Gemeente Voorst
Privacy protocollen
2023

Inhoudsopgave

Inleiding
Dit is een verzameling van privacy protocollen van de gemeente Voorst. In dit document worden verschillende werkinstructies/protocollen beschreven die te maken hebben met procedures die voortvloeien uit de Algemene verordening gegevensbescherming (AVG), Uitvoeringswet Algemene verordening gegevensbescherming (UAVG), Wet politiegegevens (Wpg) en andere relevante (privacy)wetgeving.

AVG en UAVG
De belangrijkste regels voor de omgang met persoonsgegevens in Nederland zijn vastgelegd in de Algemene verordening gegevensbescherming (AVG). De AVG is sinds 25 mei 2018 van toepassing geworden in de Europese Unie (EU). Dit betekent dat er sinds die datum dezelfde privacywetgeving geldt in de gehele EU. Op een aantal punten laat de AVG ruimte voor nationale keuzes. Deze keuzes zijn in Nederland uitgewerkt in de Uitvoeringswet AVG (UAVG).

Wet politiegegevens
De politie gebruikt allerlei persoonsgegevens om politietaken goed te kunnen uitvoeren. Bijvoorbeeld om daders van strafbare feiten op te sporen. De bescherming van persoonsgegevens bij de politie is geregeld in de Wet politiegegevens (Wpg). De Wpg is van toepassing voor de gemeente Voorst voor de boa's die zij in dienst heeft. De boa's voeren ook opsporende taken uit. De politiegegevens/persoonsgegevens die worden verwerkt als gevolg van die opsporende taak, vallen onder de Wpg.

Leeswijzer
Er wordt eerst uitgelegd hoe het werkproces van een DPIA eruit ziet. Vervolgens wordt er ingegaan op de rechten van betrokkene.

Data Protection Impact Assessment (DPIA)

Een DPIA (gegevensbeschermingseffectbeoordeling) is een verplichting die geldt voor projecten, regelgeving en beleid. Deze verplichting vloeit voort uit de AVG en de Wpg. Een DPIA heeft als doel om privacyrisico's in kaart te brengen. Met dit instrument bepaal en beoordeel je welke effecten het verwerken van de persoonsgegevens heeft op de privacy van betrokkenen. Zo kunnen vooraf maatregelen genomen worden om de privacyrisico's te verkleinen.

Wanneer voer ik een DPIA uit?

De gemeente Voorst moet in ieder geval een DPIA uitvoeren als wij:

- Systematisch en uitgebreid persoonlijke aspecten van mensen beoordelen, wat wij doen op basis van geautomatiseerde verwerking van persoonsgegevens (waaronder profilering) en waarop wij besluiten baseren die gevolgen hebben voor inwoners.
- Op grote schaal bijzondere persoonsgegevens verwerkt.
- Strafrechtelijke gegevens verwerkt.
- Op grote schaal en systematisch mensen volgt in een publiek toegankelijk gebied (bijv. cameratoezicht).

De Autoriteit Persoonsgegevens (AP) heeft een lijst vastgesteld met verwerkingen van persoonsgegevens waarbij een DPIA verplicht is. Deze lijst is toegevoegd als bijlage.

Hoe voer ik een DPIA uit?

Hieronder volgt een stappenplan met de stappen die moeten worden gevolgd om de DPIA zorgvuldig uit te kunnen voeren.

1. Verzamel alle relevante informatie over de voorgenomen regelgeving of het projectvoorstel waarbij persoonsgegevens worden verwerkt.

2. Bespreek de punten van het model (zie bijlage 2) bij voorkeur in groepsverband, waar diverse relevante expertises deel van uitmaken. Betrokkenheid van meerdere personen met verschillende achtergronden en expertises – denk aan expertise op het gebied van het betreffende beleidsterrein, regelgeving, (informatie)beveiliging en ICT – resulteert in een betere DPIA. Voor het uitvoeren van een DPIA dient in ieder geval iemand met privacy deskundigheid te worden betrokken. Leg de bevindingen schriftelijk vast in een rapport.

3. Consulteer waar passend de personen van wie persoonsgegevens worden verwerkt, de organisaties die hen vertegenwoordigen of andere belanghebbenden. Het betrekken van belanghebbenden stelt de uitvoerders van de DPIA in staat om de zorgen die spelen in kaart te brengen en tegelijkertijd transparant te zijn over de persoonsgegevens die verwerkt (zullen gaan) worden en de redenen daarvoor.
   Neem in het rapport op wat de geconsulteerde hebben geadviseerd en wat daarmee gedaan is. Indien geen consultatie plaatsvindt, motiveer deze beslissing in het rapport.

4. Leg het DPIA-rapport ter advisering voor aan de Functionaris Gegevensbescherming (FG – Yasmin Elbousaily). Neem in het rapport op wat de FG heeft geadviseerd en wat daarmee gedaan is. De AVG verplicht tot het inwinnen van advies bij de FG.

5. Indien de gegevensverwerking gepaard gaat met de bouw van een ICT-systeem, moet de Chief Information Security Officer (CISO – Marinus Wind) worden betrokken. De CISO toetst het projectplan op duidelijkheid over het verwerken van persoonsgegevens en op argumentatie over de wenselijkheid van het uitvoeren van een DPIA. Indien een DPIA gewenst is, wordt eveneens getoetst of de uitvoering heeft plaatsgevonden en of de maatregelen in het projectplan zijn opgenomen. Stel de DPIA daarom aan de CISO ter beschikking.

6. Wanneer uit de DPIA voor verwerkingen blijkt dat de verwerking een hoog risico oplevert en de verwerkingsverantwoordelijke er niet in slaagt om maatregelen te nemen om dat (rest)risico te beperken tot een acceptabel niveau, moet de AP voorafgaande aan de voorgenomen veerwerking worden geraadpleegd.

Volgens de Europese privacy toezichthouders is sprake van een onacceptabel hoog (rest)risico wanneer de betrokkene getroffen wordt met significante of onomkeerbare gevolgen die hij mogelijk niet te boven komt of de kans daarop aanzienlijk is.
Voor het schriftelijk advies van de AP over een voorgenomen verwerking geldt een termijn van acht weken. Die termijn kan, indien het gaat om iets complex, worden verlengd met zes weken. Neem in het rapport op wat de AP heeft geadviseerd en wat daarmee gedaan is.

7. Stuur het definitieve DPIA-rapport aan alle betrokkenen bij het opstellen van de DPIA, tenzij de regels met betrekking tot geheimhouding daaraan in de weg staan.

De uitkomst van een DPIA wordt verantwoord door middel van een rapport volgens het model in bijlage 2. Na vaststelling van de DPIA, dient de verwerkingsverantwoordelijke bij de verdere ontwikkeling van de voorgenomen regelgeving of het projectvoorstel rekening te houden met de uitkomsten van de DPIA.

De verwerkingsverantwoordelijke beoordeelt indien nodig of de verwerking overeenkomstig de DPIA wordt uitgevoerd. Hij doet dat in elk geval wanneer sprake is van een verandering van het risico van de verwerkingen. Risico's kunnen veranderen als gevolg van veranderingen in de onderdelen van de verwerkingen (gegevens, middelen, dreigingen, etc.), veranderingen in de context (doeleinden, faciliteiten etc.) of veranderingen in de organisatie of de samenleving.

Rechten van betrokkenen

Volgens de AVG en de Wpg hebben de personen waarvan persoonsgegevens worden verwerkt (betrokkenen) een aantal rechten als het gaat om wat je als gemeente doet met die persoonsgegevens. Dat zijn de rechten van betrokkenen. Onder de AVG hebben betrokkenen iets meer rechten dan onder de Wpg. De volgende rechten van betrokkenen zijn er:

- **Recht op informatie (AVG & Wpg)**
- **Recht op inzage (AVG & Wpg)**
- **Recht op rectificatie en correctie (AVG & Wpg)**
- **Recht op vergetelheid/vernietiging (AVG & Wpg)**
- **Recht op beperking van de verwerking (AVG)**
- **Recht op dataportabiliteit (AVG)**
- **Recht van bezwaar (AVG)**
- **Recht met betrekking tot geautomatiseerde besluitvorming en profilering (AVG)**

Er gelden specifieke regels voor de afhandeling van verzoeken van betrokkenen. Als een betrokkene een beroep doet op één van zijn rechten, moet de gemeente dit verzoek binnen één maand afhandelen. Wanneer dat niet lukt omdat het verzoek complex is, mag in uitzonderlijke gevallen deze maand (meerdere malen) verlengd worden tot een periode van maximaal drie maanden. De betrokkene moet geïnformeerd worden over het verlengen van de termijn.

De rechten van betrokkenen zijn absoluut. Dit houdt in dat de gemeente, specifiek het college van B&W, het uitoefenen van de rechten niet mag weigeren of een reden mag eisen. De gemeente moet voldoen aan het verzoek van een betrokkene. Hierop zijn wel drie uitzonderingen:

- **Rechten van anderen**
  Bij het uitoefenen van de rechten van betrokkenen, mag er geen inbreuk worden gemaakt op de rechten van anderen. De gemeente hoeft bijvoorbeeld geen inzage te geven in gegevens of dossiers van andere inwoners om te voldoen aan een inzageverzoek.
- **Bij misbruik van de rechten van betrokkenen**
  In uitzonderlijke gevallen mag de gemeente in geval van bijvoorbeeld een herhaald beroep op de rechten van betrokkenen, een verzoek afwijzen. Het moet daarbij gaan om ‘misbruik van recht’. Dit is bijvoorbeeld het geval als een inwoner 20 of 30 keer in een maand om precies dezelfde informatie vraagt, om daarmee de gemeente een administratief pak werk te bezorgen. Het eenmalig inzage geven in dezelfde informatie volstaat in dat geval.
- **Bij (het concrete vermoeden van) fysiek of mentaal gevaar van de betrokkene**
  Als het uitoefenen van een recht van de betrokkene in strijd is met een ander grondrecht van de betrokkene, hoeft in een uitzonderlijk geval geen gevolg te worden gegeven aan het verzoek van de betrokkene. Het gaat bijvoorbeeld om het inzien van een dossier van een jeugdige door de ouder(s) terwijl deze jeugdige in vertrouwen met de consulent heeft besproken dat er thuis sprake is van mishandeling of misbruik. Het inzage geven aan de ouder(s) in het dossier van de jeugdige, kan voor de jeugdige thuis tot grote problemen leiden. Alleen in dergelijke gevallen mag de gemeente een belangenafweging maken en het verzoek afwijzen van de ouder(s). Het is verstandig om samen met deskundigen deze afweging te maken en om de afweging (intern) goed op papier vast te leggen.

Recht op informatie

De gemeente is verplicht om de betrokkenen te informeren over de verwerking van hun gegevensverwerkingen. Betrokkenen hebben het recht om te weten wat er met hun persoonsgegevens gebeurt, waarom, hoe hun privacy beschermd wordt en hoe zij hun privacyrechten kunnen uitoefenen. Deze informatie wordt uiterlijk binnen één maand na ontvangst van de persoonsgegevens gegeven.

Wat zijn de regels voor dit recht?

Een betrokkene moet op de hoogte worden gesteld als zijn persoonsgegevens worden gebruikt. Daarbij hoort de betrokkene te worden verteld wat het doel is van het gebruik van de persoonsgegevens.

Volgens artikel 13 en 14 van de AVG en artikel 24a en 24b van de Wpg is het verplicht om betrokkenen te informeren over:

a) de identiteit van de gemeente;
b) de contactgegevens van de verwerkingsverantwoordelijke (het college);
c) de contactgegevens van de functionaris voor gegevensbescherming (FG);
d) de doelen (verwerkingsdoeleinden) waarvoor de persoonsgegevens worden gebruikt en indien dit doel verandert moet ook daarover informatie worden verstrekt;
e) de juridische grond (grondslag) waarop de verwerking van persoonsgegevens is gebaseerd, zoals bijv. overeenkomst, wet, publieke taak van de gemeente, toestemming of gerechtvaardigd belang;
f) indien er sprake is van verwerking op grond van gerechtvaardigd belang of vitaal belang, een toelichting van dat belang;
g) een uitleg over wie of welke organisaties de persoonsgegevens altijd zullen gaan gebruiken en ontvangen;
h) indien er persoonsgegevens buiten de EU worden gebruikt of opgeslagen: een verklaring (1) waar de gegevens opgeslagen zijn, (2) dat de gegevens conform wetgeving beveiligd zijn en (3) wat de waarborgen zijn om de privacy te beschermen.

Indien dat feitelijk en praktisch mogelijk is, dan verstrekt de gemeente ook de volgende informatie:

i) hoe lang de gegevens worden bewaard;
j) informatie over de rechten van de betrokkene;
k) als er sprake is van een verwerking van persoonsgegevens waarbij de grondslag toestemming is, dan moet de mogelijkheid om toestemming in te trekken ook worden vermeld;
l) de mogelijkheid dat de betrokkene altijd een klacht mag indienen bij de Autoriteit Persoonsgegevens (AP);
m) of, en zo ja op welke wijze, er sprake is van geautomatiseerde besluitvorming.

Indien de persoonsgegevens niet afkomstig zijn van de betrokkene zelf, dan moet de gemeente de betrokkene daarover ook informeren, aangevuld met informatie over waar de persoonsgegevens afkomstig zijn. De betrokkene moet weten dát en wát er over hem aan informatie is gedeeld.

Hoe wordt dit recht in de praktijk toegepast?

Veelgebruikte manieren voor het geven van deze informatie zijn een privacyverklaring, een privacyreglement, een register van verwerkingsactiviteiten of een dataregister. Deze informatie kan op de website van de gemeente worden gezet of er wordt verwezen naar informatie die op de gemeentelijke website staat.

De informatie wordt verstrekt aan de betrokkene op het moment dat deze – voor het eerst – zijn persoonsgegevens actief en bewust gaat delen met de gemeente. De AVG spreekt over ‘het moment van verkrijging van de gegevens’. Het mag ook op een later moment, maar wel binnen één maand. In de privacyverklaring[1] wordt ook kort weergegeven wat het beleid van de gemeente is met betrekking tot de privacy.

[1] Privacyverklaring gemeente Voorst: https://www.voorst.nl/fileadmin/user_upload/Homepage/Privacyverklaring_jun22.pdf

Recht op inzage

De betrokkene heeft het recht om zijn eigen persoonsgegevens die door de gemeente worden verwerkt, in te zien. Hier hoeft geen reden voor te worden gegeven. De betrokkene mag inzage in zijn gegevens vragen. Uitgangspunt is dat de betrokkene een kopie krijgt van de opgenomen persoonsgegevens. Er mag voor worden gekozen om de betrokkene fysiek inzage te geven in de systemen (een medewerker van de gemeente Voorst is hierbij aanwezig). Als het inzageverzoek digitaal wordt ingediend, dan krijgt de betrokkene via diezelfde weg de informatie (digitale kopieën).

Wat zijn de regels voor dit recht?

In artikel 15 van de AVG en artikel 25 van de Wpg is geregeld dat de betrokkene altijd het recht heeft om zijn persoonsgegevens in te zien. Daar hoeft de betrokkene geen reden voor op te geven.

Betrokkenen mogen op twee onderwerpen inzage hebben:

1. De betrokkene heeft het recht om op hoofdlijnen te worden geïnformeerd over het gebruik van zijn gegevens;
2. De betrokkene heeft recht om zijn eigen persoonsgegevens in te zien/te lezen.

Het recht van inzage overlapt dus deels met het recht op informatie. Ook bij het recht op inzage heeft de betrokkene het recht om te weten welke gegevens er worden gebruikt voor welke doeleinden. De reden is dat de gemeente transparant moet blijven en aan de betrokkene moet blijven uitleggen waarvoor diens gegevens gebruikt worden.
Over het gebruik van zijn gegevens heeft de betrokkene het recht om inzage te krijgen:

a) voor welke doelen (verwerkingsdoeleinden) de gegevens worden gebruikt door de gemeente;
b) om welke (categorieën van) persoonsgegevens het gaat;
c) wie de (beoogde) ontvangers en gebruikers zijn van de informatie over de betrokkene (met wie worden de gegevens uitgewisseld);
d) indien mogelijk: een opgave van de periode hoe lang de persoonsgegevens naar verwachting zullen worden opgeslagen (en indien dat niet mogelijk is, wordt gemeld wat de criteria zijn om te bepalen wat de bewaartermijnen zijn);
e) wat de privacyrechten van de betrokkene zijn en hoe hij deze kan uitoefenen;
f) dat de betrokkene het recht heeft een klacht in te dienen bij de Autoriteit Persoonsgegevens;
g) wanneer de gemeente van anderen dan de betrokkene persoonsgegevens krijgt: waar de persoonsgegevens vandaan komen;
h) het bestaan van geautomatiseerde besluitvorming.

De betrokkene heeft ook het recht om inzage krijgen in alle persoonsgegevens die over hem zijn vastgelegd. Het recht op inzage gaat alleen over inzage in de eigen persoonsgegevens, dus niet in de gegevens van andere inwoners of medewerkers. Het recht op inzage mag géén afbreuk doen aan de rechten van derden. Een inwoner kan dus geen inzage vragen in de notulen van de MT-vergadering, omdat daarin aantekeningen over veel meer inwoners en medewerkers zijn opgenomen (er kan wel een passage over de inwoner worden geknipt en aan de inwoner ter beschikking worden gesteld).

Om feitelijk inzage te geven, spreekt artikel 15 lid 3 AVG over het verstrekken van een kopie aan de betrokkene. Hiervoor mogen géén kosten in rekening worden gebracht. Pas als de betrokkene extra informatie of extra kopieën wil ontvangen (nadat de betrokkene volledig inzage heeft gehad in de eigen persoonsgegevens), mag daar eventueel een vergoeding van de kosten voor worden gevraagd. Of als het om kopieën gaat die niet-persoonsgegevens bevatten. Kosten in rekening brengen kan dus alleen bij wijze van hoge uitzondering[2]. Wel kan inzage geweigerd worden als het verzoek om inzage ongegrond of buitensporig is, of als de betrokkene expliciet en herhaaldelijk inzage vraagt in dezelfde gegevens (denk aan het geval van misbruik).

Bij het recht op inzage – omdat persoonsgegevens worden verstrekt – is het van belang om de identiteit van degene die het verzoek indient vast te stellen.

[2] https://www.autoriteitpersoonsgegevens.nl/themas/basis-avg/privacyrechten-avg/praktische-informatie-over-privacyrechten#mag-ik-kosten-in-rekening-brengen-voor-het-beschikbaar-stellen-van-gegevens-7248.

Hoe wordt dit recht in de praktijk toegepast?

Om de betrokkene op hoofdlijnen te informeren over de verwerking, kan gebruik worden gemaakt van de mogelijkheden die zijn beschreven bij het recht op informatie. De betrokkene kan bijvoorbeeld inzage krijgen in de dataregisters zodat hij weet waar en in welke systemen zijn gegevens worden gebruikt.

De gemeente is bevoegd om, voordat er inzage wordt gegeven, in redelijkheid, de identiteit van de betrokkene vast te stellen. Daarbij mag gevraagd worden om persoonlijk langs te komen bij de administratie met een identiteitsbewijs, maar de identiteit kan bijvoorbeeld ook worden vastgesteld doordat een inzageverzoek afkomstig is van een bekend e-mailadres van de betrokkene.

Bij de gemeente worden veel gegevens over inwoners gebruikt. Omdat er veel informatie is vastgelegd in veel systemen, mag de gemeente vragen om te specificeren wat de betrokkene wil inzien of wat deze aan informatie zoekt. Zo wordt voorkomen dat ‘blind’ in alle systemen van de school op gezocht moet worden naar de gevraagde informatie. Daar tegenover mag de betrokkene vragen in welke systemen persoonsgegevens zijn opgenomen.

Het is mogelijk om de betrokkene ook digitaal inzage te geven in diens gegevens. Doorgaans hebben inwoners reeds inzage in veel van hun verwerkte persoonsgegevens. De betrokkene kan worden uitgenodigd om ‘live’ inzage te geven in diens gegevens in de verschillende systemen indien het verstrekken van een kopie daarvan gecompliceerd is.

Het verstekken van een kopie is in beginsel op papier, maar mag ook digitaal als de betrokkene zijn verzoek om inzage digitaal heeft ingediend. Daarbij worden dus digitale kopieën toegezonden, gebruik hiervoor een gangbaar elektronisch formaat (bijv. in een pdf-bestand) via Filecap.

Let er op dat de gemeente niet verplicht is om een betrokkene inzage te geven in zijn dossier of informatie, als daarin persoonsgegevens van/over anderen is opgenomen. Een inwoner heeft geen recht op inzage van de mailbox van een medewerker, de medewerker stelt – op verzoek van de inwoner – slechts de e-mail ter beschikking die (alleen) over de inwoner gaat. Als een verslag wordt gedeeld dat (deels) over de inwoner gaat, mogen daarin dus stukken zwart worden als die niet over de inwoner gaan.

Recht op rectificatie (correctie)

De gemeente (het college) moet zorgen dat persoonsgegevens die worden verwerkt accuraat zijn en blijven. Wanneer de persoonsgegevens niet (meer) kloppen, heeft de betrokkene het recht om deze te laten corrigeren of aan te vullen. Eventuele correcties worden – zo mogelijk – doorgegeven aan de organisaties die eerder de verkeerde informatie hebben ontvangen.

Wat zijn de regels voor dit recht?

In artikel 16 AVG is geregeld dat een betrokkene het recht heeft om onjuiste persoonsgegevens te laten wijzigen, of om zijn persoonsgegevens aan te vullen.

Onder het recht van rectificatie is de gemeente ook verplicht om correcties of verwijderingen door te geven aan alle organisaties waarmee de persoonsgegevens van de betrokkene zijn gedeeld. Tenzij dit onmogelijk is of onevenredig veel inspanning vraagt. Denk bijvoorbeeld aan een samenwerkingsverband waar de verkeerde geboortedatum of contactgegevens van de inwoner aan zijn doorgegeven.

Als een betrokkene daarom vraagt, moet de instelling ook melden welke organisaties op de hoogte zijn gesteld van de wijzigingen (rectificaties).

Hoe wordt dit recht in de praktijk toegepast?

In geval van discussie over de juistheid van de gegevens, neemt de onderwijsinstelling een beslissing die uitgaat van de feiten.

Denk bijvoorbeeld aan de naam van een inwoner: de gemeente mag daarbij uitgaan van de informatie die is opgenomen in de openbare registers (zoals de GBA) of op het identiteitsbewijs van de inwoner is vermeld. De inwoner mag gevraagd worden om aan te tonen dat de persoonsgegevens niet juist zijn (of: wat dan wel de juiste gegevens zijn).

Soms is het niet mogelijk een rectificatie direct uit te voeren in een dossier. Er kan dan gebruik gemaakt worden van een notitie, aanvulling op het dossier of door de veerklaring/toelichting van de betrokkene op te nemen in het dossier.

Een voorbeeld is het opnemen van het geslacht van de betrokkene. De gemeente houdt het geslacht aan dat is opgenomen in de officiële registers (GBA). De gemeente kan dan een verklaring opnemen dat de betrokkene voortaan wil worden aangesproken als iemand van het andere geslacht. Zodra deze wijziging in de officiële registers is aangepast, wijzigt de gemeente dit ook in de administratie.

Recht op vergetelheid (recht op gegevenswissing)

Onder bepaalde omstandigheden mag een betrokkene verzoeken om zijn persoonsgegevens te laten verwijderen. Daarnaast heeft een betrokkene het recht om helemaal ‘vergeten te worden’, zodat hij bijvoorbeeld op het internet niet voor altijd (ten onrechte) met zijn verleden wordt geconfronteerd. Vanwege een aantal wettelijke bewaartermijnen geldt het recht op vergetelheid niet volledig voor dossiers van inwoners.

Wat zijn de regels voor dit recht?

De betrokkene mag volgens artikel 17 AVG aan de gemeente vragen om diens persoonsgegevens geheel te verwijderen in de volgende gevallen:

- de persoonsgegevens zijn niet langer nodig voor het doel waarvoor zij oorspronkelijk verstrekt zijn;
- de verwerking van persoonsgegevens vond plaats op basis van toestemming en de betrokkene trekt zijn toestemming in (denk aan toestemming voor het gebruik van foto’s);
- de betrokkene maakt bezwaar tegen de verwerking;
- de persoonsgegevens zijn onrechtmatig verwerkt (de gemeente mag de betreffende persoonsgegevens dan in geen geval hebben);
- een wettelijke nationale verplichting stelt dat de persoonsgegevens moeten worden vernietigd;
- het gaat om internetdiensten zoals sociale media.

Aan een verzoek tot het verwijderen van gegevens wordt geen uitvoering gegeven als:

- de verwijdering in strijd is met het recht op vrijheid van meningsuiting en informatie;
- de gemeente volgens de wet verplicht wordt om die persoonsgegevens wél te verwerken of te bewaren (wettelijke bewaartermijnen);
- het algemeen belang op het gebied van volksgezondheid geldt;
- met het oog op archivering het algemeen belang geldt, bijvoorbeeld in het geval van wetenschappelijk of historisch onderzoek of statistische doeleinden;
- de gegevens nodig zijn voor het voeren of voorbereiden van een juridische procedure waarin de betreffende gegevens nodig zijn.

Ook in geval van bijzondere omstandigheden zoals opgenomen in artikel 23 AVG hoeft de instelling niet aan een verzoek tot gegevenswissing te voldoen. De gemeente maakt dan een belangenafweging tussen het belang van de betrokkene (privacybelang) en het belang van de gemeente om de gegevens toch te bewaren. Hiervan is volgens de AVG sprake wanneer de gegevens nodig zijn voor:

- de nationale veiligheid, landsverdediging of openbare veiligheid;
- de voorkoming of opsporing van strafbare feiten;
- de algemene (economische of financiële) doelstellingen van de Europese en nationale overheid;
- de bescherming van de onafhankelijkheid van de rechtspraak (bijv. wissen van gepubliceerde uitspraken);
- van voorkomen en opsporen van overtredingen van beroepscodes voor gereglementeerde beroepen (denk aan tuchtzaken);
- een taak op het gebied van inspectie en toezicht;
- de bescherming van de rechten van anderen.

In het kader van deze hiervoor genoemde bijzondere omstandigheden wordt ook wel het voorkomen van misbruik van privacywetgeving genoemd als grond om een verzoek tot vergetelheid af te wijzen. In geval van gegevenswissing moet de gemeente ook alle andere organisaties die de persoonsgegevens hebben gekregen informeren dat de betreffende persoonsgegevens moeten worden gewist.

Hoe wordt dit recht in de praktijk toegepast?

Het recht wordt zonder enige vertraging uitgevoerd, maar binnen één maand na het verzoek moet de betrokkene geïnformeerd worden over de afhandeling van het verzoek.

De verwerkingsverantwoordelijke is verplicht om iedereen met wie de (verwijderde) persoonsgegevens zijn uitgewisseld, te informeren over de vernietiging. Tenzij dit onmogelijk is of onevenredig veel inspanning vraagt.

De gemeente houdt bij het recht van gegevenswissing rekening met de interne en wettelijke bewaartermijnen (gebaseerd op wettelijke bewaartermijnen). Hiervoor kan de selectielijst[3] gebruikt worden.

Verwijderen van gegevens moet gebaseerd zijn op een grond zoals opgenomen in de vorige paragraaf. De gemeente hoeft dus niet persoonsgegevens te verwijderen omdat de inwoner het niet aanstaat dat de gemeente deze verwerkt. Er mag gevraagd worden naar een onderbouwing.

Een complexe eis die in de praktijk komt bij het recht van gegevenswissing, is dat in principe persoonsgegevens uit back-ups moeten worden verwijderd. Als dat verwijderen feitelijk niet mogelijk is of te complex, dan moet daar rekening mee worden gehouden bij het eventuele terugzetten van de back-up: de gegevenswissing moet dan worden bijgehouden Bijvoorbeeld wanneer de gemeente persoonsgegevens heeft verwijderd in het kader van gegevenswissing, is het natuurlijk niet de bedoeling dat na het terugzetten van een back-up de gewiste persoonsgegevens worden teruggezet en de betrokkene een nieuw verzoek tot gegevenswissing moet indienen. De gemeente moet die gegevenswissing dan uit zichzelf opnieuw uitvoeren.

[3] https://vng.nl/sites/default/files/2020-02/selectielijst_20200214.pdf

Recht op beperking van de verwerking

Het recht op beperking van verwerking houdt in dat betrokkenen in een beperkt aantal gevallen tijdelijk de verwerking van hun persoonsgegevens stil kunnen laten zetten. De verwerking mag dan alleen nog maar in bepaalde gevallen. Dit kan voorkomen als iemand het niet eens is met het gebruik van bepaalde gegevens en een beroep heeft gedaan op correctie van die gegevens. Totdat daarover is beslist worden die betwiste gegevens niet gebruikt door de gemeente.

Wat zijn de regels voor dit recht?

Het recht op beperking van de verwerking houdt volgens artikel 18 AVG in dat de gemeente de persoonsgegevens (tijdelijk) niet mag gebruiken of wijzigen. Het feit dat *'de verwerking van de persoonsgegevens beperkt is'*, moet daar de verwerkingsverantwoordelijke duidelijk in het systeem, de software of het bestand zijn aangegeven. Vergelijk het recht op beperking van de verwerking met het 'bevriezen' van de huidige stand van zaken. De gebruikers en ontvangers van deze bevroren persoonsgegevens moeten kunnen vaststellen dat de verwerking beperkt is. Wanneer de beperking weer wordt opgeheven, moet de betrokkene daar weer van op de hoogte worden gebracht.

Het beperken van de verwerking is mogelijk in de volgende gevallen:

a) de juistheid van de persoonsgegevens wordt betwist door de betrokkene, en – gedurende de periode die de instelling nodig heeft om de juistheid van de persoonsgegevens te controleren – mogen de betwiste persoonsgegevens niet verder worden verwerkt;
b) 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;
c) de verwerkingsverantwoordelijke heeft de persoonsgegevens niet meer nodig voor de verwerkingsdoeleinden en wil de persoonsgegevens gaan verwijderen, maar de betrokkene heeft deze nodig voor het instellen, uitoefenen of onderbouwen van een rechtsvordering;
d) de betrokkene heeft bezwaar gemaakt tegen de verwerking (artikel 21, eerste lid van de AVG), en is in afwachting van het antwoord op de vraag of de gerechtvaardigde gronden van de verwerkingsverantwoordelijke zwaarder wegen dan de privacyrechten van de betrokkene.

Na het verzoeken van het beperken van de verwerking door de betrokkene mag de gemeente de persoonsgegevens (waar het verzoek over gaat) alleen nog verwerken:

a) met toestemming van de betrokkene;
b) voor het instellen, uitoefenen of onderbouwen van een rechtsvordering;
c) ter bescherming van de rechten van andere natuurlijke personen of rechtspersoon/-personen;
d) om gewichtige redenen van algemeen belang voor de Europese Unie of voor een lidstaat.

Dit recht wordt gebruik in het geval de gemeente bezig is met de uitvoering van een recht van de betrokkenen. De betrokkene kan vragen om – totdat er duidelijkheid is gegeven over een ander ingediend verzoek rondom de rechten van betrokkene – de persoonsgegevens niet te gebruiken.

Hoe wordt dit recht in de praktijk toegepast?

Een eerste voorbeeld is dat de juistheid van de persoonsgegevens door de betrokkene ter discussie wordt gesteld: de inwoner wil niet dat de gemeente bepaalde persoonsgegevens deelt. Zolang die 'discussie' loopt, mag de gemeente de betwiste persoonsgegevens niet gebruiken of uitwisselen.

Een tweede voorbeeld is dat de betrokkene een beroep heeft gedaan op gegevenswissing, en de gemeente betwist dat de betrokkene dat recht heeft. In dat geval kan de situatie worden 'bevroren' totdat een en ander is uitgezocht, of dat de toezichthouder of rechter een uitspraak heeft gedaan.

Een derde voorbeeld is een discussie over het postadres van een inwoner: zolang er geen duidelijkheid is over de juistheid van dat adres stuurt de gemeente geen post naar dat (ogenschijnlijk foutieve) adres.

Het recht van beperking van de verwerking zal in de praktijk niet vaak voorkomen. Het biedt vooral een oplossing als er een discussie is over het gebruik van persoonsgegevens, en wat de gemeente in de tussentijd doet. De gemeente heeft immers een maand de tijd om te beslissen over een verzoek van de betrokkene, en om van verkeerde persoonsgegevens te voorkomen kunnen de gegevens bevroren worden.

Recht op dataportabiliteit (overdraagbaarheid)

Het recht op dataportabiliteit houdt in dat een betrokkene zijn digitale persoonsgegevens meeneemt en overdraagt aan een andere organisatie. Het recht op dataportabiliteit geldt voor een deel van de digitale inwonergegevens (en niet een papieren dossier). Het doel van dit recht is om de zeggenschap van de betrokkene over en uitwisseling van hun persoonsgegevens te vergroten. De betrokkene heeft een recht op een kopie in een gangbare en machine-leesbare vorm. Daarmee kan een betrokkene gemakkelijk naar een andere gemeente om zijn gegevens in te laten lezen.

Wat zijn de regels voor dit recht?

Artikel 20 AVG meldt dat een betrokkene zijn gegevens van een verwerkingsverantwoordelijke moet kunnen verkrijgen in gestructureerde, gangbare en machine-leesbare vorm en het recht heeft deze gegevens aan een andere verwerkingsverantwoordelijke over te dragen, zonder daarbij te worden gehinderd tenzij dit afbreuk doet aan rechten en vrijheden van anderen.

Het recht geldt alleen in geval:

- er sprake is van geautomatiseerde processen;
- en het (alleen) gaat om één van de volgende wettelijke grondslagen waarop het gebruik van persoonsgegevens is gebaseerd:
  - de verwerking is noodzakelijk voor de **uitvoering van een overeenkomst** waarbij de betrokkene partij is, of om op verzoek van de betrokkene vóór de sluiting van een overeenkomst maatregelen te nemen;
  - de betrokkene heeft **toestemming** gegeven voor de verwerking van zijn persoonsgegevens (dit doorgaans niet van toepassing in het onderwijs – beeldmateriaal uitgezonderd -).
- en de persoonsgegeven zijn verstrekt door, of gerelateerd zijn aan de betrokkene;
- en er geen rechten en/of vrijheden van derden worden geschonden als dit recht wordt uitgeoefend in de praktijk.

De te leveren persoonsgegevens van inwoners zijn beperkt tot:

- gegevens die de betrokkenen zelf actief en bewust hebben verstrekt aan de school;
- persoonsgegevens die indirect zin verstrekt of ontstaan, door het gebruik (door betrokkene) van diensten of apparaten.

De gemeente hoeft dus niet alle persoonsgegevens van een betrokkene aan te leveren in een machine-leesbaar formaat. Betrokkenen hebben wel recht om alle gegevens in te zien (of een kopie te ontvangen) maar die data valt niet onder het recht van dataportabiliteit.

Hoe wordt dit recht in de praktijk toegepast?

Binnen de Europese Unie is er discussie over hoe het recht van dataportabiliteit moet worden uitgelegd. Het gaat dan met name over het leveren van de ‘eigen’ persoonsgegevens van een betrokkene: wat zijn dat precies? Dat kan heel nauw of breed worden uitgelegd. Wat dit voor de gemeente tot in detail betekent, is dus voorlopig onduidelijk.

Een betrokkene heeft recht op overdraagbaarheid voor zover het gaat om door hemzelf verstrekte gegevens. Volgens de richtlijn van de gezamenlijke Europese privacy toezichthouders, gaat het bij een verzoek tot dataportabiliteit ook om de persoonsgegevens die op basis van de activiteiten van gebruikers gegenereerd en verzameld worden. Onder dataportabiliteit vallen volgens de uitleg bij de wet wél indirecte persoonsgegevens (denk aan hartslaggegevens die zijn verzameld in een app), maar géén afgeleide gegevens (als de app de hartslaggegevens analyseert en een advies opstelt, valt die analyse en advies niet onder het recht van dataportabiliteit).

Indien dat technisch mogelijk is, heeft de inwoner het recht dat zijn gegevens rechtstreeks van de ene verwerkingsverantwoordelijke naar de andere worden doorgezonden (dus van gemeente naar gemeente).

Het verschil met het recht op inzage, is dat de betrokkene het bestand met persoonsgegevens kan hergebruiken zonder dat de informatie opnieuw ingevoerd moet worden. Er wordt geen papieren of digitale kopie gegeven, maar een herbruikbaar bestand.

Na het verstrekken van een digitaal bestand, is de gemeente niet meer verantwoordelijk voor wat de betrokkene daarmee doet. Het leveren van het bestand aan de betrokkene ontslaat de gemeente van de verantwoordelijkheid voor dat bestand. Dus de gemeente is niet

verantwoordelijk voor de verwerking van deze gegevens door een andere gemeente die het bestand van de betrokkene ontvangt.

Het recht van dataportabiliteit doet niets af aan de geldende bewaartermijnen. Na levering van het bestand mogen de persoonsgegevens conform de regels van bewaartermijnen worden bewaard. Als een bestand aan de betrokkene is geleverd in het kader van dataportabiliteit, mogen die gegevens dus niet verwijderd worden bij de verstrekkende gemeente.

De Autoriteit Persoonsgegevens heeft de richtlijn dataportabiliteit van de gezamenlijke Europese privacy toezichthouders gepubliceerd:
https://autoriteitpersoonsgegevens.nl/uploads/imported/nederlandse_vertaling_guidelines_dataportabiliteit.pdf

Recht van bezwaar (recht op verzet)

Een betrokkene mag in bepaalde gevallen bezwaar maken tegen (verder) verwerken van persoonsgegevens. Op basis van dat bezwaar moet de gemeente afwegen of de in het bezwaar beschreven bijzondere persoonlijke omstandigheden van de betrokkene zwaarder (moeten) wegen dan het belang dat de gemeente heeft bij het gebruik van de persoonsgegevens van de betrokkene. Als dat zo is, dan gebruikt de gemeente de persoonsgegevens niet (meer). Totdat deze afweging door de gemeente is gemaakt, mag de gemeente (het college) tijdelijk geen gebruik maken van de persoonsgegevens van de betrokkene.

Wat zijn de regels voor dit recht?

De betrokkene heeft volgens artikel 21 AVG het recht om bezwaar te maken tegen verwerking van zijn persoonsgegevens. De betrokkene vraagt dan om (een deel van) zijn persoonsgegevens niet meer te gebruiken.

Naast bezwaar maken tegen gebruik van persoonsgegevens voor direct-marketingdoeleinden, kan de betrokkene vanwege bijzondere persoonlijke omstandigheden bezwaar maken tegen verwerking van zijn persoonsgegevens in geval van:

a) een gerechtvaardigd belang (artikel 6 lid 1 onder f AVG): de verwerking van persoonsgegevens van de inwoner is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de gemeente of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de inwoner die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan de belangen van de gemeente (met name wanneer de betrokkene een kind is);
b) een algemeen belang (artikel 6 lid 1 onder e AVG): de verwerking van persoonsgegevens van de leerling is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag dat aan de gemeente is opgedragen;
c) profilering (artikel 22 AVG): er worden geen beslissingen genomen over de inwoner of op basis van persoonsgegevens van de inwoner die zijn verkregen op basis van profilering.

Er moet wel sprake zijn van bijzondere persoonlijke omstandigheden. De Autoriteit Persoonsgegevens geeft als voorbeeld dat iemand die als patiënt mee heeft gedaan aan een medisch onderzoek en er later achter komt dat een bekende als onderzoeker bij dat centrum werkt. De patiënt heeft dan een bijzonder belang om bezwaar te maken. De betrokkene moet dit dus onderbouwen, en niet met één zin stellen dat hij een ‘zwaarwegend belang heeft’ om bezwaar te maken.

In geval van een door de betrokkene ingediend bezwaar, stopt de verwerkingsverantwoordelijke met het verwerken van de persoonsgegevens tenzij:

- de gemeente dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene, of;
- de verwerking van persoonsgegevens verband houdt met de instelling, uitoefening of onderbouwing van een rechtsvordering.

De gemeente is verplicht om de inwoners goed te informeren over en te wijzen op het recht van bezwaar.

Hoe wordt dit recht in de praktijk toegepast?

In de hiervoor genoemde gevallen maakt de gemeente (het college) een belangenafweging: het belang van de gemeente (het college) om de persoonsgegevens wél te gebruiken weegt zwaarder dan het belang dat de betrokkene heeft bij bescherming van diens privacy. Als de gemeente dan zwaarwegender belang heeft, dan wordt het bezwaar afgewezen en wordt het gebruik van de persoonsgegevens voortgezet.

Zo lang het niet duidelijk is of het bezwaar gegrond is, mag de gemeente de persoonsgegevens niet verwerken. Er moet dus eerst worden vastgesteld of er dwingende gerechtvaardigde gronden voor de verwerking zijn voor de gemeente, en dat deze zwaarder wegen dan de belangen, rechten en vrijheden van de inwoner.

Een inwoner kan en mag altijd bezwaar maken, maar hij moet de zwaarwegende redenen wel aanvoeren: de inwoner moet kunnen aantonen dat de verwerking van zijn persoonsgegevens nadelige effecten voor hem heeft of kan hebben. De inwoner moet goed onderbouwen waarom hij direct geraakt wordt door de verwekring van persoonsgegevens door de gemeente. Principieel het

niet eens zijn met de verwerking van persoonsgegevens is niet voldoende: de inwoner moet nadeel ondervinden van de verwerking. Daarbij weegt de gemeente de belangen af: het belang van de gemeente om toch die persoonsgegevens te verwerken, tegenover het privacybelang van de inwoner.

Er kan geen bezwaar worden ingesteld tegen een verwerking van persoonsgegevens die noodzakelijk is om een wet na te komen of om een overeenkomst uit te voeren. Bezwaar is alleen mogelijk als de grondslag voor verwerking algemeen belang of gerechtvaardigd belang is. Als een inwoner of de ouders van een minderjarige inwoner toestemming hebben gegeven voor de verwerking van hun persoonsgegevens, dan mogen zij die toestemming altijd intrekken. Daar is dus geen bezwaar voor nodig: het intrekken van toestemming is voldoende.

Recht om niet te worden onderworpen aan geautomatiseerde individuele besluitvorming (waaronder profilering)

Bij geautomatiseerde individuele besluitvorming neemt een computersysteem een beslissing op basis van een geautomatiseerde verwerking van persoonsgegevens. Eventuele uitkomsten kunnen daardoor niet worden gecorrigeerd en er wordt geen rekening gehouden met de persoonlijke omstandigheden van de betrokkene. Hier gelden beperkingen voor. Betrokkenen hebben het recht om hier niet aan onderworpen te worden, wanneer dit rechtsgevolgen heeft of het hen op een andere wijze in een aanzienlijke mate treft.

Wat zijn de regels voor dit recht?

Artikel 22 AVG regelt het recht van de betrokkene om niet 'onderworpen' te worden aan profilering en geautomatiseerde besluitvorming. Er is géén (noemenswaardige) menselijke tussenkomst bij beslissingen die gebaseerd zijn op de geautomatiseerde verwerking van persoonsgegevens. Denk bijvoorbeeld aan een automatische weigering van een online ingediende aanvraag, of afhandeling van een digitale sollicitatieprocedure zonder menselijke tussenkomst. De betrokkene heeft altijd het recht dat een mens over hem en zijn omstandigheden beslist, en niet dat de computer een oordeel velt. Dit recht wordt ook wel 'het recht op een menselijke blik bij besluiten' genoemd.

Profilering is het indelen van personen in categorieën (profielen) op basis van hun persoonsgegevens. Op basis van deze profielen kunnen vervolgens (geautomatiseerde) individuele besluiten worden genomen, zoals het verlenen van krediet door een financiële instelling.

Met geautomatiseerde besluitvorming wordt bedoeld: het nemen van beslissingen met automatische processen of middelen zonder dat er menselijke tussenkomst is. Daarom is er in de AVG een verbod opgenomen op geheel automatische besluitvorming, tenzij er aan bepaalde voorwaarden is voldaan. Deze voorwaarden zijn:

a) de geautomatiseerde besluitvorming is noodzakelijk om een overeenkomst te sluiten met de betrokkene;
b) de geautomatiseerde besluitvorming is gebaseerd op Europese of nationale regels; of
c) de betrokkene heeft vooraf uitdrukkelijk toestemming gegeven voor deze geautomatiseerde besluitvorming (de gevolgen moeten in begrijpelijke taal zijn uitgelegd).

Betrokkenen hebben het recht om niet onderworpen te worden aan een enkel op geautomatiseerde verwerking, (waaronder profilering), gebaseerd besluit, wanneer dit:

- rechtsgevolgen heeft voor de betrokkene; of
- het de betrokkene anderszins in aanzienlijke mate treft.

De geautomatiseerde besluitvorming moet dus wel gevolgen hebben voor de betrokkene, als hier geen sprake van is valt dit niet onder het verbod.

De betrokkene heeft het recht om:

- geïnformeerd te zijn over geautomatiseerde besluitvorming;
- zijn standpunt kenbaar te maken;
- bezwaar te maken tegen geautomatiseerde besluitvorming;
- het geautomatiseerd genomen besluit aan te vechten;
- te vragen om een nieuwe beoordeling door een mens.

Een voorbeeld van geautomatiseerde besluitvorming en profilering komt uit de Verenigde Staten. Daar houdt een bank bij de aanvraag voor een lening rekening met het systeem dat de betrokkene gebruikt om de lening aan te vragen. Als de aanvrager een dure tablet of bepaalde software gebruikt, is de kans – volgens de bank – kleiner dat de aanvrager de lening niet meer terugbetaalt. De lening wordt dan sneller verleend. Hierbij is er sprake van geautomatiseerde besluitvorming (de computer beslist) én profilering: de ervaring dat mensen met een bepaalde dure tablet een lening sneller afbetalen wordt meegewogen bij de aanvraag.

Hoe wordt dit recht in de praktijk toegepast?

Zorg dat de betrokkenen goed zijn geïnformeerd over de besluitvorming. Door er voor te zorgen dat er altijd 'menselijk tussenkomst' is (in de keten van besluitvorming), wordt voorkomen dat er sprake is van geautomatiseerde besluitvorming. Een computer mag wel adviseren, maar dus niet beslissen. Dus niet: 'the computer says no'.

Van geautomatiseerde besluitvorming kan sprake zijn bij het gebruik van digitaal leer- en toetsmateriaal, of bij digitale toetsing en examinering waarbij de betrokkene geautomatiseerd geïnformeerd wordt over de uitkomst of wordt uitgesloten van examen indien niet aan een aantal vooraf opgegeven criteria is voldaan. Ook bij het proces van aanmelden en inschrijven kan sprake zijn van geautomatiseerde besluitvorming waarbij de inschrijving of aanmelding van een inwoner niet in behandeling wordt genomen indien deze niet alle vereiste gegevens heeft ingediend of niet aan de criteria voldoet.

De Autoriteit Persoonsgegevens heeft de richtlijn ‘automated individual decision-making and profiling’ van de gezamenlijke Europese privacytoezichthouders gepubliceerd: https://autoriteitpersoonsgegevens.nl/uploads/imported/guidelines_on_profiling_wp251rev01_enpdf.pdf

Bijlage 1 – Lijst van verwerkingen van persoonsgegevens waarvoor een DPIA verplicht is

De AP stelt dat voor de volgende verwerkingen van persoonsgegevens een DPIA verplicht is:

1. **Heimelijk onderzoek**
   Grootschalige verwerkingen van persoonsgegevens en/of stelselmatige monitoring waarbij informatie wordt verzameld door middel van onderzoek zonder de betrokkene daarvan vooraf op de hoogte te stellen. Een DPIA is ook verplicht in geval van heimelijk cameratoezicht door werkgevers in het kader van diefstal- of fraudebestrijding door werknemers.
2. **Zwarte lijsten**
   Verwerkingen waarbij persoonsgegevens betreffende strafrechtelijke veroordelingen en strafbare feiten, gegevens over onrechtmatig of hinderlijk gedrag of gegevens over slecht betalingsgedrag door bedrijven of particulieren worden verwerkt en gedeeld met derden.
3. **Fraudebestrijding**
   Grootschalige verwerkingen van (bijzondere) persoonsgegevens en/of stelselmatige monitoring in het kader van fraudebestrijding (bijv. fraudebestrijding door sociale diensten of door fraudeafdelingen van verzekeraars).
4. **Creditscores**
   Grootschalige verwerkingen en/of stelselmatige monitoring die leiden tot of gebruik maken van inschattingen van de kredietwaardigheid van natuurlijke personen.
5. **Financiële situatie**
   Grootschalige verwerkingen en/of stelselmatige monitoring van financiële gegevens waaruit de inkomens- of vermogenspositie of het bestedingspatroon van mensen valt af te leiden (bijv. overzichten van bankoverschrijvingen of overzichten van mobiele- of pinbetalingen).
6. **Genetische persoonsgegevens**
   Grootschalige verwerkingen en/of stelselmatige monitoring van genetische persoonsgegevens (bijv. DNA-analyses ten behoeve van het in kaart brengen van persoonlijke kenmerken).
7. **Gezondheidsgegevens**
   Grootschalige verwerkingen van gegevens over gezondheid (bijv. door instellingen of voorzieningen voor gezondheidszorg of maatschappelijke dienstverlening).
8. **Samenwerkingsverbanden**
   Het delen van persoonsgegevens in of door samenwerkingsverbanden waarin gemeenten of andere overheden met andere publieke of private partijen bijzondere persoonsgegevens of persoonsgegevens van gevoelige aard (bijv. gegevens over gezondheid, verslaving, enz.).
9. **Cameratoezicht**
   Grootschalige en/of stelselmatige monitoring van openbaar toegankelijke ruimten met behulp van camera's, webcams of drones.
10. **Flexibel cameratoezicht**
    Grootschalig en/of stelselmatig gebruik van flexibel cameratoezicht (camera's op kleding of helm van brandweer- of ambulancepersoneel, dashcams gebruikt door hulpdiensten).
11. **Controle werknemers**
    Grootschalige verwerking van persoonsgegevens en/of stelselmatige monitoring van activiteiten van werknemers (bijv. controle van e-mail en internetgebruik).
12. **Locatiegegevens**
    Grootschalige verwerking en/of stelselmatige monitoring van locatiegegevens van of herleidbaar tot natuurlijke personen (bijv. door (scan)auto's, navigatiesystemen, enz.).
13. **Communicatiegegevens**
    Grootschalige verwerking en/of stelselmatige monitoring van communicatiegegevens inclusief metadata herleidbaar tot natuurlijke personen, tenzij en voor zover dit noodzakelijk is ter bescherming van de integriteit en de veiligheid van het netwerk en de dienst van de betrokken aanbieder, of het randapparaat van de eindgebruiker.
14. **Internet of things**
    Grootschalige verwerkingen en/of stelselmatige monitoring van persoonsgegevens die worden gegenereerd door apparaten die verbonden zijn met internet en die via internet of anderszins gegevens kunnen versturen of uitwisselen (bijv. slimme televisies, slimme huishoudelijke apparaten, enz.).
15. **Profilering**
    Systematische en uitgebreide beoordeling van persoonlijke aspecten van natuurlijke personen gebaseerd op geautomatiseerde verwerking (profilering), zoals bijv. beoordeling van beroepsprestaties, prestaties van leerlingen, economische situatie, enz.
16. **Observatie en beïnvloeding van gedrag**
    Grootschalige verwerkingen van persoonsgegevens waarbij op stelselmatige wijze via geautomatiseerde verwerking gedrag van natuurlijke personen geobserveerd of beïnvloed,

dan wel gegevens daarover worden verzameld en/of vastgelegd, inclusief gegevens die voor het doel online behavioural advertising worden verzameld.

17. **Biometrische gegevens**
    Grootschalige verwerkingen en/of stelselmatige monitoring van biometrische gegevens met al doel een natuurlijk persoon te identificeren. In beginsel is verwerking van biometrische gegevens met als doel de unieke identificatie van een natuurlijk persoon, in beginsel verboden. Enkel als de verwerking strikt noodzakelijk is voor authenticatie of beveiligingsdoeleinden, is de verwerking toegestaan.

Bijlage 2 – Model DPIA

A. Beschrijving kenmerken gegevensverwerkingen

Beschrijf op gestructureerde wijze de voorgenomen gegevensverwerkingen, de verwerkingsdoeleinden en de belangen bij de gegevensverwerkingen.

1. **Voorstel**
   Beschrijf het voorstel waar de DPIA betrekking op heeft en de context waarbinnen deze plaatsvindt op hoofdlijnen.
2. **Persoonsgegevens**
   Som alle categorieën van persoonsgegevens op die worden verwerkt. Geef per categorie van betrokkene aan welke persoonsgegevens van hen verwerkt worden. Deel deze persoonsgegevens in onder de typen: algemeen, bijzonder en strafrechtelijk en wettelijk identificatienummer.
3. **Gegevensverwerking**
   Geef alle voorgenomen gegevensverwerkingen weer.
4. **Verwerkingsdoeleinden**
   Beschrijf de doeleinden van de voorgenomen gegevensverwerkingen.
5. **Betrokken partijen**
   Benoem welke organisaties betrokken zijn bij welke gegevensverwerkingen. Deel deze organisaties per gegevensverwerking in onder de rollen: verwerkingsverantwoordelijke, verwerker, verstrekker of ontvanger. Benoem tevens welke functionarissen binnen deze organisaties toegang krijgen tot welke persoonsgegevens.
6. **Belangen bij de gegevensverwerkingen**
   Beschrijf alle belangen die de verwerkingsverantwoordelijke en anderen hebben bij de voorgenomen gegevensverwerkingen.
7. **Verwerkingslocaties**
   Benoem in welke landen de voorgenomen gegevensverwerkingen plaatsvinden.
8. **Technieken en methoden van de gegevensverwerkingen**
   Beschrijf op welke wijze en met gebruikmaking van welke (technische) middelen en methoden de persoonsgegevens worden verwerkt. Benoem of sprake is van (semi-)geautoriseerde besluitvorming, profilering of big data-verwerkingen en, zo ja, beschrijf waaruit een en ander bestaat.
9. **Juridisch en beleidsmatig kader**
   Benoem de wet- en regelgeving en het beleid met mogelijke gevolgen voor de voorgenomen gegevensverwerkingen.
10. **Bewaartermijnen**
    Bepaal en motiveer de bewaartermijnen van de persoonsgegevens aan de hand van de verwerkingsdoeleinden.

B. Beoordeling rechtmatigheid gegevensverwerkingen

Beoordeel de rechtsgrond, noodzaak en doelbinding van de voorgenomen gegevensverwerkingen en rechten van de betrokkene.

11. **Rechtsgrond**
    Bepaal op welke rechtsgronden de gegevensverwerkingen worden gebaseerd.
12. **Bijzondere persoonsgegevens**
    Indien bijzondere persoonsgegevens worden verwerkt, beoordeel of één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing is. Beoordeel bij verwerking van een wettelijk identificatienummer of dit is toegestaan.
13. **Doelbinding**
    Indien de persoonsgegevens voor een ander doel worden verwerkt dan oorspronkelijk verzameld, beoordeel of deze verdere verwerking verenigbaar is met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld.
14. **Noodzaak en evenredigheid**
    Beoordeel of de voorgenomen gegevensverwerkingen noodzakelijk zijn voor het verwezenlijken van de verwerkingsdoeleinden. Ga hierbij in ieder geval in op proportionaliteit en subsidiariteit.
    a. Proportionaliteit: staat de inbreuk op de persoonlijke levenssfeer en de bescherming van de persoonsgegevens van de betrokkenen in evenredige verhouding tot de verwerkingsdoeleinden?
    b. Subsidiariteit: kunnen de verwerkingsdoeleinden in redelijkheid niet op een andere, voor de betrokkenen minder nadelige wijze, worden verwezenlijkt? Benoem hierbij de overwogen alternatieven.

15. Rechten van betrokkenen

Geef aan hoe invulling wordt gegeven aan de rechten van betrokkenen. Indien de rechten van de betrokkene worden beperkt, bepaal op grond van welke wettelijke uitzondering dat is toegestaan.

C. Beschrijving en beoordeling risico's voor de betrokkenen

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Houd hierbij rekening met de aard, omvang, context en doelen van de voorgenomen gegevensverwerkingen.

16. Risico's

Beschrijf en beoordeel de risico's van de voorgenomen gegevensverwerkingen voor de rechten en vrijheden van de betrokkenen. Ga in ieder geval in op:

a. welke negatieve gevolgen de gegevensverwerkingen kunnen hebben voor de rechten en vrijheden van de betrokkenen;
b. de oorsprong van deze gevolgen;
c. de waarschijnlijkheid (kans) dat deze gevolgen zullen intreden;
d. de ernst (impact) van deze gevolgen voor de betrokkenen wanneer deze intreden.

D. Beschrijving voorgenomen maatregelen

Beschrijf de voorgenomen maatregelen om de hiervoor beschreven risico's van de voorgenomen gegevensverwerkingen voor de vrijheden en rechten van de betrokkenen aan te pakken.

17. Maatregelen

Beoordeel welke technische, organisatorische en juridische maatregelen in redelijkheid kunnen worden getroffen om de hiervoor beschreven risico's te voorkomen of te verminderen. Beschrijf welke maatregel welk risico aanpakt en wat het restrisico is na het uitvoeren van de maatregel.

Indien de maatregel het risico niet volledig afdekt, motiveer waarom het restrisico acceptabel is.