

# Verantwoordelijkheden contactpunt

## AVG-verzoeken, informatieplicht en meldplicht datalekken



Per 1 maart 2025 geldt de Wet gegevensverwerking door samenwerkingsverbanden (WGS) voor de Zorg- en Veiligheidshuizen. Op grond van deze wet moet ieder Zorg- en Veiligheidshuis een contactpunt aanwijzen. Het contactpunt is verantwoordelijk voor:

- het behandelen van AVG-verzoeken
- het nakomen van de informatieplicht zoals bedoeld in artikel 14 AVG
- het nakomen van de meldplicht bij datalekken zoals bedoeld in artikel 33 AVG

De werkwijze van het contactpunt is verder uitgewerkt in het Besluit gegevensverwerking door samenwerkingsverbanden (BGS). In deze factsheet lees je wat het contactpunt moet regelen om aan deze verplichtingen te voldoen. Deze factsheet is een aanvulling op Factsheet 1 'Inrichten van een contactpunt gegevensverwerking'.

## Inhoud

<b>Verantwoordelijkheden contactpunt</b> .....	<b>1</b>	<b>3. Informatieverplichting (artikel 1.3 BGS)</b> .....	<b>9</b>
<b>1. AVG-verzoeken: soorten AVG-verzoeken en voorwaarden toewijsbaarheid</b> .....	<b>2</b>	3.1 Verantwoordelijkheid contactpunt.....	9
1.1 Inzageverzoek AVG (artikel 15 AVG).....	2	3.2 Inhoud informatieverplichting (artikel 14 AVG).....	9
1.2 Alleen inzage in persoonsgegevens.....	2	3.3 Alleen ten aanzien van gezamenlijke verwerking.....	9
1.3 Verzoek op grond van Woo meestal behandelen als AVG-verzoek.....	3	3.4 Ook informatieplicht als een casus niet in behandeling wordt genomen.....	10
1.4 Verzoeken om correctie of rectificatie van persoonsgegevens.....	3	3.5 Termijn.....	10
1.5 Wissings- of verwijderverzoeken.....	3	3.6 Overleg met deelnemers.....	10
1.6 Verzoeken om beperking van de verwerking.....	4	3.7 Templates.....	10
1.7 Bezwaar tegen de verwerking (artikel 21 AVG).....	4	3.8 Uitzonderingen informatieverplichting.....	11
1.8 Uitzonderingen (artikel 41 UAVG).....	4	<b>4. Meldplicht datalekken (artikel 1.4 BGS)</b> .....	<b>12</b>
<b>2. Behandeling AVG-verzoeken door contactpunt (artikel 1.2 BGS)</b> .....	<b>6</b>	4.1 Verantwoordelijkheid contactpunt.....	12
2.1 Verantwoordelijkheid contactpunt.....	6	4.2 Wat is een datalek?.....	12
2.2 Alleen ten aanzien van gezamenlijke verwerking.....	6	4.3 Alleen ten aanzien van gezamenlijke verwerking.....	12
2.3 Doorzendplicht.....	6	4.4 Termijnen.....	12
2.4 Identiteit betrokkene vaststellen.....	6	4.5 Overleg met deelnemers en informatieplicht deelnemers.....	13
2.5 Termijn voor beantwoorden AVG-verzoek.....	7	4.6 Wat moet worden gemeld?.....	13
2.6 Overleg met deelnemers.....	7	4.7 Hoe moet worden gemeld?.....	13
2.7 Beantwoording AVG-verzoek door andere overheidsdeelnemer.....	7	4.8 Maatregelen nemen.....	13
2.8 Stappenplan voor behandeling AVG-verzoeken.....	7	4.9 Datalekregister.....	14
2.9 Bezwaar en beroep.....	8	4.10 Uitzonderingen.....	14
		4.11 Stappenplan datalekken.....	14
		<b>Bijlage A – Voorbeeld stappenplan AVG-verzoeken</b> ....	<b>15</b>
		<b>Bijlage B – Voorbeeld stappenplan datalekken</b> .....	<b>16</b>

# 1. AVG-verzoeken: soorten AVG-verzoeken en voorwaarden toewijsbaarheid

## 1.1 Inzageverzoek AVG (artikel 15 AVG)

Op grond van artikel 15 AVG kan een betrokkene vragen om inzage in zijn persoonsgegevens. Het samenwerkingsverband moet de betrokkene dan de volgende informatie geven, tenzij een uitzondering van toepassing is (zie [paragraaf 1.8](#) van deze factsheet):

- de doeleinden van verwerking;
- de categorieën persoonsgegevens die worden verwerkt;
- de ontvangers van de persoonsgegevens;
- de bewaartermijnen;
- de rechten van de betrokkene;
- de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens;
- de bron(nen) van de persoonsgegevens;
- of sprake is van geautomatiseerde besluitvorming;
- een kopie van de persoonsgegevens.

**Let op:** Het recht om een kopie te krijgen van de persoonsgegevens, betekent niet dat de betrokkene recht heeft op een kopie van de *documenten* waarin deze persoonsgegevens staan.

Het recht op een kopie houdt in dat de betrokkene een letterlijke weergave krijgt van de persoonsgegevens die over hem worden verwerkt. Dit kan bijvoorbeeld door een overzicht of tabel te geven met de persoonsgegevens die over de betrokkene staan in een systeem, e-mails of andere documenten.

Het verstrekken van (gelakte) documenten *mag* natuurlijk wel, maar dit is alleen *verplicht* als dat onontbeerlijk is om de verstrekte informatie goed te kunnen begrijpen (HvJ 4 mei 2023, C-487/21, punt 45). In dat geval moet het document wel worden verstrekt. Informatie waarop een uitzondering van toepassing is (zie volgende paragraaf) moet dan worden weggelakt.

Meer informatie en een voorbeeld staan op de [website](#) van de Autoriteit Persoonsgegevens.

## 1.2 Alleen inzage in persoonsgegevens

Het inzagerecht gaat alleen over persoonsgegevens. Niet alle informatie in een dossier is een persoonsgegeven. Alleen informatie die over de betrokkene gaat, is een persoonsgegeven. In de rechtspraak is bijvoorbeeld geoordeeld dat een

juridische analyse geen persoonsgegeven is.<sup>1</sup> Een juridische analyse gaat namelijk niet over de persoon, maar over het recht of de uitleg van het recht. Hetzelfde geldt voor informatie die over anderen gaat, zoals familieleden van de betrokkene, of informatie over het beleid van de deelnemers die betrokken zijn bij de aanpak van complexe problematiek.

Soms wordt gedacht dat meningen over een persoon geen **persoonsgegevens** zijn. Dat is niet juist. Het Europese Hof van Justitie heeft geoordeeld dat het begrip persoonsgegeven ruim moet worden uitgelegd. Het gaat om elke soort informatie die de betrokkene betreft. Daaronder valt niet alleen *objectieve* informatie, zoals zijn leeftijd of adres, maar ook *subjectieve* informatie, zoals meningen of beoordelingen over de betrokkene.<sup>2</sup>

Toch hoeven meningen of beoordelingen niet altijd te worden verstrekt. Daarop kan een uitzondering van toepassing zijn (zie [paragraaf 1.8](#) van deze factsheet). Als een mening te herleiden is tot de persoon die deze heeft geuit, kan inzage namelijk in strijd komen met de rechten en vrijheden van die persoon. In dat geval moet een belangenafweging worden gemaakt.

<sup>1</sup> HvJ 17 juli 2014, C-141/12 en C-372/12, ECLI:EU:C:2014:2081; ABRvS 11 feb 2015, ECLI:NL:RVS:2015:318.

<sup>2</sup> HvJ 20 sept. 2017, ECLI:EU:C:2017:994 (Nowak)

### 1.3 Verzoek op grond van Woo meestal behandelen als AVG-verzoek

Soms beroepen betrokkenen zich op de Wet open overheid (Woo) als zij inzage willen in hun dossier. Vaak weten zij niet goed wat het verschil is tussen de Woo en de AVG. Het contactpunt moet daarom altijd zelf nagaan wat een betrokkene precies bedoelt. Op basis daarvan moet het contactpunt bepalen op grond van welke wet het verzoek moet worden behandeld.

Als een betrokkene inzage wil in zijn dossier bij het Zorg- en Veiligheidshuis of wil weten welke gegevens het Zorg- en Veiligheidshuis over hem verwerkt, moet dit verzoek meestal worden behandeld op grond van artikel 15 AVG. Dat geldt ook als de betrokkene verwijst naar de Woo.

Er zijn namelijk twee soorten Woo-verzoeken:

- **Verzoeken op grond van artikel 4.1 Woo**

Een verzoek op grond van artikel 4.1 Woo leidt tot **openbaarmaking** van de gevraagde informatie. Meestal wil een betrokkene die zijn dossier wil inzien niet dat dit dossier openbaar wordt gemaakt. Ga dit daarom altijd na als een betrokkene zich beroept op de Woo. Wil de betrokkene geen openbaarmaking, dan moet het verzoek niet worden behandeld als een verzoek op grond van artikel 4.1 Woo.

- **Verzoeken op grond van artikel 5.5 Woo**

Dat zijn verzoeken om informatie te verstrekken *zonder* dat deze informatie openbaar wordt gemaakt. Maar let op: als een verzoeker met een beroep op dit artikel informatie over zichzelf wil ontvangen, moet het verzoek toch worden behandeld als een AVG-verzoek.

In de toelichting bij artikel 5.5 Woo staat namelijk dat dit artikel een vangnetbepaling is. Dat betekent dat dit artikel alleen moet worden toegepast als de verzoeker geen beroep kan doen op een andere wet om de informatie op te vragen. Een betrokkene die inzage wil in zijn eigen dossier bij het Zorg- en Veiligheidshuis, kan wel een beroep doen op een andere wet om deze inzage te krijgen, namelijk op artikel 15 AVG.

Doet een burger dus een beroep op artikel 5.5 Woo om inzage te krijgen in zijn dossier bij een Zorg- en Veiligheidshuis, dan moet dit verzoek worden behandeld als een AVG-verzoek.

### 1.4 Verzoeken om correctie of rectificatie van persoonsgegevens

Op grond van artikel 16 AVG kan een betrokkene vragen om rectificatie van zijn persoonsgegevens, tenzij een uitzondering van toepassing is (zie [paragraaf 1.8](#) van deze factsheet).

- Als persoonsgegevens feitelijk onjuist zijn, kan de betrokkene vragen om deze gegevens te verbeteren.
- Als persoonsgegevens onvolledig zijn, kan de betrokkene vragen om deze gegevens aan te vullen.

Het rectificatierecht is niet bedoeld om meningen, onderzoeksresultaten of conclusies of constatering van de politie te corrigeren als de betrokkene het daar niet mee eens is. Wel kan aan de betrokkene worden aangeboden om zijn kant van het verhaal in het dossier op te nemen. Zo wordt duidelijk waar de betrokkene het niet mee eens is.

### 1.5 Wissings- of verwijderverzoeken

Op grond van artikel 17 AVG kan een betrokkene vragen om zijn persoonsgegevens te wissen, tenzij een **uitzondering** van toepassing is (zie [paragraaf 1.8](#) van deze factsheet).

Wissing is verplicht in de volgende gevallen, voor zover relevant voor verwerkingen onder de WGS:

- De persoonsgegevens zijn niet langer nodig voor de doeleinden waarvoor zij zijn verzameld of verwerkt. Dat is het geval als de bewaartermijn verstreken is (zie de [factsheet Bewaartermijnen](#))

- De betrokkene heeft terecht bezwaar gemaakt (zie verderop in deze factsheet).
- De persoonsgegevens zijn onrechtmatig verwerkt. Als aan de WGS wordt voldaan, is dat meestal niet het geval.
- Er is een wettelijke plicht om de gegevens te wissen. Ook dan geldt: als aan de WGS wordt voldaan, is dit meestal niet aan de orde.

Ook als wissing op één van deze gronden verplicht is, hoeft niet te worden gewist als één van de bijzondere uitzonderingen van toepassing is uit artikel 17 lid 3 AVG of als een algemene uitzondering van toepassing is (zie verderop deze pagina bij 1.8).

Voor verwerkingen onder de WGS zijn vooral de volgende bijzondere uitzonderingen van belang. De andere bijzondere uitzonderingen zullen zich waarschijnlijk niet voordoen:

- De verwerking is nodig voor de vervulling van een taak van algemeen belang. Dit zal bij verwerkingen onder de WGS meestal het geval zijn.
- De verwerking is nodig voor de instelling, uitoefening of onderbouwing van een rechtsvordering. Dit betekent dat een Zorg- en Veiligheidshuis gegevens bijvoorbeeld mag bewaren als deze nodig zijn om een bezwaar van een betrokkene te behandelen of om verweer te voeren in een bestuurs- of civielrechtelijke procedure. Let er wel op dat dit niet automatisch betekent dat

alle gegevens over de betrokkene bewaard kunnen worden. Het gaat alleen om de gegevens die relevant zijn voor de juridische procedure. Ook is het belangrijk om de gegevens goed af te schermen, zodat ze uitsluitend kunnen worden ingezien en gebruikt voor de procedure en niet voor andere doeleinden. Dat kan bijvoorbeeld door het dossier alleen te bewaren in het zaakstelsel van de juridische afdeling en niet meer in KeDo of PGAx.

### 1.6 Verzoeken om beperking van de verwerking

Op grond van artikel 18 AVG kan een betrokkene vragen om beperking van de verwerking, tenzij een **uitzondering** van toepassing is (zie verderop deze pagina bij 1.8).

Beperking houdt in dat:

- gegevens tijdelijk worden gemarkeerd, of
- gegevens tijdelijk worden afgeschermd voor gebruikers, of
- de verwerking tijdelijk wordt gestopt.

Beperking is verplicht in de volgende gevallen:

- De betrokkene heeft een rectificatieverzoek gedaan en vraagt daarnaast om de gegevens die volgens hem onjuist of onvolledig zijn, tijdelijk te markeren of af te schermen. Aan dit verzoek moet worden voldaan totdat de rectificatie heeft

plaatsgevonden of is afgewezen.

- De verwerking is onrechtmatig, maar de betrokkene wil niet dat de gegevens worden gewist. De betrokkene kan dan vragen om de gegevens af te schermen, zodat gebruikers deze niet meer kunnen inzien of gebruiken, maar de gegevens wel bewaard blijven.
- De betrokkene heeft bezwaar gemaakt (zie volgende paragraaf). De betrokkene kan dan bijvoorbeeld vragen om de gegevens af te schermen totdat op het bezwaar is beslist.

### 1.7 Bezwaar tegen de verwerking (artikel 21 AVG)

Op grond van artikel 21 AVG kan een betrokkene bezwaar maken tegen de verwerking van zijn persoonsgegevens. Het bezwaar moet worden toegewezen als er bijzondere persoonlijke omstandigheden zijn die zwaarder wegen dan het belang dat de deelnemers van het Zorg- en Veiligheidshuis hebben bij de gezamenlijke verwerking van de gegevens door het Zorg- en Veiligheidshuis.

### 1.8 Uitzonderingen (artikel 41 UAVG)

Als een AVG-verzoek terecht is en dus moet worden toegewezen, hoeft daar toch niet aan te worden voldaan. Dat is het geval als een uitzondering van toepassing is.

Hetzelfde geldt voor de plicht om de betrokkene te informeren wanneer zijn persoonsgegevens worden verwerkt (zie [hoofdstuk 3](#) van deze factsheet) en voor de plicht om een datalek aan de betrokkene te melden (zie [hoofdstuk 4](#) van deze factsheet). Ook voor deze verplichtingen geldt dat daaraan niet hoeft te worden voldaan als een uitzondering van toepassing is.

De uitzonderingen staan in artikel 41 van de Uitvoeringswet AVG (jo. artikel 23 AVG). Deze uitzonderingen worden ook wel beperkingen genoemd.



De meest voorkomende beperkingen zijn:

- **Bescherming van de rechten of vrijheden van anderen, zoals de privacy of veiligheid van anderen**

- Als dit belang van anderen zwaarder weegt dan het belang van de betrokkene bij het AVG-verzoek, kan het verzoek worden afgewezen.
- Inzageverzoeken kunnen op deze grond bijvoorbeeld gedeeltelijk worden afgewezen. Dat kan door geen inzage te geven in gegevens die de privacy of veiligheid van anderen kunnen schaden. Denk aan de namen van ambtenaren en medewerkers die betrokken zijn bij de behandeling van het dossier, de namen van burgers of slachtoffers die een melding hebben gedaan over de betrokkene, of de namen van andere betrokkenen die in het dossier worden genoemd, zoals familieleden.
- Het gaat ook om gegevens die direct of indirect herleidbaar zijn tot anderen. Functienamen, zoals 'regisseur', 'jeugdhulpverlener' of 'behandelaar van organisatie x', zijn voor de betrokkene meestal herleidbaar tot een persoon. Dat geldt ook voor de inhoud van een melding of een relaas van een familielid dat in het dossier is opgenomen. Ook als namen zijn weggelaten, kan de betrokkene uit de inhoud vaak nog afleiden wie de informatie heeft gegeven.

- **Lopend opsporingsonderzoek**

- Een AVG-verzoek kan worden afgewezen voor zover dit noodzakelijk is voor de bescherming van de nationale veiligheid, defensie, openbare veiligheid, of de voorkoming, opsporing en vervolging van strafbare feiten. Dit betekent bijvoorbeeld dat inzage kan worden geweigerd als een lopend opsporingsonderzoek daardoor in gevaar komt.

Kijk voor alle beperkingen in artikel 41 Uitvoeringswet AVG. Als een beperking later niet meer van toepassing is, bijvoorbeeld omdat een lopend opsporingsonderzoek is afgerond, moet alsnog aan het verzoek worden voldaan. Het is verstandig om dit periodiek te controleren en in het systeem een automatische herinnering in te stellen om na te gaan of de beperking nog geldt.

## 2. Behandeling AVG-verzoeken door contactpunt (artikel 1.2 BGS)

### 2.1 Verantwoordelijkheid contactpunt

Ieder Zorg- en Veiligheidshuis moet een contactpunt aanwijzen (zie de [factsheet Inrichten contactpunt](#)). Het contactpunt is onder meer verantwoordelijk voor de behandeling van AVG-verzoeken van betrokkenen. Het contactpunt moet het verzoek namens alle deelnemers beantwoorden.

De wet maakt het mogelijk dat het contactpunt de beantwoording van AVG-verzoeken mandateert aan bijvoorbeeld de manager van het bureau van het Zorg- en Veiligheidshuis (zie het [model-document mandaatbesluit AVG-verzoeken](#)).

### 2.2 Alleen ten aanzien van gezamenlijke verwerking

Bij het contactpunt kunnen alleen AVG-verzoeken worden ingediend die gaan over de *gezamenlijke* verwerking van persoonsgegevens door het Zorg- en Veiligheidshuis. Het gaat dus om de gegevens die de deelnemers verwerken in het gezamenlijke systeem van het Zorg- en Veiligheidshuis, zoals KeDo of PGAx. Gegevens die deelnemers verwerken in hun eigen systemen, vallen hier niet onder.

### 2.3 Doorzendplicht

Als een betrokkene een AVG-verzoek zoals hiervoor bedoeld niet indient bij het contactpunt, maar bij een andere overheidsdeelnemer, dan moet deze overheidsdeelnemer het verzoek doorsturen naar het contactpunt (artikel 2:3 Algemene wet bestuursrecht). Tegelijk moet de betrokkene worden geïnformeerd over deze doorzending.

Voor private partijen geldt de doorzendplicht van artikel 2:3 Awb niet. Het is wel aan te raden om ook met hen af te spreken dat zij AVG-verzoeken die bij hen worden ingediend, doorsturen naar het contactpunt of dat zij de betrokkene verwijzen naar het contactpunt.

### 2.4 Identiteit betrokkene vaststellen

Voordat het contactpunt een AVG-verzoek in behandeling neemt, moet het de identiteit van de betrokkene controleren. Zo wordt voorkomen dat iemand anders zich voordoet als de betrokkene en persoonlijke informatie ontvangt.

Het contactpunt moet daarbij kiezen voor de minst ingrijpende methode om de identiteit te controleren. Dit kan bijvoorbeeld op de volgende manieren:

#### • DigiD

Bij digitale aanvragen is inloggen met DigiD een goede en veilige methode. Gemeenten hebben vaak al een digitale mogelijkheid voor het indienen van AVG-verzoeken, waarbij met DigiD moet worden ingelogd. Het is handig om via deze ingang ook AVG-verzoeken bij het Zorg- en Veiligheidshuis mogelijk te maken.

#### • Persoonlijk

Mensen die het lastig vinden om een AVG-verzoek digitaal in te dienen, kunnen worden gevraagd om persoonlijk langs te komen, bijvoorbeeld bij de balie in het stadhuis. Zij kunnen daar een geldig identiteitsbewijs tonen, zoals een paspoort of ID-kaart.

#### • Kopie identiteitsbewijs

Als een betrokkene het verzoek schriftelijk indient, bijvoorbeeld per brief, kan worden gevraagd om een kopie van het identiteitsbewijs mee te sturen. Maar let op: vraag de betrokkene dan altijd om maatregelen te nemen om misbruik te voorkomen, voor het geval de brief in verkeerde handen komt. Geef daarbij de volgende instructies:

- Maak het Burgerservicenummer (BSN) onleesbaar, ook in de cijferreeks onderaan.
- Maak de foto onleesbaar.
- Schrijf op de kopie dat het een kopie is.

- Schrijf op de kopie voor welke instantie de kopie is bedoeld.
- Schrijf op de kopie de datum van verzending.

Voor een veilige kopie kan ook gebruik worden gemaakt van de app KopieID van de rijksoverheid.

### 2.5 Termijn voor beantwoorden AVG-verzoek

Een AVG-verzoek moet in principe binnen één maand worden beantwoord. Deze termijn begint te lopen op het moment dat de identiteit van de betrokkene is vastgesteld (zie vorige paragraaf).

In uitzonderlijke gevallen kan de termijn met twee maanden worden verlengd, bijvoorbeeld als het verzoek ingewikkeld is of als het dossier omvangrijk is. Het contactpunt moet dan wel binnen één maand aan de betrokkene laten weten dat meer tijd nodig is en waarom.

### 2.6 Overleg met deelnemers

Voordat het besluit wordt genomen, moet het contactpunt overleggen met de deelnemers die bij de behandeling van de casus betrokken zijn of waren en die gegevens hebben ingebracht en/of ontvangen. Deze deelnemers kunnen dan beoordelen of en in hoeverre een uitzondering van toepassing is op de gegevens die van hen afkomstig zijn of op hun betrokkenheid als ontvanger van persoonsgegevens (zie [paragraaf 1.8](#) van deze

factsheet). Als dat zo is, moeten zij aangeven om welke uitzondering het gaat. Ook moet worden afgestemd welke motivering daarvoor in het besluit wordt opgenomen.

Het contactpunt hoeft niet te beoordelen of het beroep van de deelnemer of de uitzondering terecht is. Die beoordeling is aan de deelnemer zelf.

Als een uitzondering naar het oordeel van de betreffende deelnemer niet meer van toepassing is, moet deze deelnemer dit zo spoedig mogelijk aan het contactpunt melden. Het contactpunt moet dan een aanvullend besluit nemen. Daarin moet het verzoek alsnog worden toegewezen zover het gaat om de gegevens die van die deelnemer afkomstig zijn.

Een AVG-verzoek mag niet zonder meer in zijn geheel worden afgewezen als volgens een of meer deelnemers een uitzondering van toepassing is. Het verzoek wordt dan alleen afgewezen zover het gaat om de gegevens waarop die uitzondering van toepassing is. Voor andere gegevens kan het AVG-verzoek wel worden ingewilligd.

### 2.7 Beantwoording AVG-verzoek door andere overheidsdeelnemer

Het kan voorkomen dat het contactpunt niet de meest geschikte partij is om het AVG-verzoek te beantwoorden. Bijvoorbeeld wanneer het dossier vooral gegevens bevat van één van de betrokken deelnemers. In dat geval kan het contactpunt met die deelnemer afspreken dat het AVG-verzoek door die deelnemer wordt afgehandeld.

Die deelnemer moet wel een overheidsdeelnemer zijn. De beantwoording van een AVG-verzoek kan dus niet worden overgedragen aan een private deelnemer. Een private deelnemer kan wel het deel van het besluit dat over zijn gegevens gaat voorbereiden, zodat het contactpunt dit kan opnemen in het besluit.

Als de behandeling van het verzoek wordt overgedragen aan een andere overheidsdeelnemer, moet het contactpunt de betrokkene hierover informeren.

### 2.8 Stappenplan voor behandeling AVG-verzoeken

Zie [bijlage A](#) bij deze factsheet voor een stappenplan dat kan worden gevolgd bij de behandeling van AVG-verzoeken.

## 2.9 Bezwaar en beroep

Het antwoord op een AVG-verzoek is een besluit in de zin van de Algemene wet bestuursrecht. Dat betekent dat de betrokkene binnen zes weken bezwaar kan maken tegen het besluit. Het bezwaar moet worden ingediend bij het contactpunt en wordt ook door het contactpunt behandeld.

Voordat het contactpunt op het bezwaar beslist, moeten belanghebbenden worden gehoord. Dat zijn in ieder geval de deelnemers die bij de behandeling van de casus betrokken zijn of waren en die gegevens hebben ingebracht en/of ontvangen. Het is daarom belangrijk dat het contactpunt deze deelnemers informeert zodra een bezwaar wordt ingediend. Het contactpunt vraagt daarbij of zij bij de hoorzitting aanwezig willen zijn en/of vooraf een schriftelijke zienswijze willen indienen. De betrokkene moet vanzelfsprekend de mogelijkheid krijgen om daarop te reageren, schriftelijk of mondeling tijdens de hoorzitting.

Na het besluit op bezwaar kan de betrokkene beroep instellen bij de bestuursrechter. Het contactpunt is dan de verweerder in de beroepsprocedure. Andere deelnemers kunnen als belanghebbende deelnemen aan deze procedure.



### 3. Informatieverplichting (artikel 1.3 BGS)

#### 3.1 Verantwoordelijkheid contactpunt

Het contactpunt is verantwoordelijk voor de nakoming van de informatieverplichting van artikel 14 AVG. Kort samengevat betekent dit dat het contactpunt ervoor moet zorgen:

- Dat de betrokkene een notificatiebrief, folder of andere schriftelijke informatie ontvangt met alle informatie die op grond van artikel 14 AVG aan de betrokkene moet worden verstrekt.
- Dat een Privacyverklaring op internet wordt gepubliceerd.

Andere vormen zijn ook mogelijk, zoals mondelinge verstrekking in een persoonlijk gesprek of een verwijzing naar informatie op internet. Zorg er bij mondelinge verstrekking wel voor dat wordt verwezen naar de Privacyverklaring of naar andere schriftelijke informatie, zodat de betrokkene de informatie later rustig kan nalezen.

Bekijk de templates die in [paragraaf 3.7](#) van deze factsheet worden besproken. In de volgende paragraaf 3.2 staat welke informatie aan de betrokkene moet worden verstrekt. In [paragraaf 3.8](#) staan de uitzonderingen op de informatieverplichting.

Het contactpunt kan voor de nakoming van de informatieplicht een machtiging verlenen aan bijvoorbeeld de manager van het bureau van het Zorg- en Veiligheidshuis (zie het [modeldocument mandaatbesluit AVG-verzoeken](#)).

#### 3.2 Inhoud informatieverplichting (artikel 14 AVG)

In artikel 14 AVG staat welke informatie aan de betrokkene moet worden verstrekt. Voor Zorg- en Veiligheidshuizen gaat het om de volgende informatie:

- de identiteit van de verwerkingsverantwoordelijken (de overheidsdeelnemers);
- de contactgegevens van het contactpunt;
- de contactgegevens van de coördinerend functionaris voor gegevensbescherming;
- de rechtsgrond voor de verwerking;
- de doeleinden van de verwerking;
- de categorieën persoonsgegevens die worden verwerkt;
- de ontvangers van de persoonsgegevens;
- de bewaartermijnen;
- de rechten van de betrokkene;
- de mogelijkheid om een klacht in te dienen bij de Autoriteit Persoonsgegevens;
- de bron(nen) van de persoonsgegevens;
- of sprake is van geautomatiseerde besluitvorming.

#### 3.3 Alleen ten aanzien van gezamenlijke verwerking

Net als bij AVG-verzoeken geldt de verantwoordelijkheid van het contactpunt alleen voor de *gezamenlijke* verwerking van persoonsgegevens door het Zorg- en Veiligheidshuis.

De informatieverplichting van het contactpunt ontstaat op het moment dat wordt begonnen met deze gezamenlijke verwerking. Dat is het moment waarop een aanmelding van een casus in behandeling wordt genomen door het Zorg- en Veiligheidshuis. Het gaat dan om het moment waarop een volledig ingevulde aanmelding is ontvangen die in aanmerking komt voor 'triage' of 'weging'. In de praktijk wordt deze triage vaak uitgevoerd door de procesregisseur of een triageteam (zie artikel 12 van het [Template Bestuurlijke afspraken](#)).

De aanmelder is verantwoordelijk om de betrokkene te informeren over de *aanmelding* bij het Zorg- en Veiligheidshuis. De aanmelder moet zelf beoordelen of de betrokkene hierover moet worden geïnformeerd. Dat hoeft bijvoorbeeld niet als er een uitzondering van toepassing is (zie [paragraaf 1.8](#) van deze factsheet).

Let op: voor de politie en het Openbaar Ministerie geldt de AVG niet. Zij moeten op grond van respectievelijk de Wet politiegegevens en de Wet justitiële en strafvorderlijke gegevens beoordelen of een betrokkene over de aanmelding moet worden geïnformeerd.

### 3.4 Ook informatieplicht als een casus niet in behandeling wordt genomen

De informatieplicht geldt ook als een casus na triage niet in behandeling wordt genomen, bijvoorbeeld omdat wordt vastgesteld dat de casus niet aan de criteria voldoet. Ook in dat geval heeft er namelijk (in formele zin) een gezamenlijke verwerking van persoonsgegevens plaatsgevonden.

### 3.5 Termijn

Uit artikel 14 lid 3 AVG volgt dat de betrokkene binnen een redelijke termijn moet worden geïnformeerd, maar uiterlijk binnen één maand nadat is begonnen met de gezamenlijke verwerking (zie daarover [paragraaf 3.3](#) van deze factsheet). In [paragraaf 3.8](#) van deze factsheet staan de uitzonderingen op de informatieplicht. Deze uitzonderingen kunnen er ook toe leiden dat de informatieplicht tijdelijk wordt uitgesteld. Het kan bijvoorbeeld voorkomen dat het niet mogelijk is om binnen één maand met alle betrokken deelnemers te overleggen (zie volgende paragraaf). In dat geval kan een beperkte

verlenging van de termijn mogelijk gerechtvaardigd zijn, bijvoorbeeld met het oog op de uitzonderingen die zijn genoemd in [paragraaf 3.8](#) onder b en/of c of ter bescherming van de rechten of vrijheden van anderen, in dit geval de deelnemers (zie [paragraaf 1.8](#) van deze factsheet).

### 3.6 Overleg met deelnemers

Voordat het contactpunt aan de informatieplicht voldoet, moet het overleggen met de betrokken deelnemers. Deze deelnemers kunnen beoordelen of en in hoeverre een uitzondering van toepassing is op de gegevens die van hen afkomstig zijn of op hun betrokkenheid (zie [paragraaf 3.8](#) van deze factsheet).

Het contactpunt hoeft niet te beoordelen of het beroep van de deelnemer of de uitzondering terecht is. Deze beoordeling is aan de deelnemer zelf.

Als een deelnemer aangeeft dat een uitzondering van toepassing is, betekent dit niet altijd dat alle informatieverstrekking achterwege moet blijven. Informatie waarop geen uitzondering van toepassing is, moet gewoon worden verstrekt. Dit kan spelen wanneer een aanmelder aangeeft dat de betrokkene niet mag weten welke partij de aanmelding heeft gedaan, bijvoorbeeld omdat dit de veiligheid van medewerkers in gevaar kan

brenge. In dat geval moet worden afgewogen of dit risico wordt weggenomen door de identiteit van de aanmelder niet te verstrekken. Als dat zo is, kan de overige informatie wel worden verstrekt.

Als een uitzondering volgens de betreffende deelnemer later niet meer van toepassing is, moet de deelnemer dit zo snel mogelijk aan het contactpunt melden. Het contactpunt moet dan alsnog de informatie verstrekken die eerder onder de uitzondering viel.

### 3.7 Templates

Er zijn twee templates voor de notificatiebrief aan betrokkenen:

- [Template notificatiebrief – als een casus in behandeling wordt genomen](#)
- [Template notificatiebrief – als een casus na beoordeling van de criteria NIET in behandeling wordt genomen](#) (zie paragraaf 3.4 op deze pagina)

Bij de notificatiebrief moet de Privacyverklaring als bijlage worden toegevoegd. In deze Privacyverklaring staat alle overige informatie die op grond van artikel 14 AVG aan de betrokkene moet worden verstrekt. De Privacyverklaring moet daarnaast ook op internet worden gepubliceerd. Zie hiervoor:

- [Template privacyverklaring](#)

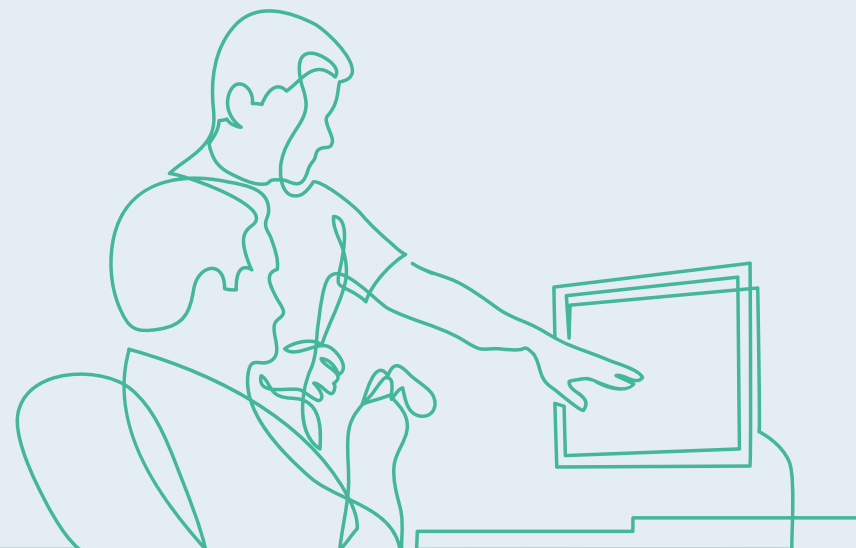
### 3.8 Uitzonderingen informatieverplichting

Op de informatieverplichting gelden verschillende uitzonderingen. In de eerste plaats gaat het om de algemene uitzonderingen besproken in **paragraaf 1.8** van deze factsheet. Daarnaast gelden de volgende uitzonderingen die (in theorie) relevant kunnen zijn voor Zorg- en Veiligheidshuizen (zie voor alle uitzonderingen artikel 14 lid 5 AVG):

- **De betrokkene beschikt al over de informatie**  
Als de betrokkene al beschikt over alle informatie die verstrekt moet worden, hoeft hij niet opnieuw te worden geïnformeerd. Dit kan bijvoorbeeld het geval zijn wanneer de aanmelder de betrokkene al volledig heeft geïnformeerd. De betrokkene moet dan wel nog worden geïnformeerd over de uitkomst van de triage of weging. Het is aan te raden om de betrokkene op dat moment voor de zekerheid alsnog de volledige informatie toe te sturen.
- **Informatieverstrekking is onmogelijk of vraagt onevenredig veel inspanning**  
De informatieverplichting geldt niet als het verstrekken van de informatie onmogelijk blijkt of onevenredig veel inspanning zou vergen. Dit kan bijvoorbeeld spelen wanneer de betrokkene geen bekend adres heeft en onvindbaar is. Zodra het weer mogelijk is om de betrokkene te informeren of dit geen onevenredige inspanning meer vergt, moet de informatie alsnog worden verstrekt.

- **Informatieverstrekking belemmert het doel van de verwerking**

De informatieverplichting geldt ook niet als het verstrekken van de informatie “de verwezenlijking van de doeleinden van de verwerking onmogelijk dreigt te maken of ernstig in het gedrang dreigt te brengen”. Dit zal bij verwerkingen door Zorg- en Veiligheidshuizen niet snel voorkomen. In theorie kan het toch gebeuren dat een goede behandeling van de casus niet mogelijk is wanneer de betrokkene weet dat hij in het Zorg- en Veiligheidshuis wordt besproken.



## 4. Meldplicht datalekken (artikel 1.4 BGS)

### 4.1 Verantwoordelijkheid contactpunt

De laatste verantwoordelijkheid van het contactpunt is het nakomen van de meldplicht bij datalekken (artikel 1.4 BGS). Deze meldplicht omvat:

- Het melden van het datalek aan de Autoriteit Persoonsgegevens (artikel 33 AVG).
- Het melden van het datalek aan de betrokkene (artikel 34 AVG).
- Het nemen van corrigerende maatregelen naar aanleiding van het datalek.

Ook op deze meldplichten zijn uitzonderingen van toepassing (zie [paragraaf 4.10](#) van deze factsheet)

### 4.2 Wat is een datalek?

In de AVG wordt een datalek “een inbreuk in verband met persoonsgegevens” genoemd. Dit begrip wordt gedefinieerd als “een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens”.

De Autoriteit Persoonsgegevens noemt de volgende doorbeelden van een datalek<sup>3</sup>:

- Persoonsgegevens die naar een verkeerde geadresseerde zijn verstuurd.
- Inzage in een dossier door een onbevoegde medewerker.
- Het verlies van een USB-stick met niet-versleutelde persoonsgegevens.
- Een cyberaanval waarbij persoonsgegevens zijn buitgemaakt.
- Een besmetting met ransomware (gijzelsoftware) waardoor persoonsgegevens ontoegankelijk zijn geworden.

De Autoriteit Persoonsgegevens maakt onderscheid tussen drie soorten datalekken:

#### • Inbreuk op de vertrouwelijkheid

Persoonsgegevens zijn openbaar gemaakt of er is toegang geweest tot persoonsgegevens door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd.

#### • Inbreuk op de integriteit

Persoonsgegevens zijn gewijzigd door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd.

#### • Inbreuk op de beschikbaarheid

De organisatie kan niet meer bij de persoonsgegevens of de gegevens zijn vernietigd. Dit is gebeurd door iemand die daartoe niet bevoegd is. Of dit is per ongeluk gebeurd. Ook een tijdelijke onbeschikbaarheid kan een datalek zijn als dit ernstige gevolgen heeft voor betrokkenen.

### 4.3 Alleen ten aanzien van gezamenlijke verwerking

Ook voor de meldplicht datalekken geldt dat deze alleen betrekking heeft op datalekken in de gezamenlijke verwerking van persoonsgegevens door het Zorg- en Veiligheidshuis. Het kan bijvoorbeeld gaan om persoonsgegevens die door medewerkers van het ondersteunend bureau, zoals de procesregisseur, per ongeluk worden verloren, vernietigd of gewijzigd of aan de verkeerde persoon worden verstrekt. Ook kan het gaan om storingen of problemen in het systeem waarin deelnemers gezamenlijk persoonsgegevens verwerken, zoals KeDo of PGAx.

### 4.4 Termijnen

Nadat het contactpunt kennis heeft genomen van een datalek, gelden de volgende termijnen:

- Neem zo snel mogelijk maatregelen om het datalek te stoppen, als dit nog mogelijk is. Neem daarnaast ook zo spoedig mogelijk maatregelen om de gevolgen van het datalek te beperken.

<sup>3</sup> <https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/wat-is-een-datalek>

- Het datalek moet aan de Autoriteit Persoonsgegevens worden gemeld “zonder onredelijke vertraging en, indien mogelijk, **uiterlijk 72 uur**” nadat het contactpunt er kennis van heeft genomen. Als de melding niet binnen 72 uur plaatsvindt, moet in de melding worden aangegeven waarom dat zo is. Bij twijfel over de vraag of moet worden gemeld of over de vraag of er daadwerkelijk sprake is van een datalek, kan bij de Autoriteit Persoonsgegevens een voorlopige melding worden gedaan. Zo kan de Autoriteit Persoonsgegevens worden geïnformeerd dat een mogelijk datalek wordt onderzocht.
- Aan de betrokkene moet het datalek “onverwijld” worden gemeld.

#### 4.5 Overleg met deelnemers en informatieplicht deelnemers

Als zich een datalek heeft voorgedaan, moet het contactpunt zo snel mogelijk overleggen met de betrokken deelnemers. Dit overleg heeft drie doelen:

- De deelnemers moeten het contactpunt zo snel mogelijk de informatie geven die nodig is om aan de meldplichten te voldoen. Doen zij dat niet, dan zijn zij zelf aansprakelijk voor het deel van de schade dat daardoor ontstaat (zie artikel 82 lid 5 AVG).
- De deelnemers moeten aangeven of een uitzondering van toepassing is waardoor de meldplicht geheel of gedeeltelijk achterwege kan blijven (zie [paragraaf 4.10](#) van deze factsheet).

- Met de deelnemers kan worden overlegd over de maatregelen die moeten worden genomen en over de vraag wie deze maatregelen uitvoert (zie verderop deze pagina bij paragraaf 4.8). De verantwoordelijkheid hiervoor ligt bij het contactpunt, maar de feitelijke uitvoering kan door één of meer deelnemers gebeuren als dat effectiever is.

Het contactpunt hoeft niet te beoordelen of het beroep van een deelnemer of een uitzondering terecht is. Die beoordeling is aan de deelnemer zelf.

Als een deelnemer aangeeft dat een uitzondering van toepassing is, betekent dit niet altijd dat de melding van het datalek helemaal achterwege kan blijven. Soms kan de meldplicht na toepassing van de uitzondering gedeeltelijk worden nagekomen.

#### 4.6 Wat moet worden gemeld?

Aan de Autoriteit Persoonsgegevens moet de volgende informatie worden verstrekt:

- De aard van de inbreuk, met daarbij de categorieën van getroffen betrokkenen en persoonsgegevensregisters en, bij benadering, het aantal getroffen betrokkenen en persoonsgegevensregisters.
- De naam en contactgegevens van de coördinerend functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen.

- De waarschijnlijke gevolgen van het datalek.
- De maatregelen die naar aanleiding van het datalek zijn genomen en voorgesteld.

Als het niet mogelijk is om al deze informatie tegelijk te verstrekken, mag de informatie in stappen worden verstrekt.

Aan de betrokkene moet dezelfde informatie worden verstrekt, in duidelijke en eenvoudige taal.

#### 4.7 Hoe moet worden gemeld?

Op de website van de Autoriteit Persoonsgegevens staat hoe een datalek moet worden gemeld.<sup>4</sup> Daar staan ook tips over de manier waarop betrokkenen kunnen of moeten worden geïnformeerd.<sup>5</sup> De melding kan worden gedaan door iedere bevoegde medewerker binnen de organisatie. Het is dus niet verplicht dat meldingen worden gedaan door de functionaris voor gegevensbescherming.

#### 4.8 Maatregelen nemen

Op het contactpunt rust ook de verplichting om de schadelijke gevolgen van het datalek te beperken. Eerst moet het datalek onmiddellijk worden gestopt, als dit nog mogelijk is. Daarna moeten

<sup>4</sup> <https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/zo-meldt-u-een-datalek>

<sup>5</sup> <https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/zo-informeert-u-slachtoffers-over-een-datalek>

maatregelen worden genomen om de negatieve gevolgen te beperken.

- De Autoriteit Persoonsgegevens noemt onder meer de volgende voorbeelden van maatregelen<sup>6</sup>:
- Een laptop, tablet of smartphone op afstand wissen of versleutelen.
- Een gepubliceerd bestand offline halen.
- Een verkeerde ontvanger vragen om te bevestigen dat de gegevens uit een brief of e-mail zijn vernietigd.
- De toegang tot een medewerkersaccount of clouddienst op afstand blokkeren.
- Bij de informatie aan betrokkenen aangeven wat zij kunnen doen om de schade te beperken.
- Diepgaand onderzoek doen bij een complex datalek.

#### 4.9 Datalekregister

Het contactpunt moet alle datalekken documenteren. Per datalek moet worden vastgelegd:

- Welke feiten hebben gespeeld.
- Wat de gevolgen van het datalek waren.
- Welke maatregelen zijn genomen.

<sup>6</sup> <https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/datalek-dit-moet-u-doen#stap-2-beperken-schadelijke-gevolgen-datalek>

Zo kan de Autoriteit Persoonsgegevens controleren of de meldplicht is nageleefd. Zie voor meer informatie de website van de Autoriteit Persoonsgegevens en de 10 tips voor een professionele datalekregistratie.<sup>7</sup>

#### 4.10 Uitzonderingen

Op de meldplichten bij datalekken zijn in de eerste plaats de algemene uitzonderingen van toepassing (zie [paragraaf 1.8](#) van deze factsheet). Daarnaast gelden de volgende uitzonderingen:

- Melding aan de Autoriteit Persoonsgegevens en de betrokkenen kan achterwege blijven als het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van natuurlijke personen. Hiervoor moet dus een risico-inschatting worden gemaakt.
- Melding aan de betrokkenen kan ook achterwege blijven in de volgende gevallen:
  - Er zijn vooraf passende maatregelen genomen die de persoonsgegevens onbegrijpelijk maken voor onbevoegden, zoals versleuteling.
  - Er zijn achteraf maatregelen genomen die ervoor zorgen dat het datalek is beëindigd en het hoge risico voor de slachtoffers zich waarschijnlijk niet of niet meer voordoet.

<sup>7</sup> <https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/datalek-dit-moet-u-doen#stap-2-beperken-schadelijke-gevolgen-datalek>

- Het individueel informeren van de slachtoffers vraagt een onevenredige inspanning.

De website van de Autoriteit Persoonsgegevens geeft handvatten om te beoordelen of deze uitzonderingen van toepassing zijn.<sup>8</sup>

#### 4.11 Stappenplan datalekken

Een stappenplan voor de behandeling van datalekken is opgenomen in [bijlage B](#) van deze factsheet.

### Meer informatie en contactgegevens

Heb je vragen of opmerkingen?

Mail naar: [werkgroepWGS@hetccv.nl](mailto:werkgroepWGS@hetccv.nl)

<sup>8</sup> <https://www.autoriteitpersoonsgegevens.nl/themas/beveiliging/datalekken/datalek-wel-of-niet-melden>

# Bijlage A – Voorbeeld stappenplan AVG-verzoeken

## Week 1

### Stap 1: Registreer ontvangst

Registreer de ontvangst van het verzoek. Het is aan te raden hiervoor een op maat gemaakt registratiesysteem te gebruiken. Daarmee kunnen ook termijnen goed worden bewaakt.

### Stap 2: Stel identiteit verzoeker vast

Controleer of de verzoeker zich heeft geïdentificeerd. Is dat nog niet gebeurd, vraag de verzoeker dan om zich alsnog te identificeren (zie [paragraaf 2.4](#) van deze factsheet)

### Stap 3: Registreer termijn

Registreer de uiterste datum waarop het verzoek moet zijn beantwoord (zie [paragraaf 2.5](#) van deze factsheet).

### Stap 4: Bevestig ontvangst

Bevestig de ontvangst van het verzoek schriftelijk aan de betrokkene. Geef daarbij aan dat ernaar wordt gestreefd om binnen een maand op het verzoek te antwoorden. Geef ook aan dat de betrokkene opnieuw bericht krijgt als het niet lukt om binnen deze termijn te reageren.

### Stap 5: Deelnemers informeren

Informeer, tegelijk met stap 4, de betrokken deelnemers over het verzoek. Vraag hen om binnen bijvoorbeeld twee weken te laten weten of en waarom een uitzondering van toepassing is (zie [paragraaf 1.8](#) en [paragraaf 2.6](#) van deze factsheet) en of zij verder nog een zienswijze hebben naar aanleiding van het AVG-verzoek.

### Stap 6: Contact met betrokkene

Overweeg of telefonisch contact met de betrokkene nodig is om beter te begrijpen wat het doel van het verzoek is. Dat kan bijvoorbeeld nodig zijn als het verzoek onduidelijk is, of als de verzoeker een beroep heeft gedaan op de Woo (zie [paragraaf 1.3](#) van deze factsheet).

Ook in andere gevallen kan contact nuttig zijn. De betrokkene kan dan toelichten wat het doel van het verzoek is. Daarmee kan bij de beantwoording rekening worden gehouden.

### Stap 7: Kwalificatie verzoek

Stel vast en registreer om welk type AVG-verzoek het gaat: inzage, correctie, wissing, beperking, bezwaar of een combinatie daarvan.

## Week 2 en 3

### Stap 8: Afstemming met deelnemers

Geef de betrokken deelnemers, als dat nodig is, een update naar aanleiding van stap 6 en 7. Ontvang en verwerk de input en zienswijzen van de deelnemers.

### Stap 9: Conceptbesluit opstellen

Stel het concept besluit op.

### Stap 10: Conceptbesluit voorleggen

Leg het conceptbesluit voor aan de deelnemers en geef hen een reactietermijn.

## Week 4

### Stap 11: Besluit finaliseren

Verwerk de eventuele opmerkingen van de deelnemers en finaliseer het besluit.

### Stap 12: Ondertekening en verzending

Zorg voor ondertekening van het besluit door het contactpunt of door de gemandateerde namens het contactpunt. Stuur het besluit daarna naar de betrokkene.

## Bijlage B – Voorbeeld stappenplan datalekken

### Dag 1

#### Stap 1: Registratie datalek

Registreer het datalek. Het is aan te raden hiervoor een op maat gemaakt registratiesysteem te gebruiken (zie [paragraaf 4.9](#) van deze factsheet).

#### Stap 2: Deelnemers informeren

Informeer de betrokken deelnemers over het datalek en vraag hen om binnen 24 uur alle informatie te verstrekken die nodig is om aan de meldplicht te voldoen (zie [paragraaf 4.5](#) van deze factsheet). Vraag ook of volgens hen een uitzondering van toepassing is (zie [paragraaf 4.10](#) van deze factsheet). Plan direct een overleg met hen in voor de volgende dag.

#### Stap 3: Formulier invullen

Begin alvast met het invullen van het meldformulier op de website van de Autoriteit Persoonsgegevens (zie [paragraaf 4.6 en 4.7](#) van deze factsheet). De melding kan als concept worden opgeslagen en later worden gewijzigd, aangevuld of ingetrokken.

### Dag 2

#### Stap 4: Overleg met deelnemers

Ontvang de informatie van de deelnemers. Stel vast of er volgens de deelnemers een of meer uitzonderingen van toepassing zijn. Overleg ook over de maatregelen die moeten worden genomen.

#### Stap 5: Informatie registreren

Registreer alle informatie over het datalek (zie [paragraaf 4.9](#) van deze factsheet).

#### Stap 6: Meldplicht en maatregelen vaststellen

Weeg af en stel vast of het datalek moet worden gemeld aan:

- de Autoriteit Persoonsgegevens en
- de betrokkene(n).

Registreer de uitkomst van deze afweging. Bepaal ook welke maatregelen moeten worden genomen. Leg vast welke maatregelen wanneer worden genomen.

#### Stap 7: Maatregelen nemen

Begin, voor zover mogelijk, met de uitvoering van de maatregelen (zie [paragraaf 4.8](#) van deze factsheet).

### Dag 3

#### Stap 8: Melding aan de Autoriteit Persoonsgegevens

Is de uitkomst van stap 6 dat het datalek moet worden gemeld, dan moet de melding op de website van de Autoriteit Persoonsgegevens worden gefinaliseerd en ingediend. Is dat niet nodig, trek dan de concept-melding in.

#### Stap 9: Melding aan de betrokkene(n)

Is de uitkomst van stap 6 is dat het datalek moet worden gemeld aan de betrokkene, meld het datalek dan aan de betrokkene(n) (zie [paragraaf 4.7](#) van deze factsheet).

#### Stap 10: Registratie afronden

Rond de registratie in het registratiesysteem af.

## Later

### **Stap 11: Achterstallige stappen alsnog uitvoeren**

Zijn niet alle stappen binnen 72 uur uitgevoerd, registreer dan waarom dat niet is gebeurd en voer deze zo spoedig mogelijk alsnog uit. Vermeld de reden ook in de melding aan de Autoriteit Persoonsgegevens, als de uitkomst van stap 6 is dat het datalek moet worden gemeld.

### **Stap 12: Reactie Autoriteit Persoonsgegevens**

Meestal reageert de Autoriteit Persoonsgegevens niet op een melding. Gebeurt dat wel, beantwoord dan de eventuele vragen en volg eventuele aanvullende instructies op.

