerd worden zodat zij niet herleidbaar zijn tot een persoon. De gemeente maakt geen gebruik van Big data onderzoek en tracking. Als zij dit gaat doen, dan zal dit alleen in overeenstemming met de voorwaarden uit de AVG zijn.

6.3 Inzet van camera's

Binnen de gemeente wordt onder bepaalde omstandigheden gebruik gemaakt van cameratoezicht, zoals vastgelegd in de Gemeentewet. Cameratoezicht wordt onder andere gebruikt voor het vergroten van de veiligheid op straat. Camera's kunnen een grote inbreuk maken op de privacy van diegene die gefilmd worden. Om de privacy zo goed mogelijk te waarborgen worden camera's alleen ingezet wanneer er geen andere manieren zijn om het doel te bereiken, en worden er eisen gesteld aan de inzet van camera's. De gemeente maakt geen gebruik van cameratoezicht zoals bedoeld in de Gemeentewet. Als zij dit gaat doen, dan zal dit alleen in overeenstemming met de voorwaarden uit de AVG zijn.

7. Slotbepalingen

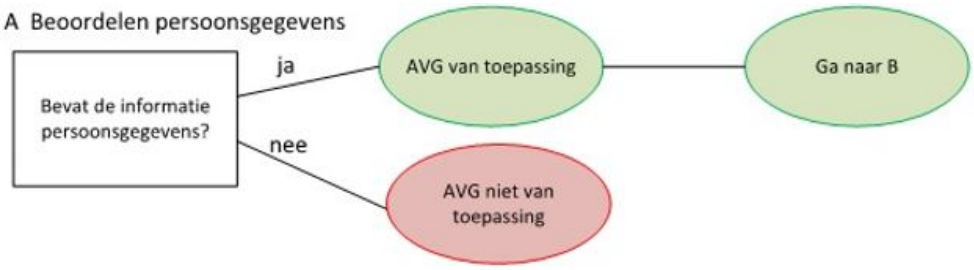
7.1 Evaluatie

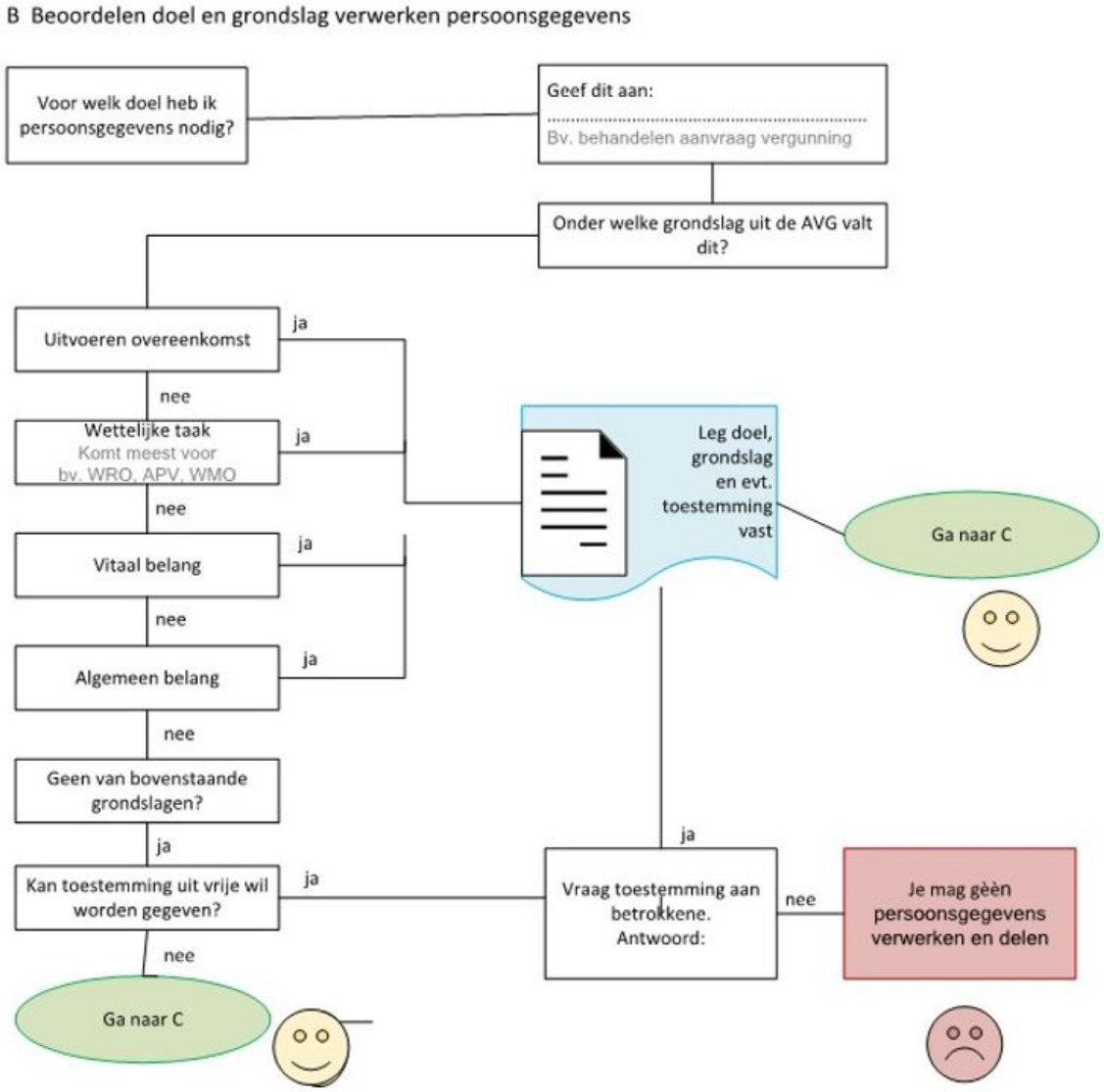
Het privacyreglement wordt eens per twee jaar geëvalueerd. Indien daartoe aanleiding bestaat, wordt het privacyreglement (eerder) bijgesteld.

7.2 Inwerkingtreding

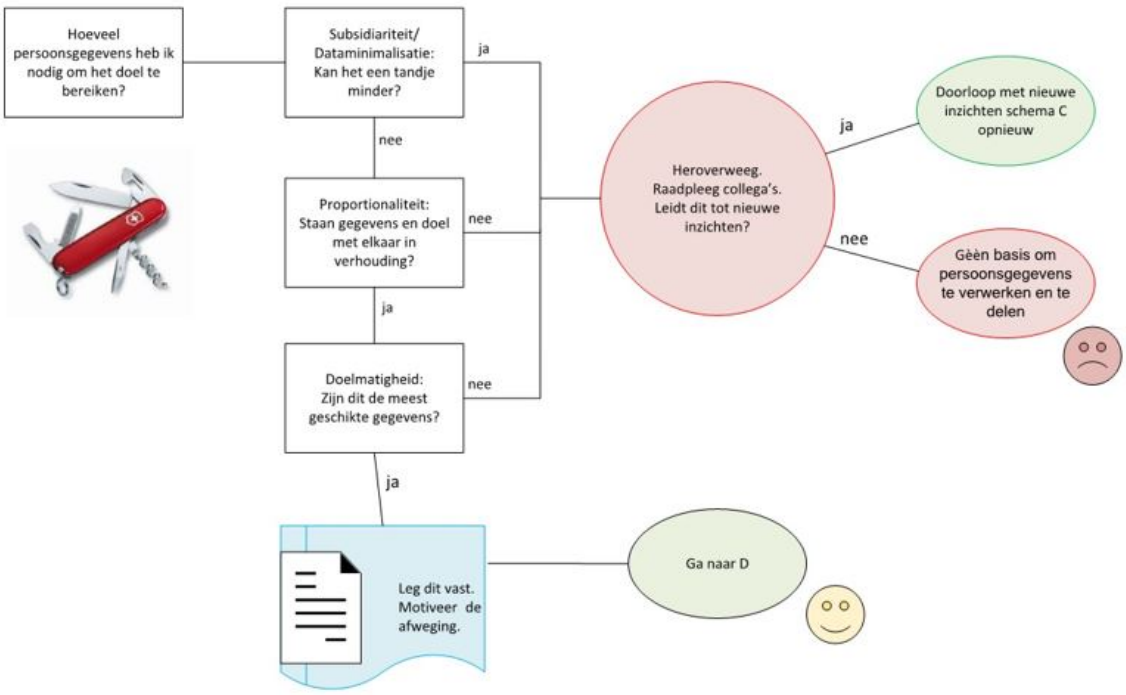
Dit privacyreglement treedt twee dagen na bekendmaking in werking.

Bijlage Afwegingskader zorgvuldig verwerken en delen van persoonsgegevens

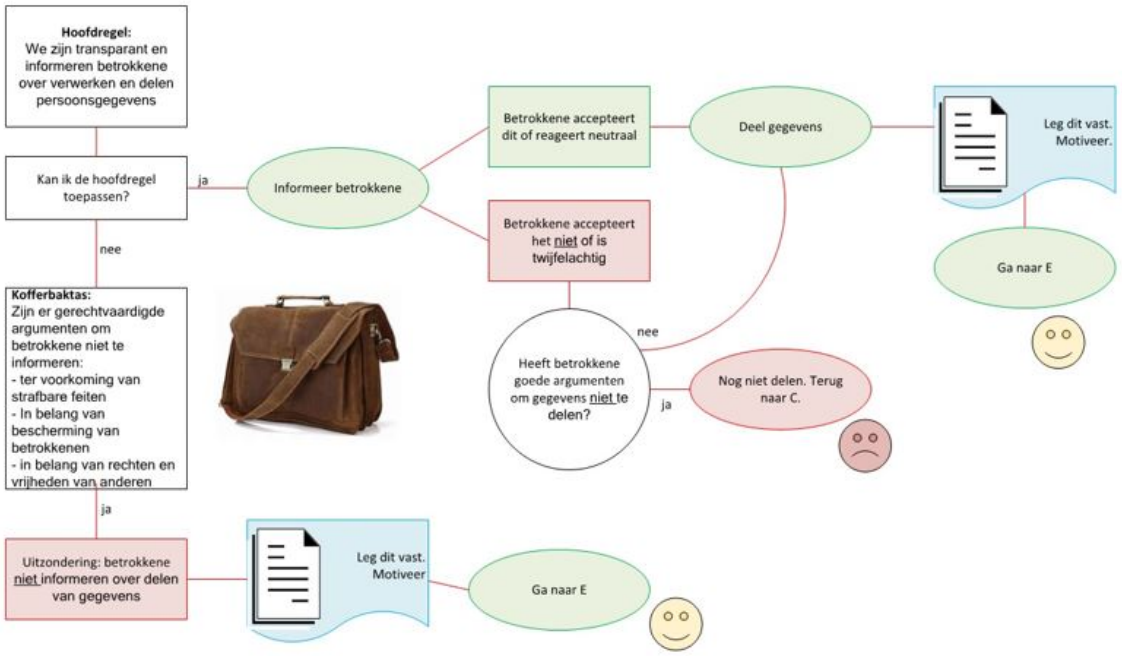




C Weging hoeveelheid persoonsgegevens: juridisch Zwitsers zakmes



D Weging informeren betrokkene over delen gegevens met anderen/partners



E Aandachtspunten veilig delen