



AVG

verstrekkingswijzer

2025



Inleiding

U bent van plan (persoons)gegevens vanuit uw organisatie te delen met een andere organisatie. Door het doorlopen van de vragen in deze verstrekkingswijzer kunt u bepalen of u de gegevens mag delen en onder welke voorwaarden dit kan. De AVG gaat voor persoonsgegevens uit van het principe ‘niet delen, tenzij’.

Hieronder vindt de uitzonderingen.

Deze verstrekkingswijzer geldt zowel voor gegevensdeling binnen als tussen het publieke en/of private domein. Deze verstrekkingswijzer geldt ook voor de gevallen waarin een andere organisatie gegevens bij uw organisatie opvraagt.

Een organisatie mag niet zomaar persoonsgegevens delen met een andere partij. Het delen van persoonsgegevens is namelijk een verwerking in de zin van de AVG. Er moet een rechtmatig doel zijn van de verwerking, wat inhoudt dat er een wettelijke grondslag nodig is, die aansluit op het doel van de verwerking. Hier wordt dieper op ingegaan in deze verstrekkingswijzer. Naast rechtmatigheid zijn er andere basisvereisten voor het verwerken (delen) van persoonsgegevens. Deze staan in artikel 5 van de AVG en een (verwerkingsverantwoordelijke) organisatie moet zich aantoonbaar kunnen verantwoorden over de naleving hiervan. Ook moet er rekening gehouden worden met (een proces rondom) de (AVG-)rechten van betrokkenen.

Naast de AVG zijn de Uitvoeringswet AVG (UAVG) en sectorale wetgeving van toepassing op besluitvorming rondom gegevensdeling. Raadpleeg daarom naast deze verstrekkingswijzer de UAVG en sectorale wetgeving om na te gaan of aanvullende vereisten of afwegingen van toepassing zijn.

Persoonsgegevens die onder de Wet op de inlichtingen- en veiligheidsdiensten (Wiv), de Wet politiegegevens (Wpg) of de Wet justitiële en strafvorderlijke gegevens (Wjsg) vallen, hebben een eigen (gesloten) verstrekking regime. Bepaal daarom eerst of het een AVG-vraagstuk is en raadpleeg de andere regimes waar van toepassing.

Onderstaand is te vinden:

Afwegingskader (stroomschema)

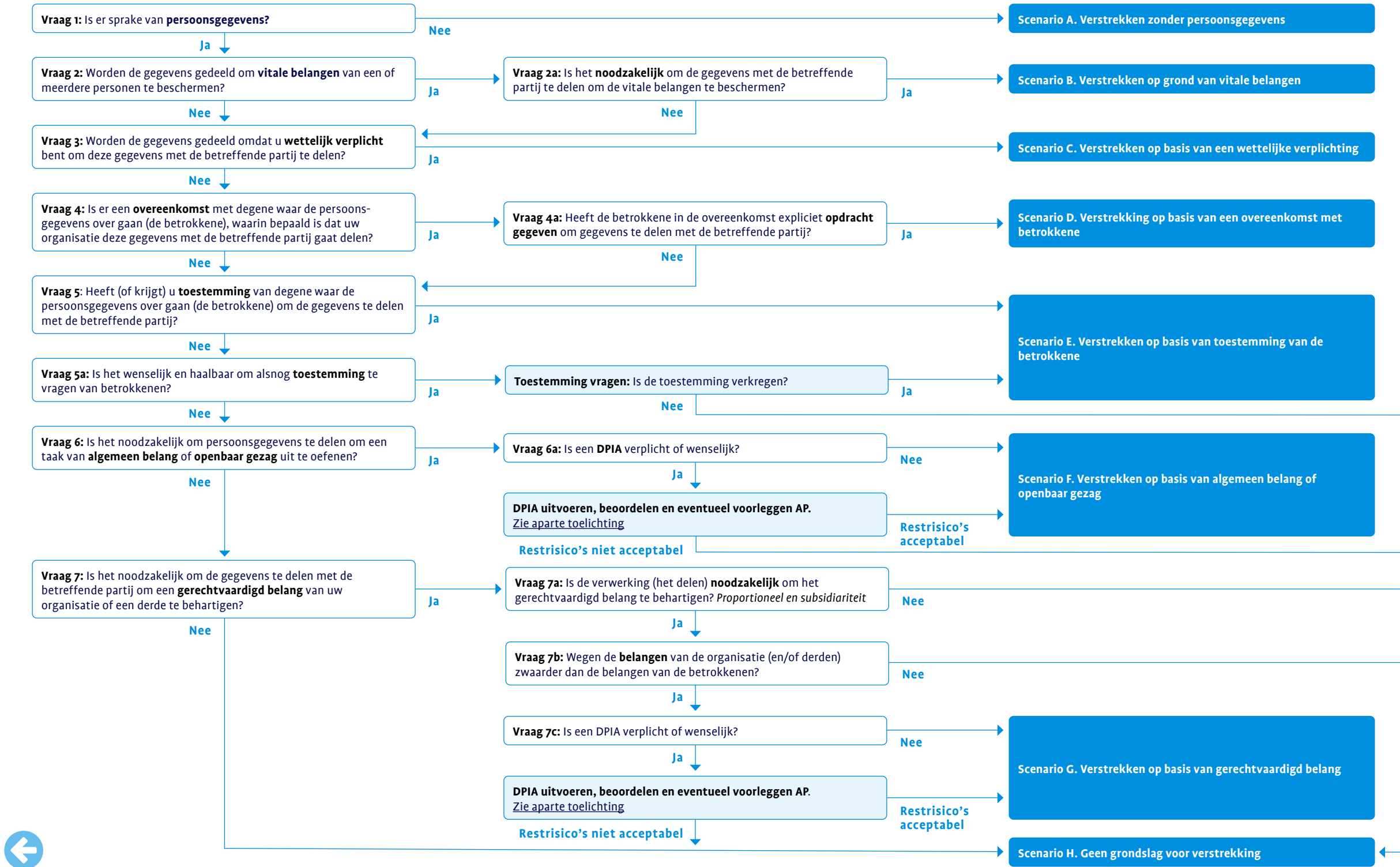


Toelichting afwegingskader



Toelichting per scenario





Afwegingskader (stroomschema) ➔

Toelichting afwegingskader ➔

Toelichting per scenario ➔

Een afwegingskader gegevensverstrekking

Als er sprake is van het delen van **persoonsgegevens**, moet vastgesteld worden op basis van welke wettelijke grondslag (artikel 6 AVG) de gegevens gedeeld kunnen worden. De vragen in deze verstrekkingwijzer vormen een beslisboom in dit kader.

* De verplichting om een DPIA uit te voeren kan bij alle grondslagen van toepassing zijn. Specifiek voor het extern delen van persoonsgegevens, waar dit afwegingskader op toeziet, ligt een DPIA-plicht echter niet voor de hand bij de eerste vier grondslagen in het stroomschema.



Vraag 1: Is er sprake van persoonsgegevens?

Persoonsgegevens zijn alle gegevens die betrekking hebben op een geïdentificeerde **of identificeerbare** natuurlijke persoon. Deze persoon wordt dan een betrokkene genoemd. Persoonsgegevens vallen onder de Algemene Verordening Gegevensbescherming (AVG). Losse gegevens, die gecombineerd kunnen leiden tot de identificatie van een persoon, worden ook gezien als persoonsgegevens.

Een voorbeeld: Een kenteken is op zichzelf geen persoonsgegeven, maar als dit gecombineerd wordt met de straatnaam van de eigenaar, is de herleidbaarheid naar die persoon aanzienlijk vergroot. In dit scenario kan zowel het kenteken als de straatnaam aangemerkt worden als persoonsgegeven.

Geanonimiseerde gegevens worden niet gezien als persoonsgegevens, en vallen daarom niet onder de AVG. Hierbij moet opgemerkt worden dat **pseudonimisering** niet gelijkstaat aan anonimisering. Anonieme gegevens zijn niet (direct of indirect) herleidbaar naar een natuurlijk persoon. Gepseudonimiseerde persoonsgegevens zijn op enige wijze getransformeerde gegevens om directe herleidbaarheid naar personen te voorkomen. Dit kan bijvoorbeeld door een naam te veranderen in een nummer. Zolang dit proces omkeerbaar is, bijvoorbeeld doordat een (encryptie)sleutel of koppeltabel bewaard blijft, worden deze gegevens nog steeds gezien als persoonsgegevens en vallen deze gewoon onder de AVG.

Anonimisering kan bereikt worden door het (afdoende) aggregeren van gegevenssets, of het volledig ontdoen van persoonsgegevens bij bijvoorbeeld een casus of een modus operandi.

Let op dat anonimiseren zelf ook een verwerking is. Tot het moment dat de gegevens geanonimiseerd zijn, is de AVG dus nog steeds van toepassing.

Afwegingskader (stroomschema) →

Toelichting afwegingskader

Toelichting per scenario →

JA Ga verder naar [vraag 2](#).

NEE Uitkomst scenario **A** uit het stroomschema van het afwegingskader is van toepassing. [Zie 'Toelichting per scenario'](#) voor het handelingsperspectief bij dit scenario.



Vraag 2: Worden de gegevens gedeeld om **vitale belangen** van een of meerdere personen te beschermen?

Deze grondslag kan slechts in enkele gevallen gebruikt worden.

Een **vitaal belang** is een belang dat essentieel is voor iemands leven of gezondheid. Deze grondslag mag alleen toegepast worden als de persoon in kwestie (de betrokkene) niet om toestemming gevraagd kan worden.

(artikel 6 lid 1, onder d, AVG)

Behalve voor de betrokkene zelf kan het vitaal belang ook een belang zijn voor andere (natuurlijke) personen, bijvoorbeeld als de betrokkene een levensbedreigende besmettelijke ziekte heeft. Maar deze grondslag is alleen geldig voor de persoonsgegevens van de persoon (of personen) waar geen toestemming van gevraagd kan worden.

 **Een voorbeeld:** Bij een bedrijfsongeval raakt iemand ernstig gewond. De persoon is bewusteloos geraakt en daardoor niet aanspreekbaar. U belt de hulpdiensten en geeft de benodigde persoonsgegevens van het slachtoffer door.

 **Een voorbeeld van wat niet mag:** Een arbo-arts heeft in het kader van re-integratie van een medewerker van uw organisatie geconstateerd dat de medewerker een slaapstoornis heeft. De arbo-arts deelt dit met de HR-verantwoordelijke van uw organisatie, zodat hier rekening mee gehouden kan worden bij het re-integratietraject.

Deze gegevensverstrekking is mogelijk wél essentieel, maar omdat de mogelijkheid er is om toestemming te vragen aan de medewerker, kan de grondslag 'vitale belangen' niet gebruikt worden.

Afwegingskader (stroomschema) 

Toelichting afwegingskader

Toelichting per scenario 

JA Ga verder naar [vraag 2a](#).

NEE Ga verder naar [vraag 3](#).



Vraag 2a: Is het **noodzakelijk** om de gegevens met de betreffende partij te delen om de vitale belangen te beschermen?

Het delen van gegevens in het kader van het beschermen van een vitaal belang is noodzakelijk als er geen alternatieve oplossingen zijn om dit doel te bereiken.

Delen is niet noodzakelijk als:

- het ook een optie is om de gegevens niet met de betreffende partij te delen, zonder dat dit levensbedreigend is voor de betrokkene;
- het een betere optie is om de gegevens met een andere partij te delen, bijvoorbeeld vanuit privacyoverwegingen of omdat een andere partij de (vitale) belangen beter kan behartigen.

Bijvoorbeeld bij een bedrijfsongeval, waarbij het slachtoffer niet aanspreekbaar is, is het noodzakelijk om persoonsgegevens aan de hulpdiensten te verstrekken, maar is het in het kader van vitale belangen in beginsel niet noodzakelijk om de huisarts van het slachtoffer in te lichten. De hulpdiensten (ambulance; brandweer) kunnen de vitale belangen van de betrokkene waarschijnlijk beter behartigen dan de huisarts. De hulpdiensten kunnen vervolgens alsnog besluiten de huisarts te benaderen.

Let op dat het hier om gegevens over gezondheid kan gaan, wat een bijzondere categorie van persoonsgegevens is. Hier geldt een verwerkingsverbod op, maar op grond van artikel 9 lid 2, onder c, AVG is er bij deze grondslag een uitzondering op dit verbod van toepassing.

In algemene zin moet het doel van het delen in verhouding zijn met de inbreuk op de privacy van de betrokkenen. (evenredigheid of proportionaliteit) Ook moet het doel niet op een andere manier bereikt kunnen worden, die minder negatieve gevolgen heeft voor betrokkenen. (subsidiariteit)

Anders is niet voldaan aan de voorwaarde van noodzakelijkheid.

Afwegingskader (stroomschema) →

Toelichting afwegingskader

Toelichting per scenario →

JA Uitkomst scenario **B** uit het stroomschema van het afwegingskader is van toepassing. Zie 'Toelichting per scenario' voor het handelingsperspectief bij dit scenario.

NEE Ga verder naar [vraag 3](#).



Vraag 3: Worden de gegevens gedeeld omdat u **wettelijk verplicht** bent om deze gegevens met de betreffende partij te delen?

Van een **wettelijke verplichting** als verstrekingsgrondslag is sprake als een wet (of ministeriële regeling) vereist dat gegevens worden gedeeld met een externe partij. (artikel 6 lid 1, onder c, AVG)

De betreffende wettelijke verplichtingen zijn niet vastgelegd in de AVG zelf, maar zijn te vinden in andere algemene en sectorale wetgeving. Dit gaat om nationale of EU-wetgeving. Als een wettelijke verplichting opgenomen wordt in lagere regelgeving, moet deze altijd een basis hebben in EU- of nationale wetgeving.

 **Een voorbeeld:** Een klant van een autogarage betaalt contant € 20.000 voor een gebruikte auto. De garagehouder moet de 'ongebruikelijke transactie' melden via het meldportaal van de Financial Intelligence Unit – Nederland, op basis van de verplichting onder de Wwft. Alleen de gegevens die noodzakelijk zijn om aan de meldplicht te voldoen, mogen worden gedeeld.

 **Een voorbeeld van wat niet mag:** Op basis van de Wet maatschappelijke ondersteuning heeft Veilig Thuis de plicht om intern gegevens over huiselijk geweld en kindermishandeling in dossiers bij te houden. Veilig Thuis wil deze gegevens met partijen binnen een samenwerkingsverband delen. Maar omdat de

wettelijke plicht niet toeziet op het delen van de gegevens met partijen binnen een samenwerkingsverband, kan deze grondslag niet gehanteerd worden voor de gegevensverstrekking.

De wet is niet altijd specifiek. Soms zegt de wet namelijk wel iets over de informatie die gedeeld mag of moet worden, maar is niet concreet opgenomen welke gegevenscategorieën daaronder vallen. Daarom moet altijd nog worden vastgesteld welke persoonsgegevens noodzakelijk zijn om te delen, om aan het doel van de wettelijke verplichting te kunnen voldoen.

Een aantal wettelijke verplichtingen is van toepassing op vrijwel alle organisaties, zoals het verstrekken van inkomensgegevens van medewerkers aan de Belastingdienst (onder de Algemene wet inzake Rijksbelastingen), of het delen van personeelsgegevens rondom uitkeringen met het UWV (onder bijvoorbeeld artikelen 38 en 39 Ziektewet). Ook kan het in geval van een ernstig misdrijf verplicht zijn om vanuit uw organisatie aangifte te doen bij de politie. (artikel 160 Wetboek van Strafvordering) Andere wettelijke verplichtingen zijn sector-specifiek. Voorbeelden hiervan zijn de Zorgverzekeringswet, Participatiewet, Jeugdwet, Wet maatschappelijke ondersteuning, Huisvestingswet, Woningwet, Telecommunicatiewet en de Drank- en Horecawet.

 **Let op:** Wanneer een betrokkene u op basis van het recht op overdraagbaarheid van gegevens (artikel 20 AVG) verzoekt om persoonsgegevens te delen met een andere partij, dan is de grondslag wettelijke verplichting voor u ook van toepassing op het delen. Een dergelijk verzoek valt dus niet onder de grondslag toestemming. Een belangrijk punt bij het recht op overdraagbaarheid, is dat dit recht niet uitgeoefend kan worden als uw organisatie verplicht is bepaalde gegevens te bewaren. Een verzoek van een personeelslid om het personeelsdossier volledig over te dragen aan een nieuwe werkgever, kan bijvoorbeeld niet gehonoreerd worden, vanwege de eigen bewaarplicht van uw organisatie.

NB Het recht op overdraagbaarheid is alleen van toepassing bij verwerking onder de grondslagen 'toestemming' of 'overeenkomst' én als de verwerking met geautomatiseerde procedures plaatsvindt.

JA Uitkomst scenario **C** uit het stroomschema van het afwegingskader is van toepassing. Zie 'Toelichting per scenario' voor het handelingsperspectief bij dit scenario.

NEE Ga verder naar [vraag 4](#).



Vraag 4: Is er een **overeenkomst** met degene waar de persoonsgegevens over gaan (de betrokkene), waarin bepaald is dat uw organisatie deze gegevens met de betreffende partij gaat delen?

Deze grondslag kan gehanteerd worden als u een **overeenkomst heeft met een persoon** (betrokkene), en daarvoor het verwerken van persoonsgegevens noodzakelijk is. (artikel 6 lid 1, onder b, AVG)

Een voorbeeld (interne verwerking):

Een telecomprovider verkoopt een telefoonabonnement aan een particuliere klant, waarbij de klant akkoord gaat met de overeenkomst. Omdat deze overeenkomst er is, is het voor de telecomprovider nu noodzakelijk om bepaalde gegevens **intern** te verwerken, zoals NAW-gegevens en het IBAN van de klant.

Een veelgemaakte fout bij het hanteren van deze grondslag, voor het **extern delen** van persoonsgegevens, is dat organisaties een overeenkomst met een andere organisatie beschouwen als grondslag voor het uitwisselen van persoonsgegevens. Omdat de betrokkene geen partij is in de overeenkomst, is een dergelijke overeenkomst niet geldig voor het toepassen van deze grondslag. In de drie voorbeelden hieronder wordt dit nader geïllustreerd.

 **Een ander voorbeeld (delen met externe partij):** Een persoon geeft een notaris (via een overeenkomst) de opdracht om zijn persoonsgegevens op een vastgesteld moment te delen met gespecificeerde derde partijen. De notaris deelt de specifieke persoonsgegevens om de

overeenkomst uit te voeren. Het delen van de persoonsgegevens gebeurt hier op basis van een overeenkomst tussen de notaris en de betrokkene.

 **Een voorbeeld van wat niet mag:** Een telecomprovider beschikt over veel persoonsgegevens van telecomklanten. De telecomprovider sluit een overeenkomst met een marketingbedrijf, dat onder die overeenkomst tegen betaling persoonsgegevens over de telecomklanten ontvangt.

De overeenkomst kan in dit geval niet als grondslag gehanteerd worden, omdat de betrokkenen (de klanten) geen partij zijn in deze overeenkomst.

 **Een ander voorbeeld van wat niet mag:** Samenwerkende partijen in het publieke en private domein sluiten een convenant, waarin bepaald wordt dat persoonsgegevens van personen in een bepaalde doelgroep worden uitgewisseld.

Een convenant mag nooit gebruikt worden om de grondslag 'overeenkomst' toe te passen voor de gegevensuitwisseling, omdat de betrokkenen geen partij zijn in deze overeenkomst.

Voor de voorbeelden van wat niet mag, moet voor het delen van persoonsgegevens bepaald

worden of een andere grondslag van toepassing is, zoals gerechtvaardigd belang, een wettelijke verplichting of toestemming van de betrokkene. Ook voor het inschakelen van verwerkers kan een verwerkersovereenkomst op zichzelf niet de grondslag zijn voor het delen van persoonsgegevens met de verwerker, omdat de betrokkene geen partij is in een verwerkersovereenkomst. In vrijwel alle gevallen is gerechtvaardigd belang ([zie vraag 7](#)) de juiste verwerkingsgrondslag voor het delen van persoonsgegevens met een verwerker.

Wanneer in een overeenkomst met een betrokkene benoemd staat dat persoonsgegevens met een andere partij gedeeld worden, moeten het doel en de grondslag voor het delen duidelijk uitgelegd worden. Wanneer toestemming gevraagd wordt voor het delen, moet deze toestemming voldoen aan de vereisten die bij vraag 5 beschreven zijn.

 **Let op:** In de meeste praktijkgevallen komt de noodzaak (of het recht) om gegevens van betrokkenen met andere partijen te delen niet voort uit de overeenkomst met de betrokkene. In die gevallen verwerkt uw organisatie dus alleen zelf persoonsgegevens op grond van de overeenkomst met de betrokkene. Voor het delen met andere partijen is dan een andere grondslag nodig.

JA Ga verder naar [vraag 4a](#).

NEE Ga verder naar [vraag 5](#).



Vraag 4a: Maakt een *opdracht van de betrokkene* om gegevens te delen met de specifieke partij onderdeel uit van deze overeenkomst?

Heeft de persoon in de overeenkomst een **opdracht gegeven** om gegevens met de ontvangende partij te delen? Alleen in dat geval is de overeenkomst de grondslag voor het delen.

Zie het tweede voorbeeld dat beschreven is bij vraag 4 voor een illustratie van hoe dit er in de praktijk uit kan zien.

 **Let op:** Als op initiatief van uw organisatie de gegevens gedeeld worden met een derde partij, en daar goedkeuring voor wordt gevraagd via de overeenkomst, dan is dat een vorm van toestemming. Dat is een andere grondslag, met aanvullende voorwaarden. Bij het doorlopen van het stroomschema uit het afwegingskader selecteert u dan 'Nee' bij vraag 4a.

Afwegingskader (stroomschema) 

Toelichting afwegingskader

Toelichting per scenario 

JA Uitkomst scenario **D** uit het stroomschema van het afwegingskader is van toepassing. Zie '[Toelichting per scenario](#)' voor het handelingsperspectief bij dit scenario.

NEE Ga verder naar [vraag 5](#).



Vraag 5: Heeft (of krijgt) u **toestemming** van degene waar de persoonsgegevens over gaan (de betrokkene) om de gegevens te delen met de betreffende partij?

Er is sprake van **toestemming** als een betrokkene verifieerbaar akkoord gegeven heeft op het delen van persoonlijke gegevens. Toestemming (artikel 6 lid 1, onder a, AVG) moet voldoen aan de volgende eisen (artikel 7 AVG):

- Vrijelijk gegeven: niet onder dwang of druk; bij geen toestemming mag de persoon niet benadeeld worden ten opzichte van personen die wél toestemming geven. Dwang of druk kan ook ontstaan in een ongelijke machtsverhouding tussen betrokkenen en een organisatie, zoals van toepassing kan zijn tussen een overheidsorganisatie en een burger, maar ook tussen werkgever en werknemer, en soms ook tussen consument en marktaanbieder.
- Geïnformeerd: het doel is duidelijk; de betrokken organisaties zijn gespecificeerd; specificatie persoonsgegevens; recht om toestemming weer in te trekken (en hoe dit kan).
- Ondubbelzinnig: een expliciete, actieve handeling van de betrokkene; geen vooraf aangevinkte vakjes.
- Specifiek: toestemming voor één doel; andere doelen en verwerkingen apart specificeren én apart toestemming voor vragen.

 **Een voorbeeld:** Een handelsonderneming heeft een overeenkomst met een leverancier. Deze leverancier wil meer inzicht in de samenstelling van de afzetmarkt. Voor een adequate analyse zijn pseudonieme gegevens nodig van klanten van de handelsonderneming. Dit houdt in dat personen niet direct geïdentificeerd kunnen worden op basis van de gedeelde gegevens, maar mogelijk wel indirect, bijvoorbeeld met een koppeltabel die de handelsonderneming beheert. Een interne analyse op de schaal van de gegevensdeling en de gevoeligheid van de persoonsgegevens wijst uit dat 'gerechtvaardigd belang' niet gehanteerd kan worden als grondslag. Toestemming van de betrokkenen blijft over als enige mogelijke grondslag. Daarbij moet voldaan worden aan de eerder genoemde eisen aan geldigheid van toestemming uit artikel 7 AVG.

 **Een voorbeeld van wat niet mag:** Verschillende organisaties hanteren bij de cookie-instellingen voor gebruikers van hun websites vooraf aangevinkte selectievakjes. Cookies, specifiek marketing-gerelateerde cookies, bepalen of gegevens van de gebruiker gedeeld worden met derde partijen. Standaard aangevinkte selectievakjes voor dit type cookies zijn niet toegestaan, omdat de actieve toestemming van websitegebruikers is vereist.

Wanneer toestemming wordt gehanteerd als grondslag voor het verwerken van bijzondere persoonsgegevens (artikel 9 AVG), dan is er een aanvullende vereiste van 'uitdrukkelijke' toestemming nodig. Dit gaat om de manier waarop betrokkenen hun toestemming tot uitdrukking brengen, in de zin van een schriftelijke (of mondelinge) verklaring.

 **Let op:** Als de toestemming nog gevraagd moet worden, moet vooraf nagedacht worden of het praktisch haalbaar is en of het wenselijk is om toestemming als grondslag te hanteren. Toestemming kan namelijk ook weer ingetrokken worden. Dit moet voor de betrokkene net zo makkelijk kunnen als het geven van de toestemming. Het is daarbij ook van belang om vooraf te bedenken wat de impact is van een ingetrokken toestemming op het delen (of al gedeeld hebben) van de persoonsgegevens. Na het intrekken van de toestemming is er namelijk geen grondslag meer voor verwerking. Het is mogelijk dat **gerechtvaardigd belang** een passendere grondslag is.

JA Uitkomst scenario **E** uit het stroomschema van het afwegingskader is van toepassing. Zie 'Toelichting per scenario' voor het handelingsperspectief bij dit scenario.

NEE Ga verder naar [vraag 5a](#).

Vraag 5a: Is het wenselijk en haalbaar om alsnog toestemming te vragen van betrokkenen?

Toestemming is een van de zes wettelijke grondslagen die in de AVG genoemd worden. Als deze grondslag goed toegepast wordt, is dit de meest onbetwistbare basis voor verwerkingen. De betrokkenen worden namelijk actief betrokken in het besluit om gegevens te verwerken. Ook kan toestemming voorkomen dat er discussie ontstaat over een (andere) grondslag voor verwerken.

Toch zijn er veel situaties waarin het vragen om toestemming praktisch onuitvoerbaar, of niet passend bij de doelstelling is. Informatie delen kan dan alleen als een van de andere grondslagen geldig is.

Via het stroomschema van deze verstrekkingwijzer heeft u al vastgesteld dat de grondslagen 'vitale belangen', 'wettelijke verplichting' en 'overeenkomst' niet van toepassing zijn. Maar mogelijk is 'algemeen belang' of 'gerechtvaardigd belang' passender voor uw situatie dan toestemming. Dit kunt u onderzoeken door in het stroomschema bij deze vraag 'nee' te selecteren om door te gaan naar de vragen en informatie over de resterende grondslagen.

Als een andere grondslag van toepassing is, maar u meer persoonsgegevens wilt delen dan onder die grondslag (en bijbehorende doelstelling) mogelijk is, dan is het waarschijnlijk dat u voor die aanvullende gegevens alsnog toestemming moet vragen.

Houd bij het overwegen van toestemming als grondslag rekening met de vier voorwaarden voor geldigheid van de toestemming, die bij vraag 5 beschreven zijn.

Praktische overwegingen rondom de grondslag toestemming:

- Is het op basis van de hoeveelheid en categorie(ën) van betrokkenen, en de beschikbaarheid van contactgegevens, redelijkerwijs haalbaar om de toestemming te vragen?
- Wat zijn de gevolgen voor uw proces en het delen van gegevens als een deel van de betrokkenen geen toestemming geeft?
- Hoe gaat u de toestemmingsadministratie inrichten en borgen in het proces dat alleen de gegevens gedeeld worden van de personen die toestemming gegeven hebben. Denk eraan dat er bij het hanteren van toestemmingsverklaringen en een toestemmingsregistratie ook verwerking van persoonsgegevens plaatsvindt.
- Op welke manier kunnen betrokkenen hun toestemmingskeuzes beheren? (Het intrekken moet net zo eenvoudig kunnen als het geven van toestemming.)
- Hoe gaat u om met reeds gedeelde gegevens van betrokkenen, vanaf het moment dat een betrokkene de toestemming heeft ingetrokken?

Afwegingskader (stroomschema) →

Toelichting afwegingskader

Toelichting per scenario →

JA Ja, vraag toestemming. Indien toestemming is verkregen ga door naar [scenario E](#), anders naar [scenario H](#).

NEE Ga verder naar [vraag 6](#).



Vraag 6: Is het noodzakelijk om persoonsgegevens te delen om een taak van *algemeen belang of openbaar gezag* uit te oefenen?

Deze grondslag gaat over de uitvoering van publieke taken. Dat zijn **taken die in de wet zijn vastgelegd**. Hierdoor kan niet elke organisatie deze grondslag hanteren. Ook moet de verwerking van persoonsgegevens onder deze grondslag **noodzakelijk zijn voor het uitvoeren van de betreffende publieke taak**. (artikel 6 lid 1, onder e, AVG)

Noodzakelijkheid houdt in dat het doel van uw verwerking in verhouding staat tot de inbreuk op de privacy van de betrokkenen (proportionaliteit) en u het doel niet op een andere manier kunt bereiken, die minder ingrijpend is voor de betrokkenen (subsidiariteit).

 **Een voorbeeld:** Een gerechtsdeurwaarder mag op basis van artikel 2 van de Gerechtsdeurwaarderswet persoonsgegevens van een gedaagde uitwisselen met een rechtbank, naar aanleiding van een dagvaarding. Dit komt voort uit het feit dat de Staat een deel van het openbaar gezag gedelegeerd heeft aan de gerechtsdeurwaarder.

 **Een voorbeeld van wat niet mag:** Een gemeente wil in het kader van 'preventieve aanpak' persoonsgegevens bij scholen in de gemeente opvragen van leerlingen (en ouders) waarbij ongeoorloofd verzuim wordt verwacht. Ondanks dat dit bij de taak van de gemeente lijkt te passen (artikel 19 e.v. Leerplichtwet), mogen er voor dit doel door de scholen geen persoonsgegevens uitgewisseld worden met een leerplichtambtenaar. Dit is het geval omdat er feitelijk nog geen sprake is van ongeoorloofd verzuim, maar alleen van signalen of een verwachting.

 **Een ander voorbeeld van wat niet mag:** Uw publieke organisatie gebruikt cameratoezicht voor de beveiliging van een gebouw en personeel. Dit kan noodzakelijk zijn, maar deze vorm van cameratoezicht heeft niet te maken met de publieke taak van uw organisatie. Het gaat om een namelijk om een privaat belang. Hierdoor kan de grondslag algemeen belang of openbaar gezag niet gehanteerd worden.

 **Let op:** Gegevensverwerking ten behoeve van opsporing, vervolging en inlichtingen valt niet onder de AVG, maar onder de Wpg, Wjsg of Wiv.

Afwegingskader (stroomschema) 

Toelichting afwegingskader

Toelichting per scenario 

JA Ga verder naar [vraag 6a](#).

NEE Ga verder naar [vraag 7](#).



Vraag 6a: Is een **DPIA** verplicht of wenselijk?

Een data protection impact assessment (DPIA) of gegevensbeschermingseffectbeoordeling is een middel om privacyrisico's van een verwerking te inventariseren, om vervolgens te bepalen of (geplande) maatregelen die risico's tot een aanvaardbaar niveau terugdringen.

Een DPIA is verplicht als het verwerken van de gegevens waarschijnlijk tot een hoog risico voor de rechten of vrijheden van betrokkenen leidt. Dit is bijvoorbeeld van toepassing bij systematische beoordeling van persoonlijke aspecten (inclusief profiling), op grote schaal verwerken van bijzondere persoonsgegevens, verwerken van strafrechtelijke gegevens, of mensen systematisch en op grote schaal volgen in publiek gebied. De inschatting of een hoog risico van toepassing is voor betrokkenen, moet ten aanzien van de DPIA-plicht ook gemaakt worden voor het extern delen van persoonsgegevens. Dit kan zijn als onderdeel van een reeds DPIA-plichtig proces of voor het delen zelf, waar ook een DPIA-plicht uit kan voortkomen.

Houd er rekening mee dat het wijzigen van een bestaande verwerking er ook toe kan leiden dat een DPIA verplicht wordt, bijvoorbeeld als de hoeveelheid verwerkte persoonsgegevens significant toeneemt.

Zwarte lijsten zijn een voorbeeld van verwerkingen waarvoor een DPIA in de meeste gevallen noodzakelijk is. Als zwarte lijsten ook extern gedeeld worden en deze strafrechtelijke persoonsgegevens bevatten, dan moet naast het uitvoeren van de DPIA hiervoor een vergunning aangevraagd worden bij de Autoriteit Persoonsgegevens.

De Autoriteit Persoonsgegevens heeft een pagina opgesteld met een overzicht van de criteria voor de beoordeling of een DPIA uitgevoerd moet worden. Zie hiervoor www.autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment-dpia. Op deze webpagina staat ook een verwijzing naar de 'DPIA-lijst' van de AP, wat een lijst is met soorten verwerkingen waarvoor de AP een DPIA verplicht heeft gesteld.

Een DPIA moet uitgevoerd worden vóórdat de verwerking (het extern delen) gestart wordt. Start daarom al met de DPIA in de ontwerpfase van de verwerking. Bij nieuwe inzichten over het proces, de risico's en de maatregelen, kunt u de DPIA vervolgens bijstellen.

Als een DPIA niet verplicht is op basis van de voorgeschreven criteria, kan het alsnog wenselijk zijn om een DPIA uit te voeren. Een DPIA is een krachtig middel om privacyrisico's te analyseren en beheersen. Ook kan de vastlegging van een DPIA bijdragen aan interne en externe verantwoording over keuzes rondom verwerkingen. Hier staat tegenover dat een DPIA een arbeids- en tijdsintensief proces is.

Afwegingskader (stroomschema) →

Toelichting afwegingskader

Toelichting per scenario →

JA DPIA uitvoeren. [Zie toelichting.](#)

NEE Uitkomst scenario **F** uit het stroomschema van het afwegingskader is van toepassing. [Zie 'Toelichting per scenario'](#) voor het handelingsperspectief bij dit scenario.



DPIA uitvoeren: Is het restrisico acceptabel?

Als de conclusie na consultatie van de functionaris gegevensbescherming (FG) is dat delen proportioneel, noodzakelijk en in overeenstemming is met de bescherming van de rechten en vrijheden van de betrokkenen, moet gekeken worden hoe restrisico's met maatregelen kunnen worden gemitigeerd. Daarbij moet onder andere worden aangegeven hoe het recht op toegang, rectificatie, en verwijdering van gegevens door de betrokkenen is geregeld. Is aan alle voorwaarden voldaan dan kan overgegaan worden naar het volgende scenario.

DPIA uitvoeren

Voer een **DPIA** uit op de verwerking, in samenwerking met een expert. Een DPIA is maatwerk. Maak hierbij een systematische beschrijving van de verwerking van persoonsgegevens, de betrokken processen, afdelingen en (externe) partijen. Beoordeel de noodzaak (proportionaliteit en subsidia-riteit) van de verwerking. Als de verwerking (het delen) niet noodzakelijk is, mag u de verwerking niet starten of voortzetten.

Beoordeel vervolgens de mogelijke gevolgen van de verwerking voor de rechten en vrijheden van de betrokkenen. Stel de aanwezige en geplande maatregelen vast, zowel organisatorisch als technisch, en beoordeel of deze de risico's voldoende adresseren. Als uw organisatie een functionaris gegevensbescherming (FG) aangesteld heeft, bent u **verplicht de FG om advies te vragen** over de DPIA en in het DPIA-rapport dit advies en de opvolging daarvan te documenteren. Als de risico's onvoldoende gemitigeerd zijn met de maatregelen, dan moet u contact opnemen met de Autoriteit Persoonsgegevens voor een **voorafgaande raadpleging**.

Wanneer het gaat om het extern delen van 'zwarte lijsten' die strafrechtelijke gegevens bevatten, bent u verplicht om een **vergunning** bij de Autoriteit Persoonsgegevens aan te vragen voor deze verwerking.

Als de uitkomst van de DPIA is dat u de gegevens mag delen onder de grondslag rondom taken van algemeen belang of openbaar gezag, dan registreert u de gegevensuitwisseling in het verwerkingsregister of een ander documentatiesysteem, met een verwijzing naar de wettekst of regeling over de wettelijke taak die uw organisatie heeft. Documenteer daar ook bij hoe deze verwerking (het delen van de persoonsgegevens) past binnen deze taak van **algemeen belang** of **openbaar gezag**. Neem daarnaast een verwijzing op naar de uitgevoerde DPIA.

DPIA tips & tricks

Als een verwerking (het delen) van persoonsgegevens waarschijnlijk leidt tot een hoog risico voor betrokkenen, neem dan het volgende in overweging.

- De Autoriteit Persoonsgegevens heeft een pagina opgesteld met een overzicht van de criteria voor de keuze om een DPIA uit te voeren. Zie hiervoor www.autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment-dpia.
- Na de initiële keuze voor het wel of niet uitvoeren van een DPIA is het van belang om deze keuze intern te laten valideren, bijvoorbeeld door procesverantwoordelijken of inhoudelijk betrokken functionarissen. Schakel een AVG-expert in voor het uitvoeren van de DPIA, of zelfs al bij de overwegingen om een DPIA uit te voeren.
- Het kan voorkomen dat een gewijzigde verwerking DPIA-plichting wordt, bijvoorbeeld als het aantal verwerkte persoonsgegevens significant toeneemt, of een gegevenscategorie wordt toegevoegd.
- Betrek bij de uitkomsten van de DPIA ook (een vertegenwoordiging van) betrokkenen om te verifiëren dat de juiste afwegingen rondom belangen, risico's en maatregelen zijn gehanteerd.
- Als de uitkomst van een DPIA is dat de geïnventariseerde risico's voor betrokken niet tot een aanvaardbaar niveau worden teruggedrongen, dan bent u verplicht een 'voorafgaande raadpleging' bij de Autoriteit Persoonsgegevens (AP) te doen. Hiermee vraagt u feitelijk advies van de AP over de verwerking, de gerelateerde risico's en de maatregelen die daar tegenover gezet (kunnen) worden.
- Privacy management tools beschikken veelal over een DPIA-module, die u aan de hand van vragenlijsten door de stappen van een DPIA heen leidt.
- U kunt ter inspiratie bij het Centrum voor Criminaliteitspreventie en Veiligheid (het CCV) inzage vragen in een uitgevoerde DPIA, rondom het Collectief Winkelvebod.

JA Uitkomst scenario **F** uit het stroomschema van het afwegingskader is van toepassing. [Zie 'Toelichting per scenario'](#) voor het handelingsperspectief bij dit scenario.

NEE Uitkomst scenario **H** uit het stroomschema van het afwegingskader is van toepassing. [Zie 'Toelichting per scenario'](#) voor het handelingsperspectief bij dit scenario.



Vraag 7: Is het noodzakelijk om de gegevens te delen met de betreffende partij om een **gerechtvaardigd belang** van uw organisatie of een derde te behartigen?

Een **gerechtvaardigd** belang (artikel 6 lid 1, onder f, AVG) moet ergens in het recht zijn opgenomen én maatschappelijk gezien worden als een belang dat door het recht beschermd moet worden. Dit kan bijvoorbeeld een grondrecht zijn, zoals vrijheid en veiligheid, of (bescherming van) eigendom.

Betrokkenen – de personen over wie de gegevens gaan – moeten bezwaar kunnen maken tegen de verwerking, als deze grondslag van toepassing is.

Voor pure overheidstaken kan deze grondslag niet gebruikt worden. [Zie vraag 6](#) voor de behandeling van de grondslag die gerelateerd is aan publieke taken.

 **Een voorbeeld:** Een organisatie met 20 werknemers schakelt een externe partij in om de salarisadministratie en -verwerking te verzorgen. Hierbij worden de benodigde persoonsgegevens gedeeld met de externe partij. Omdat de organisatie zelf onvoldoende expertise en middelen heeft voor het voeren van de salarisadministratie, wordt met de uitbesteding de zorgplicht naar de werknemers nagekomen. Dit is een gerechtvaardigd belang. Door een passende verwerkersovereenkomst aan te gaan met de externe partij, worden de spelregels voor de verwerking vastgesteld en worden negatieve gevolgen voor de werknemers zoveel mogelijk beperkt.

 **Een ander voorbeeld:** Ondernemers in een winkelgebied kunnen deelnemen aan het Collectief Winkelverbod. Dit is een vorm van een zwarte lijst, gericht op het weren van overlastveroorzakers in winkelgebieden. De lijst wordt gedeeld tussen de deelnemende ondernemers in een winkelgebied. De gerechtvaardigde belangen zijn hier een veilig leven, het beschermen van eigendommen en het nakomen van de zorgplicht voor werknemers en klanten. Omdat deze verwerking een grote inbreuk maakt op de privacy en vrijheid van een betrokkene, ligt er ook een grote nadruk op de beoordeling van noodzakelijkheid, de belangenafwegingen en de maatregelen.

Vergelijkbare voorbeelden: Collectieve horecaontzegging, Stadionverboden en de Signaleringslijst Ongewenst Huurdersgedrag.

 **Een voorbeeld van wat niet mag:** Een stichting (Safecin) heeft in 2019 een vergunningaanvraag ingediend bij de Autoriteit Persoonsgegevens (AP) voor het beheren van een fraudehelpdesk. Met deze fraudehelpdesk zouden gegevens van 'strafrechtelijke aard' (artikel 10 AVG) ten behoeve van derden worden verwerkt. Een vergunning hiervoor mag alleen worden verstrekt als de verwerking **noodzakelijk** is met het oog op een **zwaarwegend belang van derden** en de maatregelen rondom de verwerking ervoor zorgen dat de

persoonlijke levenssfeer van de betrokkene **niet onevenredig** wordt **geschaad**. De AP heeft geen vergunning afgegeven, omdat Safecin de **noodzaak en proportionaliteit** van de verwerking onvoldoende heeft aangetoond en de **verantwoordingsplicht** onvoldoende heeft nageleefd.

Zie ook www.autoriteitpersoonsgegevens.nl/uploads/imported/besluit_vergunning_fraudehelpdesk.pdf.

JA Ga verder naar [vraag 7b](#).

NEE Uitkomst scenario **H** uit het stroomschema van het afwegingskader is van toepassing. [Zie 'Toelichting per scenario'](#) voor het handelingsperspectief bij dit scenario..



Vraag 7a: Is de verwerking (het delen) *noodzakelijk*?

Een verwerking is **noodzakelijk** als aan de volgende voorwaarden is voldaan:

Het **doel** van de verwerking moet in **verhouding** staan tot de **inbreuk** op de privacy van de betrokkenen. (proportionaliteit) Daarnaast moet vastgesteld worden of het doel niet op een andere, minder ingrijpende manier, bereikt kan worden. (subsidiariteit)

Afwegingskader (stroomschema) →

Toelichting afwegingskader

Toelichting per scenario →

JA Ga verder naar [vraag 7c](#).

NEE Uitkomst scenario **H** uit het stroomschema van het afwegingskader is van toepassing. Zie 'Toelichting per scenario' voor het handelingsperspectief bij dit scenario.

Vraag 7b: Wegen de **belangen** van de organisatie (en/of derden) zwaarder dan de belangen van de betrokkenen?

Neem hierbij alle volgende onderwerpen in acht:

- i) de **ernst van de inbreuk** op de privacy
- ii) mogelijke **gevolgen** van het delen voor de rechten en vrijheden van de betrokkenen
- iii) de **belangen** voor uw organisatie en derden
- iv) (aanvullende) **maatregelen** die de risico's kunnen beperken en
- v) of een betrokkene de verwerking min of meer kan **verwachten**.

Documenteer deze analyse en de conclusie daarvan, en betrek eventueel een vertegenwoordiging van de betrokkenen om hun visie hierop te geven.

 **Een voorbeeld rondom afweging van belangen:** Bij een winkel in overdekt winkelcentrum heeft een dief waardevolle spullen gestolen. De dief is niet aangehouden, maar de winkelier heeft camerabeelden, waarop de dief herkenbaar in beeld is. De winkelier wil een foto hiervan op het raam van zijn etalage hangen om winkelend publiek en andere ondernemers bewust te maken van de dreiging vanuit deze persoon. Daarnaast wil hij de dief, en diefstal in het algemeen, afschrikken. De winkelier vindt dat hij hiermee het belang van zijn eigen organisatie én dat van derden dient (*punt iii*), in het kader van veilig leven en bescherming van eigendommen.

Hier staat tegenover dat het openbaar plaatsen van een herkenbare foto, gerelateerd aan een strafbaar feit, een ernstige inbreuk op de privacy van de betrokkene (de dief) is. (*punt i*) Ook al kan het zo uitgelegd worden dat de betrokkene de verwerking min of meer kan verwachten (*punt v*), is het waarschijnlijk dat het delen van de foto relatief grote gevolgen heeft voor de betrokkene. (*punt ii*) Naast het punt dat de publicatie van de foto zal leiden tot reputatieschade, is het aannemelijk dat de betrokkene zijn gezicht niet meer wil laten zien in het winkelcentrum. Als de betrokkene in de buurt van het winkelcentrum woont, beperkt dit hem in zijn vrijheden.

De winkelier moet de belangen van de betrokkene afwegen tegen de belangen van zijn onderneming en van derden. Als de winkelier van oordeel is dat het belang van de betrokkene minder zwaar weegt, dan moet hij alsnog vaststellen welke (aanvullende) redelijkerwijs mogelijk zijn om de risico's voor de betrokkene te beperken. (*punt iv*)

 **Let op:** Voor dit specifieke onderwerp is al diverse documentatie online beschikbaar, bijvoorbeeld vanuit de Autoriteit Persoonsgegevens en het Centrum voor Criminaliteitspreventie en Veiligheid (onderwerp: Collectief Winkelverbod). Voor andere praktijksituaties is er mogelijk minder externe input voor de afwegingen beschikbaar. In dit soort situaties kan het daarom nuttig, of zelfs noodzakelijk, zijn om een of meer onafhankelijke personen te betrekken bij de analyses.

JA Ga verder naar [vraag 7c](#).

NEE Uitkomst scenario **H** uit het stroomschema van het afwegingskader is van toepassing. Zie 'Toelichting per scenario' voor het handelingsperspectief bij dit scenario.



Vraag 7c: Is een **DPIA** verplicht of wenselijk?

Een data protection impact assessment (DPIA) of gegevensbeschermingseffectbeoordeling is een middel om privacyrisico's van een verwerking te inventariseren, om vervolgens te bepalen of (geplande) maatregelen die risico's tot een aanvaardbaar niveau terugdringen.

Een DPIA is verplicht als het verwerken van de gegevens waarschijnlijk tot een hoog risico voor de rechten of vrijheden van betrokkenen leidt. Dit is bijvoorbeeld van toepassing bij systematische beoordeling van persoonlijke aspecten (inclusief profiling), op grote schaal verwerken van bijzondere persoonsgegevens, verwerken van strafrechtelijke gegevens, of mensen systematisch en op grote schaal volgen in publiek gebied. De inschatting of een hoog risico van toepassing is voor betrokkenen, moet ten aanzien van de DPIA-plicht ook gemaakt worden voor het extern delen van persoonsgegevens. Dit kan zijn als onderdeel van een reeds DPIA-plichtig proces of voor het delen zelf, waar ook een DPIA-plicht uit kan voortkomen.

Houd er rekening mee dat het wijzigen van een bestaande verwerking er ook toe kan leiden dat een DPIA verplicht wordt, bijvoorbeeld als de hoeveelheid verwerkte persoonsgegevens significant toeneemt.

Zwarte lijsten zijn een voorbeeld van verwerkingen waarvoor een DPIA in de meeste gevallen noodzakelijk is. Als zwarte lijsten ook extern gedeeld worden en deze strafrechtelijke persoonsgegevens bevatten, dan moet naast het uitvoeren van de DPIA hiervoor een vergunning aangevraagd worden bij de Autoriteit Persoonsgegevens.

De Autoriteit Persoonsgegevens heeft een pagina opgesteld met een overzicht van de criteria voor de beoordeling of een DPIA uitgevoerd moet worden. Zie hiervoor www.autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment-dpia. Op deze webpagina staat ook een verwijzing naar de 'DPIA-lijst' van de AP, wat een lijst is met soorten verwerkingen waarvoor de AP een DPIA verplicht heeft gesteld.

Een DPIA moet uitgevoerd worden vóórdat de verwerking (het extern delen) gestart wordt. Start daarom al met de DPIA in de ontwerpfase van de verwerking. Bij nieuwe inzichten over het proces, de risico's en de maatregelen, kunt u de DPIA vervolgens bijstellen.

Als een DPIA niet verplicht is op basis van de voorgeschreven criteria, kan het alsnog wenselijk zijn om een DPIA uit te voeren. Een DPIA is een krachtig middel om privacyrisico's te analyseren en beheersen. Ook kan de vastlegging van een DPIA bijdragen aan interne en externe verantwoording over keuzes rondom verwerkingen. Hier staat tegenover dat een DPIA een arbeids- en tijdsintensief proces is.

Afwegingskader (stroomschema) →

Toelichting afwegingskader

Toelichting per scenario →

JA DPIA uitvoeren. [Zie toelichting.](#)

NEE Uitkomst scenario **G** uit het stroomschema van het afwegingskader is van toepassing. [Zie 'Toelichting per scenario'](#) voor het handelingsperspectief bij dit scenario.



DPIA uitvoeren: Is het restrisico acceptabel?

Als de conclusie na consultatie van de functionaris gegevensbescherming (FG) is dat delen proportioneel, noodzakelijk en in overeenstemming is met de bescherming van de rechten en vrijheden van de betrokkenen, moet gekeken worden hoe restrisico's met maatregelen kunnen worden gemitigeerd. Daarbij moet onder andere worden aangegeven hoe het recht op toegang, rectificatie, en verwijdering van gegevens door de betrokkenen is geregeld. Is aan alle voorwaarden voldaan dan kan overgegaan worden naar het volgende scenario.

DPIA uitvoeren

Voer een **DPIA** uit op de verwerking, in samenwerking met een expert. Een DPIA is maatwerk. Maak hierbij een systematische beschrijving van de verwerking van persoonsgegevens, de betrokken processen, afdelingen en (externe) partijen. Beoordeel de noodzaak (proportionaliteit en subsidia-riteit) van de verwerking. Als de verwerking (het delen) niet noodzakelijk is, mag u de verwerking niet starten of voortzetten.

Beoordeel vervolgens de mogelijke gevolgen van de verwerking voor de rechten en vrijheden van de betrokkenen. Stel de aanwezige en geplande maatregelen vast, zowel organisatorisch als technisch, en beoordeel of deze de risico's voldoende adresseren. Als uw organisatie een functionaris gegevensbescherming (FG) aangesteld heeft, bent u **verplicht de FG om advies te vragen** over de DPIA en in het DPIA-rapport dit advies en de opvolging daarvan te documenteren. Als de risico's onvoldoende gemitigeerd zijn met de maatregelen, dan moet u contact opnemen met de Autoriteit Persoonsgegevens voor een **voorafgaande raadpleging**.

Wanneer het gaat om het extern delen van 'zwarte lijsten' die strafrechtelijke gegevens bevatten, bent u verplicht om een **vergunning** bij de Autoriteit Persoonsgegevens aan te vragen voor deze verwerking.

Als de uitkomst van de DPIA is dat u de gegevens mag delen onder de grondslag rondom **gerechtvaardigde belangen**, dan registreert u de gegevensuitwisseling in het verwerkingsregister of een ander documentatiesysteem, met verwijzingen naar de documentatie rondom het gerechtvaardigde belang en naar de uitgevoerde DPIA.

DPIA tips & tricks

Als een verwerking (het delen) van persoonsgegevens waarschijnlijk leidt tot een hoog risico voor betrokkenen, neem dan het volgende in overweging.

- De Autoriteit Persoonsgegevens heeft een pagina opgesteld met een overzicht van de criteria voor de keuze om een DPIA uit te voeren. Zie hiervoor www.autoriteitpersoonsgegevens.nl/themas/basis-avg/praktisch-avg/data-protection-impact-assessment-dpia.
- Na de initiële keuze voor het wel of niet uitvoeren van een DPIA is het van belang om deze keuze intern te laten valideren, bijvoorbeeld door procesverantwoordelijken of inhoudelijk betrokken functionarissen. Schakel een AVG-expert in voor het uitvoeren van de DPIA, of zelfs al bij de overwegingen om een DPIA uit te voeren.
- Het kan voorkomen dat een gewijzigde verwerking DPIA-plichting wordt, bijvoorbeeld als het aantal verwerkte persoonsgegevens significant toeneemt, of een gegevenscategorie wordt toegevoegd.
- Betrek bij de uitkomsten van de DPIA ook (een vertegenwoordiging van) betrokkenen om te verifiëren dat de juiste afwegingen rondom belangen, risico's en maatregelen zijn gehanteerd.
- Als de uitkomst van een DPIA is dat de geïnventariseerde risico's voor betrokken niet tot een aanvaardbaar niveau worden teruggedrongen, dan bent u verplicht een 'voorafgaande raadpleging' bij de Autoriteit Persoonsgegevens (AP) te doen. Hiermee vraagt u feitelijk advies van de AP over de verwerking, de gerelateerde risico's en de maatregelen die daar tegenover gezet (kunnen) worden.
- Privacy management tools beschikken veelal over een DPIA-module, die u aan de hand van vragenlijsten door de stappen van een DPIA heen leidt.
- U kunt ter inspiratie bij het Centrum voor Criminaliteitspreventie en Veiligheid (het CCV) inzage vragen in een uitgevoerde DPIA, rondom het Collectief Winkerverbod.

JA Uitkomst scenario **F** uit het stroomschema van het afwegingskader is van toepassing. [Zie 'Toelichting per scenario'](#) voor het handelingsperspectief bij dit scenario.

NEE Uitkomst scenario **H** uit het stroomschema van het afwegingskader is van toepassing. [Zie 'Toelichting per scenario'](#) voor het handelingsperspectief bij dit scenario.

Scenario's per grondslag

A. Verstrekken zonder persoonsgegevens

Omdat er geen persoonsgegevens gedeeld worden, is de AVG niet van toepassing in dit geval.

Wel kunnen er vertrouwelijkheids- of geheimhoudingsafspraken gelden binnen de organisatie of de sector, die het delen van gegevens in de weg kunnen staan. Denk bijvoorbeeld aan financiële gegevens, (andere) prestatie-gerelateerde gegevens en beveiligings-/veiligheidsgegevens. Voor deze typen gegevens is het sector- en casusafhankelijk wat, hoe, met wie en in welke vorm gedeeld mag worden. Als het gaat om gegevens van een organisatie zelf, ligt de keuze (of plicht) om gegevens te delen doorgaans bij de leiding van die organisatie. Als het gaat om gegevens van andere organisaties, is de mogelijkheid tot delen van gegevens afhankelijk van de openbaarheid van die gegevens en van geheimhoudingsafspraken.

Houd er rekening mee dat versleutelde persoonsgegevens, of op andere wijze gepseudonimiseerde gegevens, onder de AVG nog steeds als persoonsgegevens gezien worden. Pseudonimiseren is dus niet gelijk aan anonimiseren. Als het proces van het versleutelen onomkeerbaar is, doordat de (encryptie)sleutel of koppeltabel weggegooid wordt, kunnen de versleutelde gegevens wél gezien worden als anoniem.

 **Let op:** Losse gegevens(velden), die gecombineerd kunnen leiden tot de identificatie van een persoon, worden ook gezien als persoonsgegevens. Denk bijvoorbeeld aan de combinatie van een straatnaam (of postcode) en een geboortedatum. Het alleen verwijderen of versleutelen van een naam is dus niet in alle gevallen voldoende om een dataset als geanonimiseerd te bestempelen.

[Terug naar vraag 1](#)

Afwegingskader (stroomschema) 

Toelichting afwegingskader 

Toelichting per scenario

De scenario's A t/m H (handelings-perspectieven) kunnen op basis van de Algemene Verordening Gegevens-bescherming en overige uitgangspunten van toepassing zijn op het delen van gegevens. Aan deze opties ligt een stroomschema ten grondslag, dat in dit document nader uitgewerkt is in de vorm van een vragenlijst met informatievoorziening en voorbeelden per onderdeel.

A **B** **C** **D** **E** **F** **G** **H**

Scenario's per grondslag

B. Verstrekken op grond van vitale belangen

U mag gegevens delen onder de grondslag vitale belangen mits voldaan wordt aan de volgende voorwaarden.

Deze grondslag kan slechts in enkele gevallen gebruikt worden. Het gaat hier om een belang dat essentieel acuut is voor iemands leven of gezondheid. Maar het mag alleen toegepast worden als de persoon in kwestie (de betrokkene) niet om toestemming gevraagd kan worden. (artikel 6 lid 1, onder d, AVG)

Ook moet het delen van de gegevens met een externe partij noodzakelijk zijn om het vitale belang te behartigen.

Dataminimalisatie: In alle gevallen geldt dat alleen de gegevens die strikt noodzakelijk zijn om het doel te behalen, gedeeld mogen worden.

Beperkte verspreidingskring: De persoonsgegevens mogen alleen gedeeld worden met de partij die binnen de doelstelling en de bijbehorende grondslag is gedefinieerd. Als deze partij een organisatie is, is het van belang dat alleen de juiste personen de gegevens ontvangen. Vermijd dus het gebruik van 'info@'-adressen (of vergelijkbaar) als ontvanger.

Veilig delen: De gegevens moeten op een veilige manier gedeeld worden, met een beveiligingsniveau dat past bij de aard en omvang van de gegevens.

[Terug naar vraag 2a](#)

Afwegingskader (stroomschema) →

Toelichting afwegingskader →

Toelichting per scenario

De scenario's A t/m H (handelingsperspectieven) kunnen op basis van de Algemene Verordening Gegevensbescherming en overige uitgangspunten van toepassing zijn op het delen van gegevens. Aan deze opties ligt een stroomschema ten grondslag, dat in dit document nader uitgewerkt is in de vorm van een vragenlijst met informatievoorziening en voorbeelden per onderdeel.

A B C D E F G H



Scenario's per grondslag

C. Verstrekken op basis van een wettelijke verplichting

U moet gegevens delen onder de grondslag wettelijke verplichting, als het delen van de betreffende gegevens met de betreffende partij is gedefinieerd in een wet. (artikel 6 lid 1, onder c, AVG)

Registratie: Registreer de gegevensverstrekking of -uitwisseling in het verwerkingsregister of een ander documentatiesysteem, met een verwijzing naar de wettekst die van toepassing is als grondslag.

Dataminimalisatie: In alle gevallen geldt dat alleen de gegevens die strikt noodzakelijk zijn om het doel te behalen, gedeeld mogen worden.

Beperkte verspreidingskring: De persoonsgegevens mogen alleen gedeeld worden met de partij die binnen de doelstelling en de bijbehorende grondslag is gedefinieerd. Als deze partij een organisatie is, is het van belang dat alleen de juiste personen de gegevens ontvangen. Vermijd dus het gebruik van 'info@'-adressen (of vergelijkbaar) als ontvanger.

Veilig delen: De gegevens moeten op een veilige manier gedeeld worden, met een beveiligingsniveau dat past bij de aard en omvang van de gegevens. Overwegingen rondom dataminimalisatie, verspreidingskring en beveiligingsniveau (bij het delen) kunnen onderdeel zijn van een DPIA.

[Terug naar vraag 3](#)

Afwegingskader (stroomschema) →

Toelichting afwegingskader →

Toelichting per scenario

De scenario's A t/m H (handelings-perspectieven) kunnen op basis van de Algemene Verordening Gegevens-bescherming en overige uitgangspunten van toepassing zijn op het delen van gegevens. Aan deze opties ligt een stroomschema ten grondslag, dat in dit document nader uitgewerkt is in de vorm van een vragenlijst met informatievoorziening en voorbeelden per onderdeel.

A B **C** D E F G H

Scenario's per grondslag

Afwegingskader (stroomschema) →

Toelichting afwegingskader →

Toelichting per scenario

D. Verstrekking op basis van een overeenkomst met betrokkene

U moet op basis van de overeenkomst met de betrokkene - de persoon waar de gegevens over gaan - gegevens delen met de betreffende partij. (artikel 6 lid 1, onder b, AVG)

Het moet om een opdracht van de betrokkene gaan, die in de overeenkomst is opgenomen.

Een overeenkomst met een derde partij (zoals een convenant), waarin de betrokkene dus geen partij is, is **niet** geldig voor het delen van persoonsgegevens onder deze grondslag.

Als u via een overeenkomst toestemming aan de betrokkene vraagt voor het delen van de gegevens, dan valt dit niet onder deze grondslag, maar onder de grondslag 'toestemming' en moet aan de voorwaarden van die grondslag voldaan worden.

Dataminimalisatie: In alle gevallen geldt dat alleen de gegevens die strikt noodzakelijk zijn om het doel te behalen, gedeeld mogen worden.

Beperkte verspreidingskring: De persoonsgegevens mogen alleen gedeeld worden met de partij die binnen de doelstelling en de bijbehorende grondslag is gedefinieerd. Als deze partij een organisatie is, is het van belang dat alleen de juiste personen de gegevens ontvangen. Vermijd dus het gebruik van 'info@'-adressen (of vergelijkbaar) als ontvanger.

Veilig delen: De gegevens moeten op een veilige manier gedeeld worden, met een beveiligingsniveau dat past bij de aard en omvang van de gegevens. Overwegingen rondom dataminimalisatie, verspreidingskring en beveiligingsniveau (bij het delen) kunnen onderdeel zijn van een DPIA.

[Terug naar vraag 4a](#)

De scenario's A t/m H (handelings-perspectieven) kunnen op basis van de Algemene Verordening Gegevens-bescherming en overige uitgangspunten van toepassing zijn op het delen van gegevens. Aan deze opties ligt een stroomschema ten grondslag, dat in dit document nader uitgewerkt is in de vorm van een vragenlijst met informatievoorziening en voorbeelden per onderdeel.

A B C **D** E F G H



Scenario's per grondslag

Afwegingskader (stroomschema) →

Toelichting afwegingskader →

Toelichting per scenario

E. Verstrekken op basis van toestemming van de betrokkene

Als u aan alle voorwaarden van toestemming als grondslag voldoet, dan mag u op basis van de toestemming gegevens delen met de betreffende partij. (artikel 6 lid 1, onder a, AVG)

Zorg ervoor dat er een goede administratie van de toestemmingen bijgehouden wordt en dat u daadwerkelijk alleen gegevens deelt van de personen die toestemming hebben gegeven.

De vier voorwaarden:

- Vrijelijk gegeven: niet onder dwang of druk; bij geen toestemming mag de persoon niet benadeeld worden ten opzichte van personen die wél toestemming geven. Dwang of druk kan ook ontstaan in een ongelijke machtsverhouding tussen betrokkenen en een organisatie, zoals van toepassing kan zijn tussen een overheidsorganisatie en een burger, maar ook tussen werkgever en werknemer, of tussen consument en marktaanbieder.
- Geïnformeerd: het doel is duidelijk; de betrokken organisaties zijn gespecificeerd; specificatie persoonsgegevens; recht om toestemming weer in te trekken (en hoe dit kan).
- Ondubbelzinnig: een expliciete, actieve handeling van de betrokkene; geen vooraf aangevinkte vakjes.
- Specifiek: toestemming voor één doel; andere doelen en verwerkingen apart specificeren én apart toestemming voor vragen.

Voor bijzondere persoonsgegevens en gegevens van kinderen onder de 16 jaar gelden aanvullende eisen voor de toestemming.

Het intrekken van toestemming moet voor de betrokkene net zo makkelijk kunnen als het geven van de toestemming. Het is dus ook van belang om vooraf te bedenken wat de impact is van een ingetrokken toestemming. Er is dan namelijk geen grondslag meer voor de verwerking.

Registratie: Registreer de gegevensverstrekking of -uitwisseling in het verwerkingsregister of een ander documentatiesysteem, met een verwijzing naar de administratie van de toestemmingen.

Dataminimalisatie: In alle gevallen geldt dat alleen de gegevens die strikt noodzakelijk zijn om het doel te behalen, gedeeld mogen worden.

Beperkte verspreidingskring: De persoonsgegevens mogen alleen gedeeld worden met de partij die binnen de doelstelling en de bijbehorende grondslag is gedefinieerd. Als deze partij een organisatie is, is het van belang dat alleen de juiste personen de gegevens ontvangen. Vermijd dus het gebruik van 'info@'-adressen (of vergelijkbaar) als ontvanger.

Veilig delen: De gegevens moeten op een veilige manier gedeeld worden, met een beveiligingsniveau dat past bij de aard en omvang van de gegevens. Overwegingen rondom dataminimalisatie, verspreidingskring en beveiligingsniveau (bij het delen) kunnen onderdeel zijn van een DPIA.

[Terug naar vraag 5](#)

[Terug naar vraag 5a](#)

De scenario's A t/m H (handelingsperspectieven) kunnen op basis van de Algemene Verordening Gegevensbescherming en overige uitgangspunten van toepassing zijn op het delen van gegevens. Aan deze opties ligt een stroomschema ten grondslag, dat in dit document nader uitgewerkt is in de vorm van een vragenlijst met informatievoorziening en voorbeelden per onderdeel.

A B C D E F G H



Scenario's per grondslag

Afwegingskader (stroomschema) →

Toelichting afwegingskader →

Toelichting per scenario

F. Verstrekken op basis van algemeen belang of openbaar gezag

Als uw organisatie een publieke taak heeft, die wettelijk is vastgelegd, kan deze grondslag van toepassing zijn. De verwerking (het delen) van persoonsgegevens onder deze grondslag moet ook noodzakelijk zijn voor het uitvoeren van de betreffende publieke taak. (artikel 6 lid 1, onder e, AVG)

Betrokkenen – de personen over wie de gegevens gaan – moeten bezwaar kunnen maken tegen de verwerking, als deze grondslag van toepassing is.

Registratie: Registreer de gegevensuitwisseling in het verwerkingsregister of een ander documentatiesysteem, met een verwijzing naar de wettekst of regeling over de wettelijke taak die uw organisatie heeft. Documenteer daar ook bij hoe deze verwerking (het delen van de persoonsgegevens) past binnen deze taak van algemeen belang of openbaar gezag.

Dataminimalisatie: In alle gevallen geldt dat alleen de gegevens die strikt noodzakelijk zijn om het doel te behalen, gedeeld mogen worden.

Beperkte verspreidingskring: De persoonsgegevens mogen alleen gedeeld worden met de partij die binnen de doelstelling en de bijbehorende grondslag is gedefinieerd. Als deze partij een organisatie is, is het van belang dat alleen de juiste personen de gegevens ontvangen. Vermijd dus het gebruik van 'info@'-adressen (of vergelijkbaar) als ontvanger.

Veilig delen: De gegevens moeten op een veilige manier gedeeld worden, met een beveiligingsniveau dat past bij de aard en omvang van de gegevens. Overwegingen rondom dataminimalisatie, verspreidingskring en beveiligingsniveau (bij het delen) kunnen onderdeel zijn van een DPIA.

[Terug naar vraag 6a](#)
[Terug naar DPIA uitvoeren](#)

De scenario's A t/m H (handelingsperspectieven) kunnen op basis van de Algemene Verordening Gegevensbescherming en overige uitgangspunten van toepassing zijn op het delen van gegevens. Aan deze opties ligt een stroomschema ten grondslag, dat in dit document nader uitgewerkt is in de vorm van een vragenlijst met informatievoorziening en voorbeelden per onderdeel.

A B C D E **F** G H



Scenario's per grondslag

Afwegingskader (stroomschema) →

Toelichting afwegingskader →

Toelichting per scenario

G. Verstrekken op basis van gerechtvaardigd belang

Een gerechtvaardigd belang (artikel 6 lid 1, onder f, AVG) moet ergens in het recht zijn opgenomen én maatschappelijk gezien worden als een belang dat door het recht beschermd moet worden. Dit kan bijvoorbeeld een grondrecht zijn, zoals vrijheid en veiligheid, of (bescherming van) eigendom.

Betrokkenen – de personen over wie de gegevens gaan – moeten bezwaar kunnen maken tegen de verwerking, als deze grondslag van toepassing is.

Om te voldoen aan de voorwaarden voor deze grondslag, moet bepaald worden of:

- de belangen van uw organisatie (en/of derden) zwaarder dan de belangen van de betrokkenen.
- de verwerking (het delen) in verhouding staat tot de inbreuk op de privacy van betrokkenen.

Voor pure overheidstaken kan deze grondslag niet gebruikt worden. [Zie vraag 6](#) voor de behandeling van de grondslag die gerelateerd is aan publieke taken.

Registratie: Registreer de gegevensuitwisseling in het verwerkingsregister of een ander documentatiesysteem, met verwijzingen naar de documentatie van de afwegingen over noodzakelijkheid, belangen, risico's en maatregelen.

Dataminimalisatie: In alle gevallen geldt dat alleen de gegevens die strikt noodzakelijk zijn om het doel te behalen, gedeeld mogen worden.

Beperkte verspreidingskring: De persoonsgegevens mogen alleen gedeeld worden met de partij die binnen de doelstelling en de bijbehorende grondslag is gedefinieerd. Als deze partij een organisatie is, is het van belang dat alleen de juiste personen de gegevens ontvangen. Vermijd dus het gebruik van 'info@'-adressen (of vergelijkbaar) als ontvanger.

Veilig delen: De gegevens moeten op een veilige manier gedeeld worden, met een beveiligingsniveau dat past bij de aard en omvang van de gegevens. Overwegingen rondom dataminimalisatie, verspreidingskring en beveiligingsniveau (bij het delen) kunnen onderdeel zijn van een DPIA.

[Terug naar vraag 7c](#)

[Terug naar DPIA uitvoeren](#)

De scenario's A t/m H (handelingsperspectieven) kunnen op basis van de Algemene Verordening Gegevensbescherming en overige uitgangspunten van toepassing zijn op het delen van gegevens. Aan deze opties ligt een stroomschema ten grondslag, dat in dit document nader uitgewerkt is in de vorm van een vragenlijst met informatievoorziening en voorbeelden per onderdeel.

A B C D E F **G** H



Scenario's per grondslag

H. Geen grondslag voor verstrekking

U heeft geen grondslag om de persoonsgegevens te delen met de externe partij. U mag de gegevens niet delen.

In sommige gevallen kan de verwerking aangepast worden om het delen van persoonsgegevens alsnog mogelijk te maken onder een van de zes grondslagen. Denk hierbij aan:

- beperken van de verwerking, in de zin van minder gegevens-categorieën of minder betrokkenen;
- toestemming vragen voor het delen van bepaalde gegevens, voor het gedeelte dat niet onder een andere grondslag valt ([zie vraag 5 in de toelichting](#)) op het afwegingskader voor de voorwaarden);
- beperken van de verspreidingskring om de risico's voor de betrokkenen te beperken;
- aanvullende maatregelen nemen om de risico's voor de betrokkenen tot een aanvaardbaar niveau te beperken.
- In alle gevallen moet alsnog bepaald worden welke grondslag van toepassing is, en of voldaan wordt aan alle voorwaarden voor het hanteren van die grondslag. Schakel bij twijfel een AVG-expert in.

Als resterende optie kunnen de te delen gegevens alsnog geanonimiseerd worden, zodat er geen sprake meer is van persoonsgegevens. Zie scenario A voor de randvoorwaarden hiervoor.

[Terug naar vraag 5a](#)
[Terug naar vraag 6a](#)
[Terug naar vraag 7](#)
[Terug naar vraag 7a](#)

Aanvullende overweging noodzaak DPIA

Als het delen van de gegevens waarschijnlijk tot een hoog risico voor de rechten of vrijheden van betrokkenen leidt, is het uitvoeren van een Data Protection Impact Assessment (DPIA) noodzakelijk. Dit is bijvoorbeeld van toepassing bij systematische beoordeling van persoonlijke aspecten (inclusief profiling), op grote schaal verwerken van bijzondere persoonsgegevens, verwerken van strafrechtelijke gegevens, of mensen systematisch en op grote schaal volgen in publiek gebied.

De verplichting tot het uitvoeren van een **DPIA kan bij elke van de zes AVG-grondslagen van toepassing zijn**, maar komt in de praktijk het meest voor bij verwerkingen op basis van de grondslagen algemeen belang of openbaar gezag, en gerechtvaardigd belang.

Een DPIA moet voorafgaand aan de verwerking (het delen) uitgevoerd worden. In een DPIA worden de privacy-risico's van de verwerking in kaart gebracht en worden de maatregelen vastgesteld die aanwezig of nodig zijn om de risico's te verlagen naar een aanvaardbaar niveau.

Zie ook de '[DPIA tips & tricks](#)' die na de vragen 6a en 7c in het onderdeel 'Toelichting afwegingskader' zijn toegevoegd.

Afwegingskader (stroomschema) →

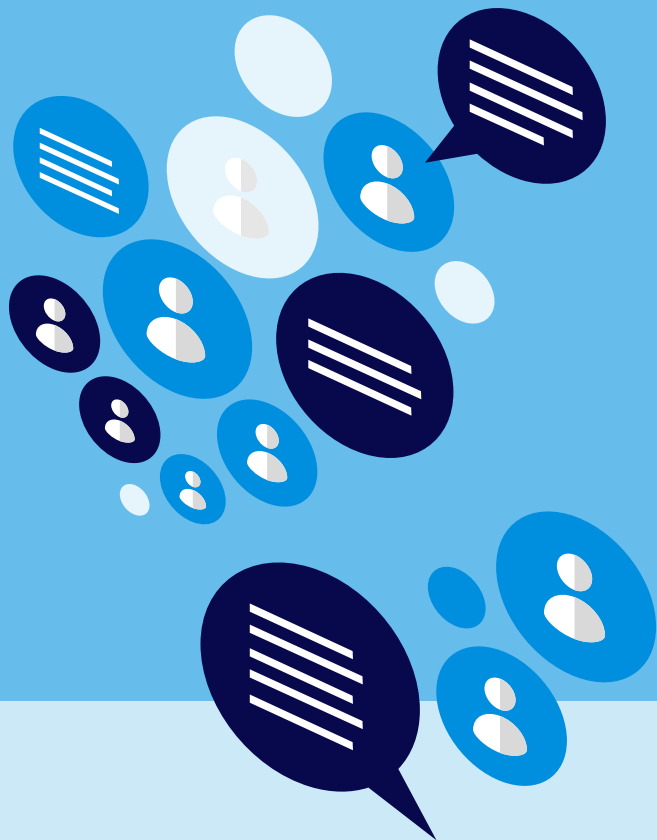
Toelichting afwegingskader →

Toelichting per scenario

De scenario's A t/m H (handelingsperspectieven) kunnen op basis van de Algemene Verordening Gegevensbescherming en overige uitgangspunten van toepassing zijn op het delen van gegevens. Aan deze opties ligt een stroomschema ten grondslag, dat in dit document nader uitgewerkt is in de vorm van een vragenlijst met informatievoorziening en voorbeelden per onderdeel.

A B C D E F G H





Disclaimer

De informatie verstrekt in de wijzer is uitsluitend bedoeld voor algemene informatiedoeleinden en mag niet worden opgevat als juridisch advies. De uitkomsten en aanbevelingen die voortkomen uit het gebruik van deze beslisboom zijn gebaseerd op de door u verstrekte gegevens en kunnen variëren afhankelijk van de specifieke omstandigheden en wetgeving die van toepassing is.

Hoewel de beslisboom zo nauwkeurig mogelijk is ontworpen, kan niet worden garanderen dat deze precies aansluit uw specifieke casus. Het is daarom raadzaam om in geval van twijfel of voor specifieke juridische vragen een gekwalificeerde juridisch adviseur te raadplegen.

De gebruiker van deze wijzer is volledig verantwoordelijk voor het gebruik van de gegenereerde informatie en de gevolgen van beslissingen die op basis daarvan worden genomen. De ontwikkelaar aanvaardt geen aansprakelijkheid voor enige schade, verlies of andere gevolgen die voortvloeien uit het gebruik van deze tool.

Door deze wijzer te gebruiken, erkent u dat u deze disclaimer hebt gelezen en begrepen, en dat u akkoord gaat met de voorwaarden van dit gebruik.

Colofon

Tekst

Het CCV in samenwerking met Donker Paard Consulting

Vormgeving

CO3, Woltera Niemeijer

Fotografie

Freepik

© het CCV, mei 2025

CCV centrum voor
criminaliteitspreventie en
veiligheid

Het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) is een onafhankelijke stichting die partijen en veiligheidsprofessionals helpt om Nederland veiliger en leefbaarder te maken.

Het CCV is een initiatief van het ministerie van Veiligheid en Justitie, het ministerie van Binnenlandse Zaken en Koninkrijksrelatie, het Verbond van Verzekeraars, werkgeversorganisatie VNO-NCW, de Vereniging van Nederlandse Gemeenten en de Raad van Korpsschefs.

Centrum voor Criminaliteitspreventie en Veiligheid

Churchillaan 11, 3527 GV Utrecht

Postbus 14069, 3508 SC Utrecht

T (030) 751 67 00

E info@hetccv.nl

I www.hetccv.nl

