Gemeente Amsterdam

Handreiking AVG/Archiefwet

Principes en strategieën voor integrale aanpak privacy en archivering 'by design'

Versie 1.0
26 april 2019
Opgesteld door: Expertisepool Recordmanagement, Expertisepool Privacy, Stadsarchief

Inhoud

Inleiding **2**

1 Definities en afbakening probleem **3**
1.1 Definities 3
1.2 Uitvoeringsprincipes 4
1.2.1 Vorm van informatie 4
1.2.2 Dimensies van informatiegebruik 4
1.2.3 Bepalen bewaartermijn en toegankelijkheidstrategie 5
1.2.4 Inrichting op basis van dataminimalisatie 6
1.2.5 Uitgaan van ideale situatie en keuzes documenteren 6

2 Type oplossingen **7**
2.1 Beperking van de toegang 7
2.2 Vernietiging / wissing 7
2.3 Pseudonimisering 8
2.4 Anonimisering 9
2.5 Conclusie 10

3 Risico voor de privacy van de betrokkenen **11**

Inleiding

De overheid is een informatiefabriek. Overheidsinformatie dient velerlei doelen: uiteraard is informatie nodig om de burger optimaal te ondersteunen vanuit de primaire processen, maar ook onder meer om verantwoording af te leggen over het eigen handelen en het vormen van cultureel erfgoed voor (toekomstig) onderzoek of het beschikbaar stellen van 'open data' voor gebruik door derden. Enerzijds vereist dit optimale toegankelijkheid en herbruikbaarheid van informatie, anderzijds heeft de overheid een plicht om de privacy van burgers maximaal te beschermen.

Bovenstaande belangen zijn gereguleerd in onder meer de AVG en de Archiefwet. Deze wetten lijken ogenschijnlijk conflicterende belangen te dienen: het bewaren vanuit algemeen belang versus bewaren vanuit individueel belang. Feitelijk zijn deze wetten echter complementair en dienen maatregelen hieruit volgend in samenhang te worden vormgegeven. Artikel 89 AVG vereist immers dat de verwerking van persoonsgegevens met het oog op archivering in het algemeen belang onderworpen is aan passende AVG waarborgen. De Archiefwet vormt het kader voor de keuze om gegevens wel of niet te bewaren, de AVG vormt het kader voor de keuze of persoonsgegevens wel of niet beschikbaar worden gesteld.

Dit memo is een handreiking waarmee informatieprofessionals privacy en archivering integraal 'by design' kunnen inrichten.

1 Definities en afbakening probleem

Allereerst is het van belang om stil te staan bij de verschillende termen en definities, zodat duidelijk is wat hieronder verstaan wordt en spraakverwarring wordt voorkomen.
In dit hoofdstuk worden allereerst de relevante definities opgesomd. Vervolgens worden deze in onderlinge samenhang geïnterpreteerd en geduid. Uit die duiding volgt een aantal uitvoeringsprincipes waarmee privacy en archivering integraal 'by design' kunnen worden ingericht.

1.1 Definities

Persoonsgegevens
Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene"); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
Bron: AVG, artikel 4:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/verordening_2016_-_679_definitief.pdf

Gegeven
De weergave van een feit, begrip of aanwijzing, geschikt voor overdracht, interpretatie of verwerking door een persoon of apparaat. Synoniem meervoud: data (gegevens).
Bron: https://archiefwiki.org/wiki/Gegeven (19122017)

Informatie
Betekenisvolle gegevens (data).
Bron: https://www.noraonline.nl/wiki/Informatie (19122017)

Archiefbescheiden
Informatie opgemaakt, ontvangen en onderhouden als bewijs en informatie door een organisatie of persoon bij het vervullen van wettelijke verplichtingen of bij zakelijke transacties.
Bron: NEN-ISO 15489:2001, 3. Termen en definities.

Database
Een database, gegevensbank of databank is een digitaal opgeslagen archief, ingericht met het oog op flexibele raadpleging en gebruik. Databases spelen een belangrijke rol voor het archiveren en actueel houden van gegevens bij onder meer de overheid, financiële instellingen en bedrijven, in de wetenschap, en worden op kleinere schaal ook privé gebruikt.
Bron: https://nl.wikipedia.org/wiki/Database

1.2 Uitvoeringsprincipes

Gezien de definities, kunnen we stellen dat informatie bestaat uit:

1. (Persoons)gegeven(s);
2. Betekenis.

Daaruit komt voort:

- Een bepaald gegeven kan verschillende betekenissen hebben en daarmee verschillende informatiewaarden vertegenwoordigen;
- Voor een bepaald soort gegeven kunnen verschillende bewaartermijnen gelden, afhankelijk van de betekenis die het gegeven vertegenwoordigt. Er is dus geen generieke bewaartermijn voor bijvoorbeeld BSN te benoemen.

1.2.1 Vorm van informatie

We onderscheiden twee verschijningsvormen van informatie:

1. Gegevens die zijn vastgelegd in een document;
2. Gegevens die zijn vastgelegd in een database.

Om hier pragmatisch mee om te kunnen gaan, hanteren we de volgende principes.

- Een document is een integraal archiefstuk;
    - Hieruit worden geen onderdelen vernietigd. Er kunnen wel maatregelen nodig zijn om AVG-conforme opslag te realiseren (zie hoofdstuk 2);
- Een database is niet per se een integraal archiefstuk;
    - Uit een database die niet als integraal archiefstuk wordt beschouwd, kunnen onderdelen worden vernietigd wanneer er geen doel meer is;
    - Let op: een database kan op zichzelf ook een integraal archiefstuk zijn. Doorgaans betreft dit databases met een statisch karakter.

1.2.2 Dimensies van informatiegebruik

Het is van belang om de verschillende dimensies van informatiegebruik te benoemen. Er is een bron waarin persoonsgegevens worden bewaard, maar dat wil niet zeggen dat die persoonsgegevens voor elke vorm van informatiegebruik beschikbaar zijn. Voorbeelden van deze dimensies van informatiegebruik zijn:

- Ondersteunen van een proces;
    - Er worden persoonsgegevens verzameld die nodig zijn om een proces te kunnen uitvoeren. Deze persoonsgegevens maken onderdeel uit van het dossier waarop ze betrekking hebben en worden als zodanig gearchiveerd. Dit is het brondossier.
- Publiceren;
    - Ten behoeve van publicatie (bijvoorbeeld in het kader van de WOB) wordt informatie geanonimiseerd. Persoonsgegevens blijven in het brondossier aanwezig, maar worden niet verstrekt aan derden.
- Creëren van managementinformatie;
    - Voor het creëren van managementinformatie geldt het principe dat deze informatie op geaggregeerd niveau wordt gecreëerd. Persoonsgegevens blijven

in het brondossier aanwezig, maar managementinformatie is niet tot deze gegevens herleidbaar.

- Hergebruiken
    - Data uit een brondossier worden soms hergebruikt, bijvoorbeeld binnen een keten of voor onderzoeksdoeleinden. Per type hergebruik wordt op basis van doelbinding bepaald welke persoonsgegevens in dat geval voor hergebruik in aanmerking komen;
    - Als ten behoeve van hergebruik een kopie van gegevens uit brondossiers wordt opgenomen in een datawarehouse, dan geldt het principe dat alleen geanonimiseerde gegevens in het datawarehouse worden opgenomen (comply or explain).

1.2.3 Bepalen bewaartermijn en toegankelijkheidstrategie

Bewaartermijnen gaan over informatie, dus over gegevens in combinatie met een doel. We onderscheiden hierin drie verschillende type doelen:

- Primair doel:
    - Uitvoering van de taak[1];
    - De uitvoering kan binnen een keten plaatsvinden.
- Secundair doel:
    - Verantwoording en bewijsvoering;
    - Hergebruik t.b.v. andere processen;
    - Hergebruik door derden.
- Tertiair doel:
    - Geschiedschrijving - vastleggen cultureel erfgoed.

Deze drie doelen bestaan naast elkaar en kunnen zich tegelijkertijd voordoen. Kenmerkend is dat het primaire doel als eerst vervalt, waarna het secundaire en tertiaire nog kunnen blijven voortbestaan. Vervolgens kan het secundaire doel vervallen, waarna het tertiaire doel nog kan blijven voortbestaan. Terwijl de gegevens

Als instrument voor het vaststellen van bewaartermijnen, hanteren we altijd de landelijk vastgestelde "Selectielijst gemeenten en intergemeentelijke organen". De bewaartermijnen die hierin zijn opgenomen, zijn aan de hand van een weging op deze drie type doelen tot stand gekomen.

Dit betekent:

- Het bewaren van persoonsgegevens wordt afgewogen tegen de drie type doelen;
- Wanneer persoonsgegevens voor geen van de drie type doelen meer relevant zijn of hun betekenis verliezen, dienen deze te worden vernietigd;
- Wanneer persoonsgegevens nog relevant zijn voor het secundaire of tertiaire doel en daarom bewaard moeten blijven, dan kan gekozen worden voor aanvullende beveiligingsmaatregelen (zie hoofdstuk 2).

Bewaartermijnen worden altijd op basis van processen in combinatie met een resultaattype toegekend. Bewaartermijnen worden niet op het niveau van afzonderlijke documenten of gegevens bepaald, maar op het niveau van een procestype waarop deze betrekking hebben.

[1] Vanuit dit doel wordt het verzamelen en vastleggen van gegevens gerechtvaardigd, meestal is dit

Gegevens in een niet-doorgegane zaak worden in de regel korter bewaard dan gegevens in een wel-doorgegane zaak. De Selectielijst biedt ruimte voor het onderscheiden van subprocessen, waardoor deelcollecties met voor reconstructie van de zaak minder relevante gegevens eerder vernietigd kunnen worden.

1.2.4 Inrichting op basis van dataminimalisatie

Bij het ontwerpen van processen en applicaties, dient het principe van dataminimalisatie te worden toegepast. De principes van 'privacy by design' en 'archivering by design' komen hier samen. Het gaat er hierbij om dat niet meer persoonsgegevens worden vastgelegd dan nodig voor het doel (privacyperspectief), maar wel voldoende om de archiveringsfunctie te laten functioneren (archiefperspectief). Dit is dus een vraagstuk waarnaar door de privacy officer en de IB-adviseur integraal gekeken moet worden. Het initieel verzamelen van persoonsgegevens mag uiteraard enkel als daarvoor een grondslag is zoals beschreven in artikel 6 van de AVG.

1.2.5 Uitgaan van ideale situatie en keuzes documenteren

Bij het ontwerp wordt uitgegaan van de ideale situatie. Het kan voorkomen dat de ideale situatie praktisch niet haalbaar is, bijvoorbeeld omdat vernietigingsfunctionaliteit niet op het gewenste niveau aanwezig is in een applicatie (dit geldt met name voor legacy-systemen). In een dergelijk geval is het van belang om op zoek te gaan naar de praktisch best mogelijke optie en te documenteren welke keuzes hierin zijn gemaakt.

2 Type oplossingen

Het doel van dit hoofdstuk is om te komen tot een beschrijving van "typen oplossingen" die kunnen worden toegepast om tot een AVG-conforme opslag van archiefbescheiden te komen. Artikel 89 AVG vereist immers dat de verwerking van persoonsgegevens met het oog op archivering in het algemeen belang onderworpen is aan passende AVG waarborgen. Overheidsorganisaties zijn hierdoor verplicht om ten aanzien van archivering de technische en organisatorische maatregelen te treffen om het beginsel van dataminimalisatie te garanderen. De eerste vraag is altijd of gegevens nog bewaard moeten blijven of dat ze vernietigd moeten worden. Indien bewaring noodzakelijk is, dan is het om te voldoen aan de AVG soms nodig om bepaalde beveiligingsmaatregelen te nemen waarmee persoonsgegevens niet of niet herkenbaar toegankelijk worden gemaakt voor de informatieconsument, zonder dat de gearchiveerde persoonsgegevens vernietigd worden. De combinatie AVG en Archiefwet kent twee middelen, namelijk: pseudonimisering en anonimisering. De beschikbare oplossingen zijn in dit hoofdstuk uitgewerkt.

2.1 Beperking van de toegang

Bij deze oplossing wordt access-management ingezet: de gegevens blijven beschikbaar, maar zijn door middel van autorisatie alleen te benaderen door een wel omschreven groep, met een wel omschreven doel. Denk onder meer aan functioneel beheer, dat na een bepaalde periode de gegevens alsnog moet vernietigen. De toegangsbeperking kan worden toegepast op complete registraties, maar ook op delen daarvan. Een voorbeeld van dat laatste is het 'onzichtbaar' maken voor gebruikers van tabbladen in een klantdossier.

2.2 Vernietiging / wissing

Het vernietigen / wissen van persoonsgegevens komt op meerdere plekken in de AVG terug.

Artikel 17 AVG biedt de grondslag voor de vernietiging van persoonsgegevens indien de betrokkene daarom vraagt. Dit is het recht op vergetelheid. Daarop is een aantal belangrijke uitzonderingen geformuleerd. Ook archivering in het algemeen belang wordt als uitzondering genoemd (derde lid, sub d): indien het recht op vergetelheid de verwezenlijking van de doeleinden van archivering in het gedrang (dreigt) te brengen, hoeven gegevens niet op verzoek gewist te worden.

Persoonsgegevens dienen verwijderd te worden als de betrokkene de toestemming intrekt en er geen andere rechtsgrond is voor de gegevensverwerking.

Daarnaast mogen persoonsgegevens op basis van artikel 5 lid 1 sub e AVG niet langer worden bewaard dan noodzakelijk met het oog op de betrokken doeleinden. Dat artikel bepaalt ook dat persoonsgegevens voor langere perioden mogen worden opgeslagen met het oog op archivering

in het algemeen belang. Hierin voorziet de Selectielijst, op basis waarvan gegevens voor langere perioden (en soms blijvend) moeten worden bewaard.

Bij voormelde uitzonderingen wordt verwezen naar artikel 89 lid 1 AVG en de passende waarborgen waaraan archiefbescheiden dienen te worden onderworpen. Deze kunnen onder andere gevonden worden in pseudonimiseren en anonimiseren, deze worden hierna beschreven.

Zodra de bewaartermijn op grond van de Selectielijst is verstreken, moeten archiefbescheiden worden vernietigd. Met het oog op de betrokken persoonsgegevens verduidelijkt de AVG niet hoe een proces rondom vernietiging moet worden ingericht. Wel moet het proces onomkeerbaar zijn: eenmaal vernietigd kunnen de gegevens niet meer worden teruggehaald. Informatiedragers (digitaal / hardcopy) moeten daarom een zodanige bewerking ondergaan, dat de informatie hierop niet meer te herleiden is. Er zijn diverse vormen van vernietiging denkbaar, zoals vernietiging door gecertificeerde vernietigingsorganisaties. De kaders hiervoor worden in archiefwetgeving gevonden.

2.3 Pseudonimisering

Ten aanzien van archivering stelt artikel 89 (1) AVG dat maatregelen moeten worden genomen om het beginsel van minimale gegevensverwerking te waarborgen. Dit betekent dat niet meer persoonsgegevens mogen worden verwerkt dan strikt noodzakelijk voor het (archiverings)doel ('archivering in het algemeen belang'). Pseudonimisering wordt daarbij genoemd als mogelijke maatregel. Indien door pseudonimisering het (archiverings)doel echter niet (meer) kan worden verwezenlijkt, behoeft pseudonimisering niet plaats te vinden.

De AVG omschrijft pseudonimisering[2] als het verwerken van persoonsgegevens op zodanige wijze dat de persoonsgegevens niet meer aan een specifieke betrokkene kunnen worden gekoppeld zonder gebruikmaking van aanvullende gegevens. Voorwaarde is dat deze aanvullende gegevens apart worden bewaard. Ook moeten technische en organisatorische maatregelen worden genomen om te zorgen dat onbevoegden de koppeling tussen de gegevens niet kunnen maken. Deze beveiligingstechniek vermindert risico's voor betrokkenen en helpt om archiefbescheiden conform de beginselen van de AVG te beschermen.

Een voorbeeld van pseudonimisering is het vervangen van een naam door een uniek nummer (niet zijnde BSN). De gegevens die betrekking hebben op de naam kunnen dan worden gekoppeld aan het nummer in plaats van aan de naam. Hierdoor is voor onbevoegden niet zichtbaar wie de persoon is waar de gegevens aan toebehoren. Alleen degenen die de koppeling kunnen maken tussen de naam en het unieke nummer kunnen de gegevens koppelen aan een geïdentificeerde natuurlijke persoon.

De meest gebruikelijke pseudonimiseringstechnieken zijn:

1. **Encryptie** met een geheime sleutel. Hierbij staan de persoonsgegevens nog steeds in de dataset, maar in gecodeerde vorm. De partij die over de sleutel beschikt, kan de dataset en de betreffende persoonsgegevens eenvoudig decoderen;

[2] Art. 4(5) AVG.

Een voorbeeld hiervan is bijvoorbeeld het pseudonimiseren van leerling-gegevens in het onderwijs, door het gebruik van het persoonsgebonden nummer (PGN) van een leerling (zie onder meer het advies van de AP hierover van 8 november 2016);

2. **Polymorfe pseudonimisering**: Een vorm van versleuteling, waarbij specifieke pseudoniemen voor een gebruiker worden gevormd per ontvangende partij, zonder dat de vormende partij het specifiek pseudoniem kan herleiden of de identiteit van de gebruiker bij gebruik hoeft te kennen. Deze techniek is ontwikkeld door de Radboud Universiteit en wordt onder meer gebruikt in het onderwijs;
3. **Hashen**: hierbij worden de ingevoerde persoonsgegevens, ongeacht de omvang/grootte ervan (de invoer) vervangen door een ' uitvoer' van een vaste grootte.

Voor het pseudonimiseren van papieren archiefstukken, is het noodzakelijk dat deze eerst worden gescand op een zodanige wijze dat de inhoud van de gescande bestanden bewerkt kan worden. Te denken valt aan het gebruik van een OSR-scanner.

Omdat gepseudonimiseerde gegevens in theorie nog steeds gekoppeld kunnen worden aan een natuurlijk persoon (de-identificatie is immers niet onomkeerbaar), worden gepseudonimiseerde gegevens gezien als 'persoonsgegevens' in de zin van de AVG. De AVG blijft dan ook van toepassing. Risico's voor betrokkenen worden echter sterk beperkt. Het mogelijk toepassen van pseudonimisering op archiefbescheiden wordt dan ook gezien als een passende waarborg om de AVG-verplichtingen inzake gegevensbescherming na te komen.[3]

2.4 Anonimisering

Wanneer de doeleinden van archivering kunnen worden bereikt door de identificatie van betrokkenen niet langer mogelijk te maken, moet dat op die manier gebeuren.[4] Met andere woorden, zodra het mogelijk is om het archiveringsdoel te bereiken met geanonimiseerde gegevens, moet anonimisering worden toegepast. Omgekeerd geldt dus ook dat indien door anonimisering het doel 'archivering in het algemeen belang' niet (meer) kan worden verwezenlijkt, anonimisering niet plaats hoeft te vinden.

Anonimisering betekent dat persoonlijk identificeerbare informatie *onomkeerbaar* wordt veranderd, op zodanige wijze dat een betrokkene niet langer (in)direct kan worden geïdentificeerd. Met andere woorden, re-identificatie moet onmogelijk worden gemaakt. Om te bepalen of iemand nog identificeerbaar is, moet rekening worden gehouden met alle middelen waarvan redelijkerwijs valt te verwachten dat zij kunnen worden gebruikt om iemand (in)direct te identificeren. Denk daarbij aan factoren zoals kosten en tijd benodigd voor identificatie.[5] Kortgezegd: re-identificatie moet onevenredig veel moeite kosten.

De AVG verduidelijkt niet hoe een proces om gegevens anoniem te maken uitgevoerd moet worden. De nadruk ligt op het resultaat: het mag niet mogelijk zijn iemand te identificeren. Er zijn diverse anonimiseringstechnieken denkbaar, zoals:

1. **Randomisatie**: dit zijn technieken waarbij de waarheidsgetrouwheid van de gegevens wordt veranderd, met als doel: het loskoppelen van de persoon. De gegevens in de set zijn

[3] Preambule 156 AVG.
[4] Art. 89 (1) AVG.
[5] Preambule 26 AVG.

dan niet meer te herleiden tot individuele personen. De één-op-één relatie tussen de record en de betrokkene blijft intact. Voorbeelden hiervan zijn:

   a. Ruistoevoeging, waarbij specifieke gegevens in de dataset minder nauwkeurig worden gemaakt (maar de algemene verdeling wel behouden blijft). Een voorbeeld is het minder nauwkeurig maken van afmetingen of locaties, denk aan het afknippen van de laatste vier cijfers van een MAC-adres alvorens de overige cijfers gepseudominiceerd worden. Om echt tot anonimisering te leiden, moet deze techniek worden gecombineerd met andere anonimiseringstechnieken.
   b. Permutatie – een specifieke vorm van ruistoevoeging, in tabellen – waarbij de (persoons)gegevens in een dataset worden verwisseld, zodat deze aan andere betrokkenen worden gekoppeld.

2. **Generalisatie**: het generaliseren van de gegevens door de schaal te vergroten (bijvoorbeeld de regio benoemen in plaats van de stad, of van maanden in plaats van weken). Het aggregeren van persoonsgegevens is hier een voorbeeld van. Deze technieken zullen niet voor de hand liggen voor toepassing binnen de gemeentelijke archieven.

Nu geanonimiseerde gegevens niet meer gebruikt kunnen worden om een natuurlijk persoon te identificeren, vallen ze buiten de werking van de AVG.[6] Het toepassen van anonimisering op archiefbescheiden kan dan ook uitkomst bieden om onder strikte AVG eisen uit te komen. Daarbij moet het archiveringsdoel in het oog worden gehouden. Als dit niet bereikt kan worden met geanonimiseerde gegevens, hoeft anonimisering niet plaats te vinden.

2.5 Conclusie

Bij verwerkingen van persoonsgegevens voor archiveringsdoeleinden dient de AVG in aanmerking te worden genomen. Het accent hierbij ligt bij dataminimalisatie: niet meer persoonsgegevens mogen worden verwerkt dan strikt noodzakelijk voor het archiveringsdoel. Zodra het mogelijk is om dit doel te halen met geanonimiseerde gegevens (niet langer herleidbaar tot een natuurlijke persoon) moet deze ontkoppeling worden uitgevoerd. Als tussenvorm kan gewerkt worden met pseudonimisering. Daarbij is koppeling nog wel mogelijk, maar de daarvoor benodigde informatie (de 'sleutel') is niet direct beschikbaar. Indien gegevens verwijderd moeten worden, bijvoorbeeld op grond van de Selectielijst, dient daartoe te worden overgegaan. De optimale oplossing moet per situatie worden gekozen en geïmplementeerd.

Daar waar de overtuiging bestaat dat het archiveringsdoel niet kan worden behaald met implementatie van de in dit memorandum genoemde oplossingen, kan worden gezorgd voor een gedegen onderbouwing van de vraag *waarom* dit niet kan. Op die manier kunnen wij richting toezichthoudende autoriteiten (en mogelijk betrokkenen) voldoen aan onze verantwoordingsplicht.

[6] Preambule 26 AVG.

3 Risico voor de privacy van de betrokkenen

Indien het langdurig bewaren van een dossier of specifieke documenten daarin potentieel een hoog risico vormt voor de privacy van betrokkene(n) dient kritisch gekeken te worden naar de onderdelen van het proces. Mogelijk kan er binnen het proces onderscheid gemaakt worden tussen verschillende subprocessen. Dit kan aan de orde zijn wanneer een regulier proces voor een specifieke doelgroep wordt aangevuld met extra eisen en toetsingskaders. Een voorbeeld daarvan zijn assessments die specifiek zijn ontwikkeld om statushouders naar de arbeidsmarkt te begeleiden, binnen het reguliere proces van het verlenen van uitkeringen en toeleiding naar de arbeidsmarkt. De extra vereisten of werkzaamheden, met de daarbij behorende persoonsgegevens kunnen dan worden gevat in een 'subproces' binnen het reguliere hoofdproces. Voor het hoofdproces worden dan de reguliere bewaartermijnen gehanteerd, waar voor het subproces vervolgens apart beoordeeld dient worden welke bewaartermijn gehanteerd zou moeten worden. De selectielijst biedt ruimte om op deze manier specifieke onderdelen apart te waarderen.

Een hoog risico voor de privacy van betrokkenen kan onder andere ontstaan door de aard van de persoonsgegevens die verwerkt worden en/of de categorie betrokkenen (kwetsbare personen) waarvan de gegevens worden verwerkt.

Bijzondere persoonsgegevens:
- Gezondheid;
- Biometrische gegevens (bijv. vingerafdrukken of gezichtsherkenning);
- Genetische gegevens;
- Seksuele gedragingen of voorkeuren;
- Lidmaatschap vakbond;
- Politieke opvattingen;
- Religie of levensbeschouwelijke overtuigingen;
- Ras of etnische afkomst.

Strafrechtelijke gegevens:
- Gegevens over strafbare feiten of hinderlijk gedrag (incl. zwarte lijsten of waarschuwingslijsten).

Gevoelige gegevens:
- Locatiegegevens (bijv. via navigatie, telefoon, in het OV);
- Gegevens over elektronische communicatie (incl. IP-adres, apparaat ID, MAC adres, Wifi verbindingen);
- Financiële gegevens (bijv. inkomensgegevens, uitkeringsgegevens, rekeningnummer, bankgegevens);
- BSN;
- Kopie paspoort.

Categorieën van kwetsbare betrokkenen:
- Kinderen (in het bijzonder kinderen die jeugdhulp ontvangen);

- Hulpbehoevende ouderen;
- Statushouders;
- Mensen met taalachterstand;
- Mensen die een WMO-voorziening ontvangen;
- Andere kwetsbare individuen (bijv. bijstandsgerechtigden, minima);
- Slachtoffers van (huiselijk of seksueel) geweld.