Infosheet: Algemene Verordening Gegevensbescherming (AVG)

Februari 2019

(Deze infosheet vervangt de Infosheet Wet Bescherming Persoonsgegevens - Januari 2017)

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden. In dit infosheet wordt de wetgeving naar de praktijk vertaald: Hoe vindt een lokale organisatie, die vrijwilligers inzet bij een dienst thuisadministratie, een formulierenbrigade of een inloopspreekuur, de optimale balans tussen privacybescherming en werkbare ondersteuning van hulpvragers? Welke maatregelen kunnen en moeten genomen worden om de gegevens te beschermen?

Tips voor diensten thuisadministratie:

- Verzamel en gebruik alleen noodzakelijke persoonsgegevens. Verwijder, waar mogelijk, namen en andere identificerende kenmerken uit de gegevens die worden verwerkt.
- Bespreek de bescherming van persoonsgegevens regelmatig . Creëer bewustzijn en transparantie. Zo kunnen (nieuwe) knelpunten en risico's in praktijksituaties worden beoordeeld.
- Beperk de toegang tot persoonsgegevens en verklein daarmee de kans op datalekken. Rapporteren de vrijwilligers per e-mail aan de coördinator?
- Zorg dat de bestanden (met de gegevens over hulpvragers) beveiligd zijn met een wachtwoord.

Loggen de vrijwilligers -om te rapporteren- in op een website?

- Zorg voor een adequate toegangsbeveiliging en een afdoende bescherming van de persoonsgegevens voor verdere verwerking door zoekmachines.

Investeer in moderne beveiligingstechniek om hacken te voorkomen.

- Voor beveiligingstechnologie is geld nodig. Maak de noodzaak hiervan duidelijk aan uw financiers!
- Volgens de richtlijnen van de Autoriteit Persoonsgegevens moet van verwerking van persoonsgegevens worden afgezien als het realiseren van het vereiste beveiligingsniveau niet mogelijk is.
- Evalueer regelmatig of de gekozen organisatorische en technische beveiligings-maatregelen nog afdoende zijn.

Inhoud:

1. Algemene Verordening Gegevensbescherming (AVG)

Vanaf 25 mei 2018 is de Algemene Verordening Gegevensbescherming (AVG) in werking getreden, ter vervanging van de Wet Bescherming Persoonsgegevens (WBP). De AVG bevat een aantal wijzigingen, zoals op het gebied van de gegevensverwerking. De AVG laat een frisse wind waaien op privacy gebied. Het gaat er dan met name om wat een gegevensverwerkende organisatie moet doen om ervoor te zorgen dat het de privacyregels naleeft, structureel waarborgt en daarover ook verantwoording kan afleggen.

Elke organisatie in Nederland is verplicht maatregelen te treffen voor de bescherming van persoonsgegevens. Iedere organisatie dient te weten welke persoonsgegevens worden opgeslagen en verwerkt, waarom en hoe deze gegevens worden beschermd.
De personen wiens persoonsgegevens worden verwerkt, hebben meer rechten gekregen:

- Recht op inzage: Het recht om gegevens in te zien. Als iemand daar een beroep op doet, moet de organisatie een kopie geven van alle verwerkte gegevens.
- Recht op correctie: De gegevens van de betrokkene moeten verbeterd worden als iemand onderbouwd aangeeft dat ze onjuist zijn of ze moeten aangevuld worden als ze onvolledig zijn.
- Recht op dataportabiliteit: Mensen hebben het recht om de persoonsgegevens te ontvangen die een organisatie van hen heeft**.** Ook kan men vragen om gegevens rechtstreeks over te dragen aan een andere organisatie.
- Recht op vergetelheid: Het recht op verwijdering en vergetelheid betekent dat de organisatie alles in het werk stelt om iedere koppeling naar of kopie van de gegevens te wissen.

De AVG legt de verantwoordelijkheid bij de organisatie om aan te tonen dat aan de privacyregels voldaan wordt. Door te voldoen aan de verantwoordingsplicht (accountability) levert een organisatie een belangrijke bijdrage aan de bescherming van het grondrecht van mensen op privacy.
De privacyregels dwingen een organisatie goed na te denken over hoe persoonsgegevens verwerkt en beschermd worden. Een organisatie moet bijvoorbeeld kunnen laten zien dat zij de juiste technische en organisatorische maatregelen heeft genomen om de persoonsgegevens te beveiligen.

2. Wat zijn persoonsgegevens?

Persoonsgegevens zijn alle gegevens aan de hand waarvan een persoon kan worden geïdentificeerd. Naam- en adresgegevens, emailadressen, pasfoto's, vingerafdrukken en IP-adressen. Persoonsgegevens zijn ook gegevens die een waardering geven over een persoon, bijvoorbeeld iemands IQ.
Onder verwerking van persoonsgegevens wordt verstaan elke handeling met betrekking tot die gegevens. Het raadplegen of ordenen van gegevens, maar ook het laten zien van gegevens aan een andere organisatie valt onder verwerking. Er is dus al gauw sprake van het verwerken van persoonsgegevens.

Als organisatie mag u niet zomaar persoonsgegevens verwerken. Uw organisatie moet daarvoor een wettelijke grondslag hebben. De AVG kent 6 grondslagen. Kan uw organisatie de gegevensverwerking niet baseren op minimaal één van deze grondslagen? Dan mogen er géén persoonsgegevens worden verwerkt. De 6 grondslagen zijn:
Toestemming van de betrokken persoon.
De gegevensverwerking is noodzakelijk voor de uitvoering van een overeenkomst.
De gegevensverwerking is noodzakelijk voor het nakomen van een wettelijke verplichting. De gegevensverwerking is noodzakelijk ter bescherming van de vitale belangen.
De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag.
De gegevensverwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen.

Uw organisatie is zelf verantwoordelijk om te beoordelen of uw organisatie zich voor een verwerking van persoonsgegevens kan baseren op één van de 6 grondslagen.

Persoonsgegevens die door hun aard bijzonder gevoelig zijn worden met de AVG extra beschermd. Bijzondere persoonsgegevens zijn:

- Persoonsgegevens waaruit ras of etnische afkomst blijkt.
- Persoonsgegevens waaruit politieke opvattingen blijken.
- Persoonsgegevens waaruit religieuze of levensbeschouwelijke overtuigingen blijken.
- Persoonsgegevens waaruit het lidmaatschap van een vakvereniging blijkt.
- Gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.
- Gegevens over gezondheid.
- Genetische gegevens.
- Biometrische gegevens met het oog op de unieke identificatie van een persoon.

Let op: Opslaan van een kopie van een ID bewijs met foto is niet toegestaan! Een foto wordt namelijk gezien als een persoonsgegeven waaruit ras of etnische afkomst blijkt.

De verwerking van bijzondere persoonsgegevens is verboden. Tenzij uw organisatie zich kan beroepen op een wettelijke uitzondering én op één van de grondslagen voor het verwerken van 'gewone' persoonsgegevens. Dit zal bij diensten thuisadministratie niet snel voorkomen.

3. Beveiligen van persoonsgegevens

Een organisatie heeft als verwerkingsverantwoordelijke de plicht om de juiste maatregelen te nemen om persoonsgegevens te beveiligen tegen diefstal, verlies of andere vorm van onrechtmatige verwerking. Een organisatie moet de verplichtingen uit de AVG nakomen en bovendien op elk moment kunnen laten zien dat deze verplichtingen zijn/worden nagekomen.

Wat passende maatregelen zijn is afhankelijk van de aard, omvang, context en het doel van de verwerking, de risico's voor de betrokkenen (hoe groot is de kans dat het risico bewaarheid wordt, en als dat gebeurt hoeveel nadeel heeft de betrokkene daarvan dan?), de stand van de techniek en privacyregelgeving.
Informatiebeveiligingsmaatregelen die als passend worden beoordeeld:

- De versleuteling van persoonsgegevens;
- Het vermogen om -op permanente basis- vertrouwelijkheid, integriteit, beschikbaarheid van verwerkingssystemen en diensten te garanderen;
- Het vermogen om -bij een fysiek of technisch incident- de beschikbaarheid en de toegang tot persoonsgegevens tijdig te herstellen;
- Een procedure van periodiek testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking.

3.1 Datalek

Met de AVG wordt de verplichting ingevoerd om een inbreuk in verband met persoonsgegevens of datalek te melden aan de bevoegde nationale toezichthoudende autoriteit: de Autoriteit Persoons-gegevens (AP). In bepaalde gevallen moet de inbreuk ook meegedeeld worden aan de personen op wier persoonsgegevens het betrekking heeft. Bijvoorbeeld als er sprake is van een ernstige inbreuk die leidt tot (de aanzienlijke kans dat) ernstige nadelige gevolgen intreden voor de betrokkene.

Voorbeelden van datalekken:

- Een medewerker stuurt een mail met persoonsgegevens aan een verkeerde ontvanger.
- Door een verkeerde instelling zijn vertrouwelijke klantgegevens toegankelijk voor alle bezoekers van de website.
- Een opzettelijke hacker of ontslagen medewerker neemt een kopie mee van de database met persoonsgegevens.

Elke beveiligingsinbreuk is een datalek!
Het bieden van inzicht in de aard van het lek, de mogelijke gevolgen ervan en het aanbieden van advies hoe te handelen, kan de (negatieve) consequenties voor de betrokkenen beperken.

Het is verplicht om alle datalekken te registreren met de details en welke gevolgen het datalek heeft gehad voor de organisatie en voor betrokkenen. Tevens moet worden geregistreerd welke corrigerende maatregelen zijn getroffen om herhaling te voorkomen.

4. Verantwoordingsplicht AVG

In de AVG staat een aantal verplichte maatregelen om aan de verantwoordingsplicht te voldoen. Naast de verplichte maatregelen kunnen ook extra maatregelen genomen worden.

De ***verplichte maatregelen*** die de AVG concreet noemt zijn:
Register bijhouden van verwerkingsactiviteiten (verwerkingsregister).
Register bijhouden van datalekken die zijn opgetreden.
Aantonen dat een betrokkene daadwerkelijk toestemming heeft gegeven voor gegevensverwerking.
Privacybeleid hebben.
Onderbouwen waarom en wanneer ervoor gekozen is wel/geen functionaris voor de gegevensbescherming (FG) aan te stellen. Dit is iemand die binnen de organisatie toezicht houdt op toepassing en naleving van de AVG.

Let op: Zorg dat uw organisatie aan de verantwoordingsplicht kan voldoen. Als de Autoriteit Persoonsgegevens het vraagt is een organisatie verplicht verantwoording af te leggen over de gegevensverwerking.

Er kan voor gekozen worden ***extra maatregelen*** te nemen:
Aansluiten bij een gedragscode.
Hanteren van een specifiek ICT-beveiligingsbeleid.
Verantwoording afleggen over de verwerking van persoonsgegevens in een jaarverslag of in een speciaal privacyjaarverslag.
Deze maatregelen zijn niet verplicht! Zij kunnen wel helpen om aan de toezichthouder te laten zien dat er voldaan wordt aan de eisen van de AVG.

4.1 Verwerkersovereenkomst

Als een organisatie andere partijen inschakelt om persoonsgegevens te verwerken, moet met deze partij een 'verwerkersovereenkomst' worden afgesloten. Bijvoorbeeld bij het laten uitvoeren van de personeels- en salarisadministratie of wanneer een organisatie software gebruikt waarbij persoonsgegevens in een Cloud[1] worden opgeslagen.
In de overeenkomst staat wat er met de gegevens moet gebeuren en hoe. Met een verwerkers-overeenkomst sluit een organisatie uit dat de andere partij de persoonsgegevens voor eigen doelen mag verwerken. Alleen verwerkers die voldoende garanties bieden dat zij aan de wettelijke vereisten voldoen, mogen worden ingeschakeld.

Let op: Als uw organisatie de gegevensverwerking door een ander/ verwerker laat uitvoeren, dan is uw organisatie nog steeds verantwoordelijk voor de naleving van de AVG.

Met het verstrekken van persoonsgegevens aan een andere partij, zodat die aan iemand een product of een dienst kan leveren, is die ook verwerkingsverantwoordelijke.

In de overeenkomst legt een organisatie in ieder geval het volgende vast:
Het onderwerp en de duur van de gegevensverwerking.

[1] Opslaan van bijzondere gegevens in een Cloud als 'Dropbox' of 'OneDrive' kan beter niet worden gedaan. Voor andere gegevens geldt dat de organisatie zich ervan moet vergewissen dat de verwerkers zich bevinden binnen de EER (EU met Noorwegen, IJsland en Liechtenstein).

De aard en het doel van de gegevensverwerking.
Het soort persoonsgegevens.
De categorieën van betrokkenen.
De rechten en verplichtingen van de verwerkingsverantwoordelijke.

5. Balans tussen privacybescherming en werkbare ondersteuning aan hulpvragers

5.1 Verwerkingsregister

De persoonsgegevens, waarvoor de organisatie verantwoordelijk is en die worden verwerkt, worden opgesteld en periodiek bijgehouden in een verwerkingsregister.
Kleine organisaties (MKB) dienen alle ***structurele*** verwerkingen vast te leggen. Als een organisatie ook bijzondere persoonsgegevens (zie pag.3) vastlegt moeten ***alle*** verwerkingen worden opgenomen in het register.
Een verwerkingsregister moet op verzoek van de AP worden overlegd.
Zie bijlage 1: Voorbeeld Verwerkingsregister.

5.2 Overeenkomst hulpvrager

De hulpvrager moet toestemming geven voor het verwerken van diens persoonsgegevens. De hulpvrager moet snappen waarom bepaalde gegevens nodig zijn om de ondersteuning te kunnen geven. Informeer de hulpvrager al bij het eerste contact: - wat de vrijwilliger wel en niet doet;
- welke gegevens voor de vrijwilliger en/of de coördinator en/of de organisatie voor welke doelen noodzakelijk zijn om bij te houden of te delen (en met wie);
- dat met de gegevens niet méér dan het noodzakelijke wordt gedaan, hoe lang ze worden bewaard en wat er gedaan wordt om onzorgvuldig gebruik van de gegevens te voorkomen.
Zie bijlage 2: Model Overeenkomst Hulpvrager

Uit de praktijk: hulpvrager heeft geen internet Om online formulieren in te vullen of wijzigingen door te geven is vaak internet nodig. Om (al dan niet opzettelijk) onrechtmatig gebruik van de gegevens te voorkomen, is het onwenselijk dat vrijwilligers de gegevens (al helemaal geen wachtwoorden) meenemen naar huis. Het is beter dat de vrijwilliger samen met de hulpvrager naar een plek gaat waar computer en internet beschikbaar zijn, bijvoorbeeld de openbare bibliotheek. De hulpvrager doet dan zelf de benodigde online handelingen, zo nodig met ondersteuning van de vrijwilliger.

Een andere optie is een beschikbare computer bij de organisatie te gebruiken. Vrijwilligers kunnen ook een laptop meenemen op huisbezoek. Het is veiliger om hiervoor een (leen)laptop van de organisatie te laten gebruiken, die de vrijwilliger niet voor andere doeleinden gebruikt. Na afloop van de ondersteuning (of vertrek van de vrijwilliger) worden de gegevens verwijderd (of de laptop terug gegeven). De vrijwilliger beschikt niet langer dan nodig is over de gegevens van de hulpvrager(s).

5.3 Vrijwilligersovereenkomst

De AVG bepaalt dat er organisatorische en technische maatregelen getroffen moeten worden om te voorkomen dat gegevens verloren raken of onrechtmatig worden verwerkt. Duidelijke afspraken maken met de vrijwilliger over wat deze wel en niet mag doen is een organisatorische maatregel. Deze afspraken kunnen worden vastgelegd in een vrijwilligersovereenkomst. Bij de meeste diensten thuisadministratie is de insteek dat de hulpvrager alles (zoals het invullen van gegevens op formulieren) zelf uitvoert, met ondersteuning en begeleiding van de vrijwilliger. Als de vrijwilliger handelingen voor de hulpvrager uitvoert, lijkt het risico groter dat gegevens verloren raken of niet correct worden verwerkt. In dat geval is het belangrijk te zorgen voor een daarbij passend beveiligingsniveau.

Neem in de vrijwilligersovereenkomst duidelijke afspraken op over wat de vrijwilliger wel/niet mag doen met welke gegevens over de hulpvrager en wat te doen als het vrijwilligerswerk stopt. Neem in de overeenkomst ook de verplichting tot geheimhouding op en wat de vrijwilliger zelf moet doen om een datalek te voorkomen. Beveiligingsincidenten en datalekken die (mogelijk) gevolgen hebben voor betrokkenen moeten direct gerapporteerd worden aan de coördinator. Zie bijlage 3: Model Vrijwilligersovereenkomst.

5.4 Privacyverklaring

Zet een Privacyverklaring op de website, zodat alle betrokkenen weten hoe u omgaat met privacy en bescherming persoonsgegevens en welke persoon daarvoor het aanspreekpunt is (met contactgegevens).
Zie bijlage 4: Voorbeeld Privacyverklaring voor op de website

5.5 Privacy Beleidsplan

Persoonsgegevens mogen alleen voor bepaalde en gerechtvaardigde doeleinden worden verzameld. Neem hierover een beschrijving op in het beleidsplan van de dienst thuisadministratie.
Beschrijf ook de risico's, de beveiligingsmaatregelen en verdeling van de verantwoordelijkheden met betrekking tot de beveiliging van persoonsgegevens.

In het Privacy Beleidsplan staan in ieder geval:
Wat het Privacy beleid is.

- Hoe met persoonsgegevens en het verwerkingsregister (invoeren en actueel houden) wordt omgegaan.
- Hoe de beveiliging van (persoons-)gegevens (intern en extern) geregeld is.
- De procedure bij een datalek.

Zie bijlage 5: Voorbeeld Privacy Beleidsplan

6. Bijlagen

Bijlage 1: Voorbeeld Verwerkingsregister
Bijlage 2: Model Overeenkomst Hulpvrager
Bijlage 3: Model Vrijwilligersovereenkomst
Bijlage 4: Voorbeeld Privacyverklaring voor op de website
Bijlage 5: Voorbeeld Privacy Beleidsplan

De bijlagen zijn op te vragen door een email te sturen naar info@lsta.nl

7. Bronnen

www.autoriteitpersoonsgegevens.nl
Grip op de AVG: de nieuwe privacywet voor niet-juristen, K. Versmissen, J. Terstegge en N. Krijgsman, Uitgeverij Wolters Kluwer, 2017

Met dank aan Stichting VOTA in Bodegraven-Reeuwijk voor het mogen delen van hun AVG-documenten met andere organisaties met een dienst thuisadministratie (zoals het Verwerkingsregister en hun Privacyverklaring) en voor het gebruiken van de overeenkomst met hulpvragers en hun vrijwilligersovereenkomst om op basis hiervan een voorbeeld te maken om als model te delen.