INFORMATIEBLAD PERSOONSGEGEVENS

TRAINING DIGITALE VAARDIGHEDEN
MODULE INFORMATIEBEVEILIGING EN PRIVACY

DIGIVAARDIG IN DE ZORG

INFORMATIEBLAD PERSOONSGEGEVENS

Deze lesmodule bestaat uit een Informatieblad, Opdrachtblad en Antwoordblad. Lees eerst dit Informatieblad en maak daarna de opdrachten van het Opdrachtblad. De juiste antwoorden vind je ten slotte in het Antwoordblad.

Persoonsgegevens

Sinds 25 mei 2018 zijn de regels rondom het verwerken van persoonsgegevens voor iedereen in de Europese Unie geregeld in de *Algemene Verordening Gegevensbescherming* (AVG). Met deze wet kunnen burgers hun persoonsgegevens beter beschermen.
Voor organisaties die persoonsgegevens verwerken, brengt dat nieuwe verantwoordelijkheden met zich mee. Ook voor jou als zorgverlener. In deze lesmodule leer je wat dat voor jou betekent. Wat is dataclassificatie? Hoe ga je om met verschillende persoonsgegevens en wat moet je doen als ze volgens de wet verkeerd worden gebruikt?

Gegevens en dataclassificatie

Zorginstellingen beschikken over veel en verschillende soorten (persoons)gegevens. Ze zijn daarom verplicht deze vertrouwelijke gegevens te beschermen tegen bijvoorbeeld uitlekken. Om te bepalen welke gegevens (data) organisaties in meer of mindere mate moeten beschermen, classificeren zij ze in verschillende mate van vertrouwelijkheid. Dit heet *dataclassificatie*.

In een organisatie kunnen bijvoorbeeld vier niveaus van vertrouwelijkheid van gegevens zijn:

1. *Openbaar*. Hierbij gaat het om gegevens die openbaar gebruikt mogen worden en voor iedereen toegankelijk zijn. Denk bijvoorbeeld aan informatie op een website.
2. *Bedrijfsvertrouwelijk*. Hier gaat het om gegevens die alleen voor medewerkers van een organisatie inzichtelijk zijn. Denk aan presentaties of beleidsplannen.
3. *Vertrouwelijk*. Dit betreft gevoelige informatie die alleen inzichtelijk is voor medewerkers die dit nodig hebben voor hun functie. Het uitlekken ervan kan grote schade toebrengen aan een organisatie of aan betrokken personen (cliënten of medewerkers). Denk hierbij aan (financiële) stukken die nog bewerkt moeten worden en nog niet volledig zijn, of aan cliëntdossiers.
4. *Geheim*. Deze informatie is slechts toegankelijk voor een klein aantal medewerkers van een organisatie. Het uitlekken ervan kan grote schade aanrichten. Denk hierbij bijvoorbeeld aan een lijst met potentiële kandidaten voor een directeursfunctie.

Een bijzondere categorie van data zijn persoonsgegevens. Zij vallen onder dataclassificatie-niveau 3. Omdat zorginstellingen veelvuldig persoonsgegevens *verwerken*, moeten zij hier extra verantwoordelijk mee omgaan. Zeker sinds de komst van de AVG in 2018.

WEETJE?! Met het *verwerken* van persoonsgegevens wordt bedoeld:
het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verspreiden, afschermen of uitwissen van persoonsgegevens.

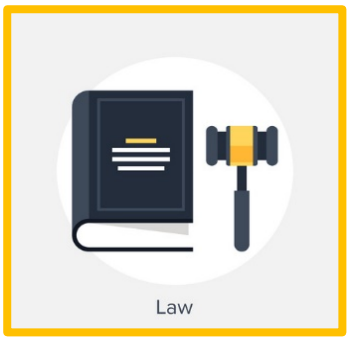
De AVG en persoonsgegevens

De *Algemene Verordening Gegevensbescherming* (AVG) is een privacywet die bescherming van persoonsgegevens van individuele burgers regelt. Een persoonsgegeven is informatie die iets over een specifiek persoon zegt óf dat in combinatie met andere gegevens herleidbaar is naar deze specifieke persoon.

Er zijn twee soorten persoonsgegevens:

1. *'Gewone' persoonsgegevens.* Dit zijn gegevens die organisaties mogen verwerken als zij voldoen aan minstens één van de zes grondslagen (zie volgende pagina).
   Denk bij 'gewone' persoonsgegevens aan gegevens als voornaam, achternaam, Burgerservicenummer (BSN), geslacht, geboortedatum, geboorteplaats, straatnaam, postcode, woonplaats, telefoonnummer en e-mailadres.
2. *Bijzondere persoonsgegevens.* Dit zijn gegevens die zó gevoelig zijn dat de verwerking ervan iemands privacy ernstig zou kunnen aantasten. Daarom mogen organisaties deze gegevens niet verwerken, tenzij daarvoor in de wet een uitzondering is én als zij voldoen aan minstens één van de zes grondslagen (zie volgende pagina). Erkende zorginstellingen voldoen aan deze wettelijke uitzondering en mogen wel *bijzondere persoonsgegevens* verwerken.
   Voorbeelden van bijzondere persoonsgegevens zijn gegevens die iets zeggen over iemands gezondheid, ras, godsdienst, politieke voorkeur, strafrechtelijk verleden of seksuele geaardheid.

De zes grondslagen van de AVG



Als organisatie mag je niet zomaar persoonsgegevens verwerken. Of het nu gaat om gewone of bijzondere persoonsgegevens, je moet daarvoor voldoen aan minstens één van de zes wettelijke grondslagen van de AVG:

1. *Je moet toestemming hebben van de betreffende persoon.*
   Bijvoorbeeld: de cliënt geeft vrijwillig toestemming aan je organisatie om persoonsgegevens met een andere zorgaanbieder te delen.

2. *Je hebt de persoonsgegevens nodig voor het sluiten van een overeenkomst.*
   Bijvoorbeeld: voor het uitvoeren van de zorgovereenkomst met cliënten of het maken van een arbeidsovereenkomst.

3. *Je hebt de persoonsgegevens nodig voor het nakomen van een wettelijke verplichting.*
   Bijvoorbeeld: de wettelijke verplichting om voor iedere cliënt een zorgdossier bij te houden.

4. *Je hebt de persoonsgegevens nodig om iemands vitale belangen te behartigen.*
   Bijvoorbeeld: wanneer de gezondheid van een cliënt acuut in gevaar is, zoals bij een cliënt met suikerziekte die buiten bewustzijn is. Het ambulancepersoneel moet daarvan dan op de hoogte zijn om passende zorg aan de cliënt te kunnen bieden.

5. *Je hebt de persoonsgegevens nodig voor het uitvoeren van een taak van algemeen belang, of voor de uitoefening van openbaar gezag.*
   Bijvoorbeeld: wanneer je een cliënt verdenkt van het verstoren van de openbare veiligheid door mishandeling.

6. *Je hebt de persoonsgegevens nodig voor de behartiging van gerechtvaardigde belangen.*
   Bijvoorbeeld: je werkgever gebruikt je privételefoon(nummer) om je familie te waarschuwen in een noodsituatie.

Persoonsgegevens en identiteitsbewijzen

Soms wil een organisatie de identiteit van een klant vast kunnen stellen. Bijvoorbeeld om fraude te voorkomen. Een organisatie kan de klant dan vragen om een identiteitsbewijs te laten zien, bijvoorbeeld een ID-kaart, een paspoort of een rijbewijs. Of de organisatie vraagt om een kopie van dat identiteitsbewijs. Maar mag dat zomaar?

Identiteitsbewijs controleren

Bij sommige organisaties zoals zorginstellingen, is legitimeren verplicht. De zorgverlener mag cliënten vragen om een identiteitsbewijs te laten zien om zo hun identiteit te kunnen controleren. Hierdoor weet je zeker dat je de juiste persoon voor je hebt en komt de juiste zorgverlening ook bij de juiste cliënt terecht.

Een zorgverlener moet in bepaalde gevallen ook het Burgerservicenummer (BSN) overnemen van het identiteitsbewijs. Met het BSN controleer je of de cliënt degene is die bij het opgegeven nummer hoort. Je noteert het BSN, het soort identiteitsbewijs en het documentnummer in de administratie. Je mag als medewerker van een zorginstelling echter nooit een kopie van een identiteitsbewijs maken!

WEETJE?! De regels omtrent het gebruiken van een BSN in de zorg staan omschreven in de *Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg*. Kijk voor meer informatie op www.rijksoverheid.nl en zoek naar 'Burgerservicenummer in de zorg' of klik hier (https://www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/burgerservicenummer-bsn/bsn-in-de-zorg).

Identiteitsbewijs kopiëren

Slechts enkele organisaties mogen een kopie van een identiteitsbewijs maken.
Dat geldt voor:

- Overheidsinstanties
- Banken
- Notarissen
- Casino's
- Werkgevers
- Levensverzekeraars

Als je zelf te maken krijgt met een organisatie die om een kopie van je identiteitsbewijs vraagt, stel die dan zo veilig mogelijk ter beschikking. Let daarbij op de volgende drie tips:

1. Schrijf in de kopie dat het een kopie is en voor welke organisatie deze is bedoeld.
2. Schrijf in de kopie op welke datum de kopie is gemaakt.
3. Maak in de kopie je pasfoto en BSN onleesbaar.

Liever meteen digitaal geregeld? Je kunt ook de app 'KopieID' van de Rijksoverheid downloaden via de appstore van je tablet of smartphone, zoals de Apple App Store, Google Play Store of Windows Phone. Hiermee maak je meteen een veilige kopie van je identiteitsbewijs.

WEETJE?! Op identiteitsbewijzen die vanaf 2014 zijn uitgegeven, staat het BSN op de achterkant. Meestal is alleen een kopie van de voorkant van het identiteitsbewijs voldoende om aan te leveren. Je BSN is daarmee dus veiliggesteld!

Persoonsgegevens en een datalek

Wanneer je in je werk persoonsgegevens gebruikt, bestaat er een kans dat gegevens worden vernietigd, gewijzigd of vrijkomen zonder dat dat de bedoeling is. Als persoonsgegevens opzettelijk of onopzettelijk worden vernietigd, gewijzigd of in handen komen van onbevoegden, wordt dat een *datalek* genoemd.

Je kunt twee dataleksoorten onderscheiden:

1. *Online datalek*. Hierbij gaat het om het lekken van digitale informatie en gegevens. Bijvoorbeeld door:
   - Verlies van je mobiele apparaat van je werkgever (laptop, telefoon, tablet, USB-stick).
   - Een hack. Je mobiele apparaat is dan gekraakt.
   - Persoonsgegevens naar onbevoegden te sturen.
   - Besmetting met een virus (ransomware).
   - Geen back-up te hebben bij technisch falen of een onherstelbaar defect van apparatuur.

2. *Offline datalek*. Denk aan papieren persoonsgegevens via dossiers in je werktas die je kwijtraakt, de documenten die open en bloot op je bureau liggen of de printjes die je eigenlijk niet bij oud papier had moeten gooien.

Datalek en meldplicht

Organisaties moeten zelf maatregelen treffen om datalekken te voorkomen. Voor een individu kan een datalek ten slotte flinke nadelige gevolgen hebben. Denk bijvoorbeeld aan zorgdossiers waarin persoonlijke informatie staat van een cliënt over zijn behandeling. Het gevolg kan stigmatisering (vooroordelen of misvattingen over cliënten) zijn. Daarnaast zijn verschillende organisaties - waaronder ook zorginstellingen - verplicht een Functionaris Gegevensbescherming (FG) aan te stellen. De FG is iemand die binnen de organisatie toezicht houdt op de toepassing en naleving van de AVG.

Wanneer sprake is van een ernstig datalek waarbij bijzondere persoonsgegevens, of zeer gevoelige informatie (zoals inloggegevens) worden gelekt, heb je als organisatie een meldplicht. Het datalek moet zonder onnodige vertraging en binnen 72 uur na de ontdekking, worden gemeld aan de Autoriteit Persoonsgegevens. In een aantal gevallen moet het datalek ook gemeld worden aan de betrokkenen. De FG is degene die de ernst van een datalek beoordeelt en indien nodig meldt. Als een datalek ten onrechte niet bij de Autoriteit Persoonsgegevens wordt gemeld, kan je organisatie een flinke boete krijgen.

Informatiebeveiliging

In de zorg werk je vaak samen met andere organisaties en soms moet je gevoelige informatie of persoonsgegevens delen. Wanneer je hebt vastgesteld of je de data mag delen met de andere partij is het belangrijk de data goed te *beveiligen* tijdens het uitwisselen. Een BSN nummer van een cliënt kan je niet zomaar via de email naar een ander versturen.

Zivver en *Zorgmail* zijn veel gebruikte programma's in de zorgsector om vertrouwelijke persoonsgegevens beveilig te versturen. De privacy gevoelige informatie wordt *versleuteld* verstuurd zodat je er zeker van bent dat alleen de juiste persoon bij de gegevens kan.

WEETJE?! In 2019 werden er in Nederland 27.000 datalekken gemeld. Maar 3% van de datalekken kwam door *hacking, phising* of een *computervirus*. De meeste data lekte uit doordat medewerkers informatie onbeveiligd met elkaar uitwisselden.
Bron: Zivver

Wat kun je zelf doen?

Organisaties zijn verplicht maatregelen te nemen tegen datalekken. Maar wat kun jij eigenlijk zelf doen? Lees de volgende negen tips:

1. Gebruik sterke wachtwoorden voor digitale diensten en wijzig ze regelmatig.
2. Klik niet zomaar op bijlagen in verdachte e-mails.
3. Ga zorgvuldig om met clouddiensten en USB-sticks.
4. Deel geen onbeveiligde maar privacygevoelige informatie; niet online maar ook niet in openbare gelegenheden zoals bijvoorbeeld tijdens een gesprek in de treincoupé met een collega.
5. Gooi privacygevoelige documenten niet bij het oud papier maar in de papierversnipperaar.
6. Als het kan binnen je organisatie: stel 'beveiligd printen' in. Hiermee moet je je aanmelden bij de printer voordat je printopdracht wordt uitgevoerd. Je voorkomt hiermee dat jouw printje door iemand anders wordt meegenomen.
7. Ruim papier met persoonsgegevens goed op: uit het zicht of beter nog, achter slot.
8. Bewaar digitale documenten zodanig dat ze alleen leesbaar zijn voor mensen die toegang moeten hebben tot de documenten.
9. Verspreid zo min mogelijk per mail en schoon je mailbox regelmatig op: ook de verzonden items en de prullenbak! Wat er niet is, kan ook niet lekken.

Tip: Meer informatie over hoe je veilig om kan gaan met persoonsgegevens vind je in de lesmodule Veiligheid.

Je weet nu wat dataclassificatie is, wat de AVG inhoudt, hoe je met verschillende persoonsgegevens om moet gaan en wat je moet doen als ze volgens de wet verkeerd worden gebruikt. Je bent klaar om het Opdrachtblad te maken van de lesmodule Persoonsgegevens.

Bronnen:

- www.rijksoverheid.nl
- www.autoriteitpersoonsgegevens.nl
- www.nos.nl
- www.fundaments.nl
- www.privacy-web.nl

Deze module is gemaakt door De Nova Learning in opdracht van 's Heeren Loo en bewerkt door Jongleert in opdracht van Utrechtzorg.

Heb je opmerkingen of vragen over deze module? Mail dan naar info@digivaardigindezorg.nl

TRAINING DIGITALE VAARDIGHEDEN
MODULE INFORMATIEBEVEILIGING EN PRIVACY

DIGIVAARDIG IN DE ZORG