

Factsheet grondslagen/ rechtsgronden (AVG)*

** De informatie in dit factsheet is gebaseerd op de nieuwe privacywet, de Algemene Verordening Gegevensbescherming*

Uw organisatie gebruikt (de juridische uitdrukking is “verwerkt”) een bepaalde “set” persoonsgegevens.

Bijvoorbeeld als werkgever voor werknemersgegevens, als websitehouder voor klantgegevens, als energieleverancier voor abonneegegegevens, of als winkeleigenaar voor camerabeelden.

Wanneer uw organisatie persoonsgegevens gebruikt dan moet uw organisatie voor ieder soort gebruik van die gegevens een “grondslag” hebben. In de AVG wordt dit “rechtsgrond” genoemd. Zo’n rechtsgrond moet er zijn voor ieder soort gebruik dat van de persoonsgegevens wordt gemaakt: zoals voor het verzamelen van de persoonsgegevens, het interne gebruik daarvan en het doorgeven van aan een externe partij (behalve [verwerkers/bewerkers](#)).

Is zo’n rechtsgrond er niet, dan mag uw organisatie de persoonsgegevens niet gebruiken.

De persoonsgegevens mogen alleen worden gebruikt als één van de volgende rechtsgronden aanwezig is:

1. Toestemming

De betrokken persoon geeft toestemming voor het gebruik van zijn of haar persoonsgegevens.

Aan het vragen van geldige toestemming zijn de volgende voorwaarden verbonden:

- ❖ De toestemming moet worden gevraagd **voordat** de persoonsgegevens worden verzameld.
- ❖ De persoon moet vooraf worden **geïnformeerd** over het gebruik van de gegevens waar de persoon toestemming voor geeft:
 - U moet de **identiteit** van uw bedrijf bekend maken.
 - U moet aangeven voor **welke** soort gebruik (**doeleinden**) de toestemming wordt gegeven. De toestemming moet worden gegeven voor **specifieke doeleinden**:

De persoon moet de toestemming geven voor **alle doeleinden** waarvoor de gegevens worden gebruikt en al het soort gebruik dat ervan wordt gemaakt.

Dus bijvoorbeeld: voor het analyseren van surfgedrag om zelf gepersonaliseerde aanbiedingen te doen, voor het doorgeven van die informatie aan derde partijen zodat zij gepersonaliseerde aanbiedingen kunnen doen.

Als uw organisatie veel persoonsgegevens gebruikt, of de persoonsgegevens voor veel verschillende doeleinden gebruikt, is het aan te raden om per doeleinde “**gelaagde**” toestemming te vragen.

Noot: Het is niet voldoende om in het algemeen te verwijzen naar de privacyverklaring en de websitebezoeker daar mee akkoord te laten gaan.

- Aan moet worden gegeven voor welke (soorten) persoonsgegevens de toestemming wordt gegeven.
- De persoon moet worden geïnformeerd over het feit dat de toestemming altijd weer kan worden **ingetrokken**.
- Als het gaat om toestemming in verband met [uitsluitend geautomatiseerde individuele besluitvorming, waaronder profiling](#), moet duidelijk informatie worden gegeven over de belangen en de gevolgen daarvan voor de persoon en in eenvoudige taal: wat de logica is achter de beslissingen.
- Als er toestemming wordt gevraagd in het kader van doorgifte naar buiten de EER ([data-export](#)) moet worden aangegeven wat de mogelijke risico's zijn van de

doorgifte naar dat derde land als daar geen passend beschermingsniveau is.

- ❖ De toestemming moet worden gegeven door middel van een **duidelijke bevestigende handeling** van de persoon.

Bijvoorbeeld het aanvinken van een checkbox op een website, het aanpassen (“aanzetten”) van settings in een account op een website, het verschuiven van een knopje op een telefoon of het zetten van een handtekening onder een formulier. Het uitblijven van een reactie of voor-aangevinkte checkboxes gelden niet als zodanig.

- ❖ De toestemming moet **vrijelijk** worden gegeven:
 - De persoon mag **niet “onder druk”** worden gezet om toestemming te geven, bijvoorbeeld door te zeggen dat alleen gebruik mag worden gemaakt van de diensten als de persoon toestemming geeft voor het gebruik van de gegevens. Gegevens die u nodig hebt voor het uitvoeren van de overeenkomst vallen hierbuiten.
 - Als de persoonsgegevens niet noodzakelijk zijn voor het uitvoeren van de overeenkomst met de persoon en uw organisatie maakt de toegankelijkheid van de dienst afhankelijk van de toestemming voor het verwerken van de persoonsgegevens, dan wordt de toestemming vermoed niet vrij te zijn gegeven.

- Wanneer de persoon in een **afhankelijke relatie** staat van uw organisatie, bijvoorbeeld werknemers, wordt in het algemeen aangenomen dat de toestemming niet vrij wordt gegeven. In de regel betekent dit dat toestemming geen geschikte rechtsgrond is voor het verwerken van gegevens van werknemers.

Alléén als het de persoon echt vrij staat om “nee” te zeggen (bijvoorbeeld: bij werknemers of hij wel of niet in een “smoelenboek” wordt opgenomen), dan kan het geldig zijn.

- ❖ Vraagt u toestemming voor het gebruik van gegevens van **kinderen** (onder 16 jaar) in een online context – of moet u dat doen omdat geen van de andere rechtsgrond en geldt?

- Dan moet u in plaats van toestemming van het kind te vragen, de toestemming vragen van de **ouders of wettelijke vertegenwoordigers (voogden)**.

Het is niet altijd mogelijk om online de leeftijd van een betrokken persoon na te gaan. Uw organisatie zal wel de nodige moeite moeten doen om te achterhalen of de persoon ouder is dan 16 en of de ouders of wettelijk vertegenwoordigers toestemming hebben gegeven. Daarbij mag uw organisatie rekening houden met de status van de technische voorzieningen op het moment dat u het vraagt.

- In de praktijk kan uw organisatie er voor kiezen om personen onder de 16 jaar helemaal geen toegang te geven tot de diensten.
- Als uw organisatie dat wel toestaat, zal moeten worden gevraagd naar de leeftijd van de persoon en om een bevestiging en verificatie dat de ouders of wettelijk vertegenwoordigers toestemming hebben gegeven.
- ❖ Als toestemming wordt gevraagd middels een **schriftelijk verklaring** die ook op andere onderwerpen ziet moet de toestemming voor het gebruik van de gegevens duidelijk worden gescheiden van die andere onderwerpen. De informatie moet worden gegeven in een begrijpelijke en makkelijke toegankelijke vorm.

Let op: Als een persoon eenmaal toestemming heeft gegeven mag hij of zij de toestemming altijd weer op een makkelijke manier intrekken. Uw organisatie moet dan voor de toekomst staken met het gebruik van de gegevens (tenzij uw organisatie, in uitzonderlijke gevallen, een beroep kan doen op een andere rechtsgrond. Dit kan dus in sommige gevallen betekenen dat toestemming niet een praktische rechtsgrond is.

Uw organisatie zal moeten kunnen **aantonen** dat de persoon toestemming heeft gegeven en dat is voldaan aan de hiervoor genoemde voorwaarden. Het is dus van belang om dit bij te houden in de (elektronische) administratie.

2. Overeenkomst.

De gegevens zijn **noodzakelijk** voor het voorbereiden of uitvoeren van een overeenkomst met de betrokken persoon.

Let op: alleen als de gegevens daadwerkelijk noodzakelijk zijn voor het voorbereiden of uitvoeren van de overeenkomst, en dus niet (behoorlijk) zonder die gegevens kan worden uitgevoerd, kan een beroep worden gedaan op deze rechtsgrond.

3. Wettelijke plicht

De persoonsgegevens zijn nodig om te voldoen aan een wettelijke plicht waar uw organisatie aan moet voldoen. Het moet gaan om een wettelijke plicht op basis van een Nederlandse of Europese wet.

4. Vitaal belang

De persoonsgegevens zijn nodig voor een “vitaal belang” van de betrokken persoon of een ander – het gaat hier om een acute medische situatie waar niet vaak sprake van zal zijn.

5. Publieke taak of algemeen belang

De persoonsgegevens zijn nodig voor het vervullen van een taak van algemeen belang of van een taak die aan de organisatie is opgedragen in het kader van de uitoefening van openbaar gezag.

6. Gerechtvaardigd belang

De persoonsgegevens zijn nodig voor het “gerechtvaardigd belang” van uw organisatie of een ander en het belang van de betrokken persoon gaat niet vóór het belang van uw organisatie of die ander.

Noot: Overheidsinstanties of -organen die persoonsgegevens verwerken voor het uitvoeren van hun taken, mogen persoonsgegevens vanaf het inwerkingtreden van de AVG niet verwerken op basis van het gerechtvaardigd belang.

Voor de meeste soorten “commercieel gebruik” zal dit de rechtsgrond zijn waar uw organisatie zich op kan beroepen.

Maar let op: uw organisatie zal altijd een afweging moeten maken tussen het belang van de organisatie om de gegevens te verzamelen en het privacybelang van de betreffende persoon.

Daarbij gelden de volgende “vuistregels”:

- Alleen als de gegevens echt **nodig** zijn voor het “gerechtvaardigd belang” van uw organisatie mag u de gegevens gebruiken. Als u ook andere gegevens kunt gebruiken die bijvoorbeeld niet herleidbaar zijn tot de persoon dan moet u die gegevens gebruiken.
- Hoe gevoeliger de gegevens, hoe zwaarder het belang van de persoon weegt. Als het om [bijzondere persoonsgegevens](#) of andere zeer gevoelige gegevens gaat dan zal het belang van de persoon in de regel zwaarder wegen dan het

gerechtvaardigd belang.

- Als uw organisatie [gegevens van kinderen](#) (personen onder de 16 jaar) gebruikt dan zal het belang van het kind sneller voorgaan dan het belang van uw organisatie.

Dit staat uitdrukkelijk in de AVG. In feite betekent dit dat, met de ingang van de AVG, de rechtsgrond voor het verwerken van gegevens van kinderen vaker toestemming zal moeten zijn.

- De **relatie** van uw organisatie ten opzichte van de persoon. Als de persoon een afhankelijkheidsrelatie heeft met uw organisatie dan zal het privacybelang van de persoon in de regel zwaarder wegen dan wanneer de persoon de vrije keuze heeft om geen relatie met uw organisatie aan te gaan.
- Als u de persoon de mogelijkheid hebt gegeven om **bezwaar** te maken tegen het gebruik van zijn persoonsgegevens en hij heeft daar geen gebruik van gemaakt, dan weegt zijn privacybelang doorgaans minder zwaar.

Let op: als het gebruik van persoonsgegevens wordt gebaseerd op de rechtsgrond van het gerechtvaardigd belang of worden verwerkt voor een publieke taak of het algemeen belang, heeft de betrokken persoon onder bepaalde omstandigheden het recht om zich tegen het gebruik van de gegevens te verzetten, o.a. wanneer de gegevens niet meer relevant zijn. Als het verzet terecht is moet uw organisatie het gebruik van de gegevens staken.

Vragen?

Het is niet altijd makkelijk om vast te stellen welke rechtsgrond geldt. Als u twijfelt, neem dan contact op met een [jurist](#), vraag naar de mogelijkheden.