FACTSHEET: PERSOONSGEGEVENS

In deze factsheet voor de training ‘Persoonsgegevens’ vind je alle relevante informatie over wat gewone en bijzondere persoonsgegevens zijn, hoe je hiermee omgaat met persoonsgegevens en identiteitsbewijzen, en over hoe je moet handelen bij een datalek.

Persoonsgegevens en bijzondere persoonsgegevens

Vanaf 25 mei 2018 zijn de regels rondom het verzamelen en verwerken van persoonsgegevens voor iedereen op een gelijke manier geregeld in de Algemene Verordening Gegevensbescherming (AVG).

Wat zijn (bijzondere) persoonsgegevens?

In de AVG is opgenomen wat persoonsgegevens zijn. Een persoonsgegeven is alles wat in verband gebracht kan worden met een persoon. Denk bijvoorbeeld aan naam, adres of e-mailadres.
Sommige gegevens worden *bijzondere* persoonsgegevens genoemd. Een bijzonder persoonsgegeven is erg gevoelige informatie over een persoon. Hierbij kun je denken aan gegevens over de gezondheid, het Burgerservicenummer (BSN), lidmaatschap van een vakvereniging, godsdienst of seksuele geaardheid van een persoon.

Bron: www.privacy-web.nl

Verdieping!
De wettelijke omschrijving van persoonsgegevens is vrij lastig te begrijpen, maar goed om toch eens door te lezen. Deze luidt als volgt:
“Alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (“de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.”
Bron: Artikel 4, Algemene Vordering Gegevensbescherming.

Vergelijk deze definitie eens met de uitleg in de factsheet!

Het verwerken van (bijzondere) persoonsgegevens

Het gebruiken van *persoonsgegevens* is aan strenge regels verbonden. Met het gebruiken van persoonsgegevens kan worden bedoeld het: opslaan, bewerken, aanvullen, delen met onbevoegden of printen van persoonsgegevens.

Je mag persoonsgegevens alleen gebruiken voor het doel waarvoor je ze hebt gekregen. Daarnaast moet je een grond hebben om de persoonsgegevens te gebruiken. Deze zes gronden staan in de AVG. Je moet aan één van deze gronden voldoen. Deze gronden zijn:

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 uitvoeren of sluiten van een overeenkomst.
   Bijvoorbeeld: voor het uitvoeren van de zorgovereenkomst met cliënten of het maken van een arbeidsovereenkomst.

Tip:
Ga op het internet naar de volgende site https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-nieuwe-europese-privacywetgeving/mag-u-persoonsgegevens-verwerken.
Hier kun je meer informatie vinden over de zes gronden van de AVG.

Klik vervolgens op: 'Wanneer mag u bijzondere gegevens verwerken?' voor de tien wettelijke uitzonderingen van de AVG.
Lees de tien wettelijke uitzonderingen goed door.

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 dan van de suikerziekte 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, zoals kindermishandeling.

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.


Law

Ben je werkzaam bij 's Heeren Loo? Dan wordt in je werk gesproken over vijf gronden. Dit komt doordat grond 5: 'De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of uitoefening van openbaar gezag', bij 's Heeren Loo nooit van toepassing is.

Het gebruiken van *bijzondere persoonsgegevens* is verboden. Tenzij er wordt voldaan aan één van de zes bovenstaande gronden én aan één van de tien wettelijke uitzonderingen. Binnen de zorg wordt meestal aan een wettelijke uitzondering voldaan, namelijk: 'De verwerking is noodzakelijk voor doeleinden van preventieve of (arbeids)geneeskunde aard, zoals het beoordelen van arbeidsgeschiktheid en/of het verstrekken van gezondheidszorg'. Hierdoor gelden bij een zorginstelling dezelfde eisen voor het gebruiken van gewone en bijzondere persoonsgegevens. Meer uitleg over de andere negen wettelijke uitzonderingen, kun je vinden via de tip hieronder.

Verdieping!
Er zijn meer wetten in Nederland die van toepassing zijn op het verwerken van persoonsgegevens in de zorg, bijvoorbeeld:

- Wet op de Geneeskundige Behandelingsovereenkomst (WGBO), voor meer informatie zie: http://wetten.overheid.nl/BWBR0005290/2018-02-01#Boek7_Titeldeel7_Afdeling5.

Identiteitsbewijzen

Welke organisaties mogen een kopie van een ID-kaart, paspoort of rijbewijs vragen?

Er zijn twee manieren waarop organisaties je identiteit kunnen controleren. Dit gebeurt door te vragen om:

1. je identiteitsbewijs te laten zien (identificeren of legitimeren), of
2. door een kopie te (laten) maken van je identiteitsbewijs.

Deze twee manieren worden hieronder toegelicht.

Je identiteitsbewijs laten zien

Bij sommige organisaties, zoals een zorginstelling, is legitimeren verplicht. Cliënten of patiënten worden gevraagd om een identiteitsbewijs te laten zien om hun identiteit te controleren. Hierdoor weet je zeker of de persoon is wie hij zegt dat hij is. Ander voorbeeld van een organisatie die kan vragen je te legitimeren is de gemeente wanneer je een nieuw identiteitsbewijs aanvraagt.

Een zorginstelling moet naast het controleren van de identiteit van een persoon die in zorg komt, in bepaalde gevallen het BSN ook overnemen van het identiteitsbewijs en gebruiken. Met het BSN controleer je of de cliënt degene is die bij het opgegeven nummer hoort. Je noteert het BSN, soort identiteitsbewijs en documentnummer in de administratie. Je mag als medewerker van een zorginstelling geen kopie maken!

Verdieping!
De regels omtrent het gebruiken van een BSN in de zorg staan in de Wet gebruik BSN in de zorg (wbsn-z), voor meer informatie zie: www.rijksoverheid.nl/onderwerpen/privacy-en-persoonsgegevens/burgerservicenummer-bsn/bsn-in-de-zorg.

Het (laten) maken van een kopie

Je mag alleen in bijzondere gevallen om een kopie van een ID-kaart, paspoort of rijbewijs vragen. Voor sommige organisaties is het bijvoorbeeld verplicht om een kopie van een identiteitsbewijs te vragen. Hiermee kunnen ze bewijzen dat ze aan de identificatieplicht hebben voldaan.

De organisaties die verplicht kunnen zijn om een kopie van een identiteitsbewijs te vragen, zijn:

- Overheden
- Financiële instellingen
- Politie, toezichthouder of conducteur
- Je eigen werkgever
- Holland Casino

Hoe stel je een kopie van een ID-kaart, paspoort of rijbewijs zo veilig mogelijk ter beschikking?

Soms wordt er om een kopie van je identiteitsbewijs gevraagd, terwijl dit niet volgens de wet is vastgesteld.

Maak dan je kopie veilig! Hiernaast zie een voorbeeld ven een veilige kopie.

Je maakt een veilige kopie door je BSN en pasfoto af te schermen op je identiteitsbewijs (zie nr. 3). Let op: Je BSN staat ook onderaan het identiteitsbewijs!

Bron: www.rijksoverheid.nl

Je maakt je kopie nog veiliger door er ook groot op te schrijven dat het om een kopie gaat en voor wie het bedoeld is (zie nr. 1). Daarnaast door aan te geven op welke datum de kopie is gemaakt (zie nr. 2).

Er is ook een app 'KopieID' van de Rijksoverheid te downloaden via de appstore van je tablet of smartphone, zoals de Apple App Store, Google Play Store of Windows Phone. Hiermee maak je een veilige kopie van je identiteitsbewijs.

Tip: Op de nieuwste rijbewijzen staat het BSN op de achterkant van het rijbewijs. Vaak hoef je alleen een kopie van de voorkant van het identiteitsbewijs aan te leveren. Kies daarom voor het aanleveren van je rijbewijs om zeker te zijn dat het BSN veilig is.

Organisaties moeten goed nadenken over het doel van het opvragen van een kopie van het identiteitsbewijs. Zo min mogelijk, maar zo veel als nodig, is het motto. Het kan zijn dat je via een andere weg minder of geen persoonsgegevens hoeft op te vragen. Twijfel je bij het opvragen van persoonsgegevens, overleg dan altijd even met je leidinggevende.

Persoonsgegevens bij onbevoegden

Wanneer je in je werk persoonsgegevens gebruikt, bestaat er een kans dat gegevens op straat komen te liggen. Dit wordt een *datalek* genoemd. Het kan zo zijn dat persoonsgegevens verkeerd worden gebruikt. De betreffende persoon kan hier last van hebben.

Wat is een datalek?

Je hebt te maken met een *datalek* als onbevoegden toegang hebben tot je persoonsgegevens. En daarnaast je persoonsgegevens worden vernietigd, gewijzigd of vrijkomen zonder dat dit de bedoeling is. Wanneer onbevoegden toegang hebben tot persoonsgegevens, wordt dit een incident genoemd. In dit geval wordt hiermee een gebeurtenis in de zorg bedoeld, waarbij iets is misgelopen met digitale gegevens of ICT. Je kunt twee soorten datalek onderscheiden: een online en offline datalek.

Online datalek

Bij een *online datalek* gaat het om het lekken van digitale informatie en gegevens. Voorbeelden waarin sprake kan zijn van een online datalek, zijn:

- Je computer wordt gehackt
- Je bent je USB-stick kwijtgeraakt
- Je laptop is gestolen
- Je heb je persoonsgegevens naar een onjuist e-mailadres verzonden
- Er is een brand in het datacentrum, terwijl er geen back-up beschikbaar is.

Bron: www.fundaments.nl

Tip:
Vind je het nog lastig om je een beeld te vormen van wat een online datalek is?
Recentelijk is er veel in het nieuws over een online datalek.
Typ bij Google ‘datalek’ in en lees enkele nieuwberichten hierover.
Kijk bijvoorbeeld naar het artikel op nos.nl ‘Erasmus MC schendt privacy van jonge patiënten’ door te klikken op de volgende link: https://nos.nl/artikel/2223353-erasmus-mc-schendt-privacy-van-jonge-patienten.html

Offline datalek

Denk je bij een datalek direct aan digitale gegevens? Dat hoeft niet altijd zo te zijn. Denk bijvoorbeeld aan de dossiers in je werktas die je kwijtraakt, de documenten die open en bloot voor iedere bezoeker op je bureau liggen of de printjes die je eigenlijk niet zomaar in de papierpak naast de printer had moeten gooien. Je noemt dit een *offline datalek*.

Ernstig datalek en meldplicht

Wanneer sprake is van een *ernstig datalek*, moet dit 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.

Bron: www.autoriteitpersoonsgegevens.nl

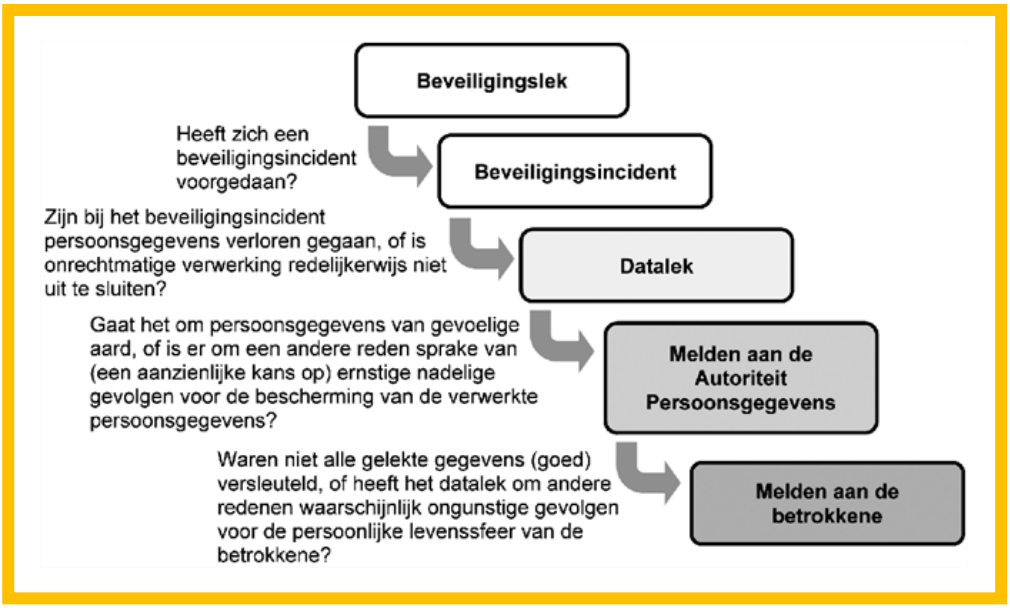
Onder een ernstig datalek wordt het lekken van bijzondere persoonsgegevens, of zeer gevoelige informatie (zoals inloggegevens) verstaan. Daarnaast ligt het aan het aantal betrokkenen die de dupe zijn van een datalek. Het is dus erg lastig om te beoordelen of er sprake is van een ernstige datalek. Hiervoor is mogelijk een Functionaris Gegevensbescherming (FG) in je organisatie aangesteld.

Als medewerker meld je een mogelijk datalek niet direct bij de Autoriteit Persoonsgegevens, maar aan je leidinggevende of aan de FG. In de zorg wordt er verplicht een FG binnen de organisatie aangewezen. Dit is omdat er op grote schaal bijzondere persoonsgegevens worden verwerkt. Als medewerker meld je een datalek *altijd* bij deze persoon. Je volgt hierbij de procedure ‘melden van een datalek’ van je organisatie. Als binnen je organisatie een datalek ten onrechte niet bij de Autoriteit Persoonsgegevens wordt gemeld, dan kan de Autoriteit Persoonsgegevens je organisatie een flinke boete geven.

Sommige organisaties hebben een FG, andere niet.
Ben je werkzaam bij ’s Heeren Loo?
‘s Heeren Loo heeft als grote zorgaanbieder een FG aangesteld. De FG is degene die datalekken meldt bij de Autoriteit Persoonsgegevens. Dit doe je dus niet zelf! Daarnaast heeft ’s Heeren Loo een procedure rondom datalekken op het medewerkersportaal staan. Hierin staat dat je contact dient op te nemen met de Service Desk als je een datalek vermoedt. Neem de procedure ‘Melden Datalekken’ uitgebreid door!

Belangrijk om te weten is dat je niet zelf de ernst van het datalek moet beoordelen. Dit is altijd aan de FG. Ieder datalek is een incident, maar niet ieder incident is een datalek.
Zet de melding van je datalek dus gelijk door.

Bij het melden van een datalek aan een FG, maakt hij/zij de afweging of het datalek wordt gemeld bij de Autoriteit Persoonsgegevens. Deze afwegingen worden weergeven in het schema hieronder.



Bron: www.wetten.overheid.nl

Wees open over voorvallen waarin sprake is van een datalek. Je kunt met je team en organisatie hiervan leren, om dergelijke voorvallen in de toekomst te voorkomen. Denk dus niet alleen aan je persoonlijke belangen, maar ook aan de belangen van je organisatie en cliënten.

Gevolgen van een datalek

Voor de personen van wie de gegevens gelekt zijn, kan een datalek 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) van deze cliënt zijn. De AVG moet eraan bijdragen, dat organisaties de door hen gebruikte persoonsgegevens nog beter beveiligen. Zo wordt het risico op een datalek verkleind.

Bronnen:

- www.rijksoverheid.nl
- www.wetten.overheid.nl
- www.autoriteitpersoonsgegevens.nl
- www.nos.nl
- www.fundaments.nl