Alembo

Algemene Verordening Gegevensbescherming

Outsourcen volgens de AVG

Inhoudsopgave

Inleiding

De AVG/GDPR is alweer enige tijd van toepassing. De AVG (of GDPR) heeft onder andere tot doel om privacy gerelateerde persoonlijke informatie te beschermen.

Alembo verwerkt voor veel van haar klanten persoonsgegevens die vallen onder de AVG. Uiteraard werkt Alembo volledig conform de richtlijnen beschreven in de AVG. Voor iedere opdracht waarbij privacy gerelateerde informatie wordt verwerkt, stelt Alembo een verwerkersovereenkomst op basis van het Europees standaard model op. In dit document wordt beschreven hoe Alembo privacygevoelige informatie verwerkt conform de AVG.

Bewerking wordt uitgevoerd in een land buiten de Europese Unie

Alembo voert als bewerker de werkzaamheden uit in een land buiten de Europese Unie. De werkzaamheden worden uitgevoerd in Suriname en in de zin van de AVG wordt Suriname als een derde land beschouwd.

De hoofdregel is dat een organisatie persoonsgegevens alleen mag doorgeven naar derde landen (landen buiten de EU m.u.v. de Europese Economische Ruimte; EER-landen) met een passend beschermingsniveau.

Definitie Betrokkene, Verantwoordelijke en Bewerker

In artikel 28 lid 3 AVG staan de afspraken opgenomen die in ieder geval tussen een verantwoordelijke en bewerker in een schriftelijke overeenkomst dienen te zijn vastgelegd. Alembo gebruikt modelcontracten die aansluiten bij de bepalingen van de AVG.

In wezen kent de AVG drie partijen:

1. **De Betrokkene:**
   Een natuurlijke persoon van wie de gegevens worden verwerkt.

2. **De Verantwoordelijke:**
   De partij die eindverantwoordelijk is voor de verwerking. De betrokkene mag aan de verantwoordelijke bv. opvragen welke gegevens van de betrokkene worden opgeslagen.

3. **De Bewerker:**
   Degene die namens de verantwoordelijke de gegevens bewerkt.

Beschermingsmaatregelen die Alembo heeft genomen

Als bewerker werkt Alembo op afstand en via VPN beveiligde verbindingen, vaak in de systemen en applicaties van de eindverantwoordelijke. Alembo slaat dan geen gegevens lokaal op. Is het voor de verwerking nodig dat Alembo gegevens opslaat, dan doen wij dat op servers in Nederland (bij TransIP). In wezen zijn en blijven de gegevens of in Nederland of op de systemen en applicaties van de opdrachtgever.

Het Internet maakt het daarbij eenvoudig om de gegevens te verwerken, ook al blijven de gegevens op de applicaties in Nederland. Laat onverlet dat wij een verwerkersovereenkomst conform de EU richtlijnen opstellen, waarbij de gegevens in Suriname mogen worden verwerkt.

In de verwerkersovereenkomst wordt opgenomen wat de voor de opdracht gewenste ICT- Proces- en Organisatorische maatregelen zijn.

Aanvullende ICT maatregelen:

- Logische toegangscontrole door gebruik van sterke wachtwoorden, die via een password manager encrypted worden opgeslagen.
- Gebruik van VPN verbindingen met verantwoordelijke.
- Het niet mogelijk maken om geheugendragers (memory sticks) op de werkstations aan te sluiten.
- Beveiliging van netwerkverbindingen via Secure Socket Layer (SSL) of Transport Layer Security (TLS) technologie.

Procedurele en organisatorische maatregelen:

- NDA afstemmen met de verantwoordelijke.
- Geheimhoudingsplicht opgenomen in personeelscontracten.
- Fysieke controle via bewakers en/of vingerprint scanner bij de toegang.

Deze specifieke maatregelen worden opgenomen in de bewerkersovereenkomst.

Bijlage 1: Recht van de betrokkene

Veranderingen AVG

Onder de AVG krijgen betrokkenen (mensen van wie persoonsgegevens worden verwerkt) meer en verbeterde privacy rechten. Eindverantwoordelijke dient voor zichzelf die rechten in kaart te brengen zoals beschreven op de volgende pagina's. Uit systemen moeten overzichten kunnen worden gehaald of gegevens moeten kunnen worden aangepast of verwijderd, IT systemen moeten hieraan kunnen voldoen.

Bijlage 1

Rechten Betrokkene

1

Recht van de betrokkene (omschrijving)

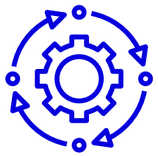
Recht op inzage in persoonsgegevens verwerking.

Wat houdt het recht in?

Als iemand verzoekt om inzage wat er over hem/haar aan persoonsgegevens wordt verwerkt, moet Verantwoordelijke in staat zijn per systeem een uitdraai aan te leveren of een overzicht aan data die worden opgeslagen in die systemen. Op het ogenblik kun je als je die informatie moet verstrekken er geld voor vragen volgens het besluit Onkostenvergoeding WBP.

Wordt dit recht nog aangepast door inwerkingtreding van de AVG?

Recht van inzage moet in principe gratis worden verstrekt, tenzij er sprake is van een verzoek om inzage dat te ver gaat of ongefundeerd is of er regelmatig inzage wordt gevraagd, dan kan nog wel een redelijke vergoeding worden gevraagd. Dit moeten wij te zijner tijd verwerken in het privacy statement. Het recht van inzage moet onder de AVG binnen 1 maand uiterlijk worden verstrekt! Om een verzoek te honoreren, moet wel eerst gecheckt worden of degene die om inzage verzoekt ook daadwerkelijk degene is die hij/zij zegt te zijn.



Wat moet er mogelijk zijn in het ICT systeem?

Een uitdraai geven van alle verwerkte persoonsgegevens van de betreffende persoon per systeem. Onder de AVG moet dit binnen een maand worden verstrekt.

Bijlage 1

Rechten Betrokkene

2

Recht van de betrokkene (omschrijving)

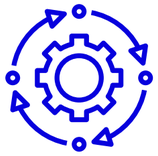
Recht op informatie

Wat houdt het recht in?

Dit betreft het recht dat een betrokkene informatie moet krijgen over de wijze van het verwerken van persoonsgegevens. Dit staat meestal uitgebreid in het privacy statement en daarom wordt het als voldoende geacht als een betrokkene daar naar verwezen wordt. Informatie die moet worden verschaft: alle gegevens van degene die verantwoordelijk is voor het verwerken van gegevens, het doel van de verwerking van de gegevens oftewel de juridische grondslag, welke soorten persoonsgegevens worden verwerkt, met welke derde de gegevens worden gedeeld, wie de persoonsgegevens ontvangt, de periode gedurende welke de gegevens bewaard blijven, de rechten van de betrokkene en hoe deze die kan uitoefenen.

Wordt dit recht nog aangepast door inwerkingtreding van de AVG?

Hieraan moet worden toegevoegd het recht dat toestemming voor verwerking kan worden ingetrokken en hoe dat kan, het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens AP (zie 5), hoe degene die verwerkt aan de persoonsgegevens is gekomen.



Wat moet er mogelijk zijn in het ICT systeem?

Dit moet in het privacy statement worden geregeld.

Rechten Betrokkene

3

Recht van de betrokkene (omschrijving)

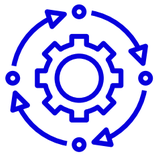
Recht op correctie van persoonsgegevens

Wat houdt het recht in?

Eenieder mag zijn/haar persoonsgegevens laten aanpassen, aanvullen of wijzigen.

Wordt dit recht nog aangepast door inwerkingtreding van de AVG?

Als de AVG in werking is getreden moet dit binnen 1 maand gebeuren, tenzij dit uit technische redenen niet mogelijk is, dan mag de termijn verlengd worden bijv. door 2 maanden te hanteren. Dit moet wel uitlegbaar zijn.



Wat moet er mogelijk zijn in het ICT systeem?

De vraag is of voldaan wordt aan de vereiste tijdsduur van de AVG (1 maand)?

Rechten Betrokkene

4

Recht van de betrokkene (omschrijving)

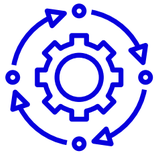
Recht op verwijdering van persoonsgegevens (ook wel bekend als “right to be forgotten”).

Wat houdt het recht in?

Onder de huidige regelgeving kan dit recht alleen worden uitgeoefend als het bewaren van die gegevens leidt tot schade en betrokkene dit kan aantonen. Dit recht is ingevoerd naar aanleiding van diverse arresten o.a. Facebook en Google.

Wordt dit recht nog aangepast door inwerkingtreding van de AVG?

Onder de AVG wordt dit recht verruimd; ieder kan vragen om gegevens te verwijderen. Maar een organisatie mag dat weigeren omdat de gegevens bijv. fiscaal bewaard moeten worden, omdat dit noodzakelijke gegevens zijn voor een juridische procedure, of omdat de organisatie de gegevens bemoedigd heeft in het kader van het maatschappelijk belang of voor statische redenen of risico management.



Wat moet er mogelijk zijn in het ICT systeem?

Is het mogelijk makkelijk gegevens te verwijderen?

Rechten Betrokkene

5

Recht van de betrokkene (omschrijving)

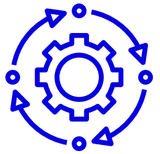
Recht op dataportabiliteit (dit is een nieuw recht dat wordt ingevoerd onder de AVG en dus pas van toepassing is per 26/5/2018).

Wat houdt het recht in?

Dit houdt in dat de Verantwoordelijke en de verwerker die voor de Verantwoordelijke verwerkt ervoor moeten zorgen dat een betrokkene diens gegevens makkelijk kan krijgen en vervolgens kan doorgeven aan een andere organisatie als deze dat wil.

Wordt dit recht nog aangepast door inwerkingtreding van de AVG?

Is een nieuw recht dat onder de AVG wordt ingevoerd.



Wat moet er mogelijk zijn in het ICT systeem?

Kunnen de gegevens makkelijk worden overgezet?

Rechten Betrokkene

6

Recht van de betrokkene (omschrijving)

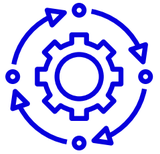
Klachtenrecht

Wat houdt het recht in?

Er moet een proces zijn om een klacht in te dienen.

Wordt dit recht nog aangepast door inwerkingtreding van de AVG?

Betrokkenen kunnen bij Autoriteit Persoonsgegevens (AP) een klacht indienen over de manier waarop de Verantwoordelijke met hun gegevens omgaat. AP is verplicht om deze klacht te behandelen. Er wordt in het privacy statement en in het klachtenreglement opgenomen dat eenieder een klacht in kan dienen bij AP over de wijze waarop de Verantwoordelijke persoonsgegevens verwerkt.



Wat moet er mogelijk zijn in het ICT systeem?

Dit moet geregeld zijn via een privacy statement en een klachtenprocedure

Rechten Betrokkene

1. De AVG stelt dat iedere instelling (verwerkingsverantwoordelijke of de verwerker (in de WBP geheten bewerker)) moet kunnen aantonen dat de instelling compliant is met de AVG. Dit betekent documentatieplicht; er moet een overzicht komen met gegevensverwerkingen als volgt:

Welk persoonsgegeven	Voor welk doel wordt dit verwerkt?	Waar komt dit vandaan?	Met wie wordt het gedeeld?	In welk systeem/systemen staat dit aangegeven?

2. Worden er gegevens verwerkt van minderjarigen? De AVG stelt dat minderjarig is of jonger dan 16 jaar of jonger dan 13 jaar, afhankelijk van welke leeftijd de EU-Lidstaat kiest en vastlegt in een nader uitvoeringsbesluit. Vooralsnog wordt in Nederland uitgegaan van jonger dan 16 jaar. In dat geval moet er toestemming zijn van de ouders. Het systeem moet dus dan kunnen lokaliseren dat er gegevens worden verwerkt van een minderjarige.

3. Privacyrisico’s moeten in kaart worden gebracht. Dit moet via een Privacy Impact Analyse (PIA). Tevens moet beoordeeld worden hoe gegevens nu beschermd worden en hoe doelmatig dat is.

4. Er moeten organisatorische en technische beveiligingsmaatregelen worden genomen om te zorgen dat persoonsgegevens veilig verwerkt worden en alleen die gegevens die noodzakelijk zijn voor het specifieke doel waarvoor verwerkt wordt (dit is het beginsel van privacy by default). Om hieraan te voldoen kan een beveiligingsprotocol worden opgesteld en er een richtlijn zijn of een beleid omtrent het bewaren van persoonsgegevens. Bij het ontwerpen van producten/diensten en systemen moet een organisatie zorgen dat persoonsgegevens goed worden beschermd (dit is het beginsel van privacy by design).

5. Als er veel verwerkingen plaatsvinden en er worden gevoelige gegevens verwerkt, moet de organisatie aan de hand van de AVG bekijken of er een data protectie officer (ook wel privacy officer ofwel functionaris gegevensbescherming) moet worden aangesteld. Deze persoon heeft gedurende 2 jaar van de uitoefening van diens functie dezelfde ontslagbescherming als een lid van de ondernemingsraad.

6. Meldplicht datalekken: wordt hieraan voldaan? Is er een proces hiervoor ingericht? Is er een proces opgesteld?

7. Bewerkersovereenkomst of Verwerkersovereenkomst; Deze moet worden opgesteld als het verwerken van data wordt uitbesteed.

8. Leidend toezichthouder: er kan een leidend toezichthouder worden aangesteld. De EU gaat mogelijk in de toekomst een European Data Board instellen.

9. Er moet voldaan worden aan bijzondere regels als persoonsgegevens worden doorgegeven aan een land dat buiten de EU is gevestigd. Zie hiervoor bijlage 2.

Bijlage 2: Doorgifte binnen en buiten de EU

Doorgifte binnen en buiten de EU

De bescherming van persoonsgegevens is niet in alle landen hetzelfde geregeld, hierdoor verschilt het beschermingsniveau per land. Binnen de Europese Unie wordt dit gereguleerd door de huidige privacy richtlijnen en vanaf 25 mei 2018 door de AVG.

Hoofdregel is thans: Persoonsgegevens doorgeven vanuit Nederland naar het buitenland is niet toegestaan, tenzij de doorgifte geschiedt aan een land dat voldoende bescherming biedt.

Deze drie landen hebben zich verplicht de Europese privacyrichtlijn te implementeren in eigen wetgeving. Zij kennen dus een gelijkwaardig niveau van bescherming van persoonsgegevens. EER-Lidstaten worden daarom gelijk behandeld als EU-Lidstaten.

Binnen de EU en de EER wordt het niveau van gegevensbescherming dus geacht gelijk te zijn, omdat de nationale wetgevingen van de EU-Lidstaten de principes volgen van de Europese privacyrichtlijn. Dit wordt straks verstevigd door de AVG.

Geeft een organisatie thans gegevens door van Nederland naar een ander land gevestigd binnen EU of EER? Dan hoeft die organisatie thans alleen te voldoen aan de algemene eisen uit de Nederlandse Wet bescherming persoonsgegevens.

Voor doorgifte van persoonsgegevens vanuit Nederland naar landen buiten de EU, zogeheten derde landen, geldt dat dit in principe niet is toegestaan. Derde landen zin dus alle landen buiten de EU, met uitzondering van de EER-landen.

De hoofdregel is dat een organisatie persoonsgegevens alleen mag doorgeven naar derde landen met een passend beschermingsniveau. Buiten die gevallen is doorgifte thans slechts toegestaan op basis van een wettelijke uitzondering (zoals een verdrag) of met een vergunning van het Ministerie van Veiligheid en Justitie, dat inmiddels vervangen is door de regel dat doorgifte bij uitzondering kan geschieden op basis van een door de Europese Commissie goedgekeurd modelcontact (standard contractual Clauses).

De AVG verandert dit doordat deze in veel meer instrumenten voorziet die het mogelijk maken om persoonsgegevens door te geven naar landen die geen passend beschermingsniveau bieden.

De AVG staat doorgifte toe op basis van:

1. Modelcontracten die zijn goedgekeurd door hetzij de Europese Commissie, hetzij de nationale toezichthouders;

2. Een adequaatheidsbesluit van de Europese Commissie. Hierin stelt de Europese Commissie dat een derde land, een gebied of zelfs een organisatie een passend beschermingsniveau biedt voor de doorgifte van persoonsgegevens. Bij het vaststellen van dit niveau kijkt de Europese Commissie o.a. naar de bescherming van mensenrechten in het land, de aanwezigheid van toezichthoudende autoriteiten (zoals de Autoriteit Persoonsgegevens) en eventuele internationale toezeggingen die het land gedaan heeft. Als een dergelijk adequaatheidsbesluit is genomen dan mag doorgifte van persoonsgegevens plaatsvinden;

3. Bindende bedrijfsvoorschriften (binding corporate rules). Hiermee moet de organisatie passende waarborgen bieden waardoor toch doorgifte kan plaatsvinden. Deze waarborgen staan opgesomd in de AVG en moeten een vergelijkbaar beschermingsniveau bewerkstelligen als de AVG eist in EU-lidstaten.

4. In aanvulling op de hierboven genoemde doorgifte instrumenten, staat de AVG nog uitzonderingen toe op grond waarvan toch doorgifte van persoonsgegevens mag plaatsvinden naar derde landen die geen passend beschermingsniveau bieden. Dit is het geval als:

   a. De betrokkene van de gegevens heeft ingestemd met doorgifte – daarbij moet de betrokkene uitdrukkelijk toestemming hebben gegeven en ingelicht zijn over de risico's die gepaard gaan met doorgifte;

   b. Doorgifte nodig is voor uitvoering van de overeenkomst die gesloten is met de betrokkene. Er moet sprake zijn van een situatie van noodzaak;

   c. Doorgifte nodig is voor de instelling, uitoefening of onderbouwing van een rechtsvordering;

   d. Doorgifte nodig is voor de bescherming van vitale belangen van betrokkene;

   e. Doorgifte geschiedt uit publieke registers.

In de gevallen a t/m e moet daarnaast voldaan zijn aan de volgende voorwaarden:

1. De doorgifte mag niet repetitief zijn;
2. Het aantal betrokkenen moet beperkt zijn;
3. De doorgifte moet nodig zijn voor gerechtvaardigde belangen van de verwerkingsverantwoordelijke die niet ondergeschikt zijn aan de belangen of rechten en vrijheden van betrokkene;
4. De verwerkingsverantwoordelijke moet alle omstandigheden in verband met de gegevensdoorgifte hebben beoordeeld en op basis daarvan passende waarborgen voor de bescherming van persoonsgegevens hebben geboden;
5. De nationale toezichthouder en betrokkenen moeten over de mogelijke doorgifte zijn geïnformeerd.

Alembo

Meer info?

www.alembo.nl

Koelmalaan 350
1812 PS Alkmaar
Unit 1.04
Nederland

Telefoon: +31 (0)72 737 00 00
E-mail: reacties@alembo.nl

Must reads:

Whitepaper overzees outsourcen

Whitepaper Virtuele Assistent