ANTWOORDBLAD:

TRAINING PERSOONSGEGEVENS

ANTWOORDBLAD: TRAINING PERSOONSGEGEVENS

Hieronder vind je de antwoorden op de veertien opdrachten van de training ‘Persoonsgegevens’. Controleer of je de goede antwoorden hebt gegeven!

Antwoord: Opdracht 1

In de tabel hieronder vind je voorbeelden van gewone en bijzondere persoonsgegevens.

Voorbeelden van gewone persoonsgegevens	Voorbeelden van bijzondere persoonsgegevens zijn:
Naam Adres Telefoonnummer E-mailadres Postcode Huisnummer Mobiel telefoonnummer	(Ras) of etnische afkomst (Religieuze of) levensbeschouwelijke overtuiging Politieke opvatting Gezondheid Lidmaatschap van een vakvereniging Seksueel gedrag of seksuele geaardheid Genetische informatie Biometrische informatie BSN

Antwoord: Opdracht 2

In het voorbeeld van de zorgverzekering worden gewone persoonsgegevens opgevraagd.

Antwoord: Opdracht 3

Deze opdracht heeft betrekking op je eigen werkzaamheden binnen je organisatie. Kijk nog eens naar je antwoord en vergelijk dit met je antwoord bij opdracht 1.

Antwoord: Opdracht 4

a. In deze opdracht wordt gevraagd naar *gewone* persoonsgegevens.
b. Er zijn zes gronden waaraan je tenminste moet voldoen om deze *gewone* persoonsgegevens volgens de wet te mogen gebruiken. Kijk of je er tenminste twee van hebt genoemd:

1. *Toestemming van de betreffende persoon.*
2. *Je hebt de persoonsgegevens nodig voor het uitvoeren of sluiten van een overeenkomst.*
3. Je hebt de persoonsgegevens nodig voor het nakomen van een wettelijke verplichting.
4. Je hebt de persoonsgegevens nodig om iemand vitale belangen te behartigen.

5. Je hebt de persoonsgegevens nodig voor het uitvoeren van een taak van algemeen belang, of voor de uitoefening van openbaar gezag.

6. Je hebt de persoonsgegevens nodig voor de behartiging van gerechtvaardigde belangen.

In het voorbeeld van opdracht 4 zijn grond 1 en 2 het meest van toepassing.
Je moet de cliënt om toestemming vragen voor het gebruiken van zijn persoonsgegevens. Daarnaast heb je deze gegevens nodig voor het uitvoeren van de zorgovereenkomst tussen de cliënt en je organisatie.

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' nooit van toepassing is.

Voor het verwerken van de *bijzondere* persoonsgegevens moet er daarnaast ook aan minstens één van de onderstaande uitzonderingen worden voldaan:

1. Iemand heeft uitdrukkelijk toestemming gegeven voor de verwerking van zijn/haar persoonsgegevens voor één of meer specifieke doelen.

2. De verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van u of de betrokken persoon. Dit op het gebied van het arbeidsrecht en het sociale zekerheids- en sociale beschermingsrecht.

3. De verwerking is noodzakelijk ter bescherming van de vitale belangen van de betrokken persoon of van een andere natuurlijke persoon. Dit geldt alleen wanneer diegene fysiek of juridisch niet in staat is om zijn toestemming te geven.

4. De verwerking wordt gedaan door een stichting, een vereniging of een andere instantie zonder winstoogmerk die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is. En die organisatie verwerkt gegevens in het kader van gerechtvaardigde activiteiten en met passende waarborgen.

5. De verwerking heeft betrekking op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt.

6. De verwerking is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering. Of wanneer gerechten handelen in het kader van hun rechtsbevoegdheid.

7. De verwerking is noodzakelijk vanwege een zwaarwegend algemeen belang.

8. *De verwerking is noodzakelijk voor doeleinden van preventieve of (arbeids)geneeskunde aard. Zoals het beoordelen van arbeidsgeschiktheid en/of het verstrekken van gezondheidszorg.*

9. De verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid.

10. De verwerking noodzakelijk is met het oog op de archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

Uitzonderingen 2, 7, 8, 9 en 10 zijn alleen in te roepen als daarvoor in de nationale wet een rechtsbasis is gecreëerd. Uitzondering 8 is *meestal* van toepassing op een zorginstelling.

Antwoord: Opdracht 5

Hieronder staan enkele mogelijke negatieve gevolgen voor een cliënt, wanneer zijn gegevens op straat komen te liggen. Mogelijke negatieve gevolgen zijn:

- Kans op identiteitsfraude.
- Kans op stigmatisering (vooroordelen of misvattingen over cliënten).
- Kans op misbruik van persoonsgegevens.
- Kans op uitsluiting (bijv. bij sportclubs of werkgevers).
- Kans op vrijgeven van privacygevoelige informatie.

Antwoord: Opdracht 6

Alleen in bijzondere gevallen mag een organisatie om een kopie van een identiteitsbewijs aan hun klanten vragen. Voor sommige organisaties is dit echter verplicht, om hiermee te bewijzen dat ze aan de identificatieplicht hebben voldaan.

Organisaties die wel om een kopie identiteitsbewijs mogen vragen	Organisaties die niet om een kopie identiteitsbewijs mogen vragen
Overheden	Telecomproviders
Financiële instellingen	Zorginstellingen
Holland Casino	Makelaars
Werkgevers	Sportscholen

Antwoord: Opdracht 7

Een organisatie moet goed nadenken over het doel van het opvragen van een kopie van het identiteitsbewijs. Mogelijk is er een andere manier waarop minder persoonsgegevens opgevraagd worden.

Je kunt in bovenstaande tabel checken of de betreffende organisaties wel of niet rechtmatig om een kopie van je identiteitsbewijs hebben gevraagd. De kolom met organisaties die niet rechtmatig om een kopie identiteitsbewijs hebben gevraagd is niet compleet. Dit zijn een aantal voorbeelden.

Antwoord: Opdracht 8

Sommige organisaties vragen om een kopie van een identiteitsbewijs, terwijl zij dit niet op een wet baseren. In dat geval mag je je BSN en pasfoto op je identiteitsbewijs afschermen. Daarnaast is het zo veilig mogelijk om groot op de kopie te schrijven dat het een kopie betreft, voor wie deze kopie is, het doel ervan en de datum.

Vergelijk je kopie met die van de afbeelding in de factsheet of doe een check met de 'KopieID' app (opdracht 9).

Antwoord: Opdracht 9

Zie antwoord opdracht 8.

Antwoord: Opdracht 10

a. Check je top 3 aan de hand van de antwoorden bij de opdrachten 3 t/m 9.
b. Dit hangt af van de organisatie waar je werkzaam bent. Dit kun je eventueel met een collega of een leidinggevende bespreken.

Antwoord: Opdracht 11

Een aantal incidenten die in dit filmpje naar voren komen, zijn:

- Gestolen smartphone van medewerker met data van cliënten
- Data per ongeluk gepubliceerd op het internet
- Datalek niet gemeld
- Data verstuurd naar foutieve emailadressen

Antwoord: Opdracht 12

a. In het filmpje kan iemand het BSN van een ander terughalen. Dit is een persoonsgegeven van gevoelig aard, omdat hier identiteitsfraude mee gepleegd kan worden. Over het aantal gelekte gegevens wordt niks in het filmpje benoemd. Maar omdat je dit aantal niet kan uitsluiten, is er sprake van een 'ernstig' datalek.

   Toelichting:
   Een lek kan 'ernstig' zijn als er persoonsgegevens van gevoelige aard zijn gelekt. Denk bijvoorbeeld aan inloggegevens, financiële gegevens, kopieën van identiteitsbewijzen of gegevens die betrekking hebben op godsdienst of levensovertuiging, ras, politieke gezindheid, of gezondheid.

   Ook andere factoren, zoals de hoeveelheid gelekte persoonsgegevens per persoon of het aantal betrokkenen van wie er persoonsgegevens zijn gelekt, kunnen bepalend zijn of er sprake is van een 'ernstig' datalek. De aard en omvang van het datalek spelen hierbij dus een belangrijke rol.

b. Volgens de wet moet een 'ernstig' datalek, zonder onnodige vertraging, en zo mogelijk niet later dan 72 uur na de ontdekking, worden gemeld aan de Autoriteit Persoonsgegevens.

Antwoord: Opdracht 13

a. Beide situaties moeten door jou intern gemeld worden, afhankelijk van de organisatie bij je leidinggevende, een interne service-desk of bij de Functionaris Gegevensbescherming (FG) in je organisatie.

b. Dit antwoord is specifiek voor je organisatie. Kijk hiervoor naar de procedure over het melden van een datalek, zoals deze is opgesteld door je organisatie. Als er geen FG in je organisatie is aangewezen, worden deze taken waarschijnlijk in een andere functie opgepakt.

   Daarnaast is het belangrijk dat je je 'fouten' bij het lekken van persoonsgegevens durft te delen in je team en met je leidinggevende. Stop het niet in de doofpot, maar voorkom dat anderen ook deze fout maken. Je leidinggevende, collega's en FG kunnen je juist ondersteunen.

c. De FG bepaalt of deze melding van 'ernstige' aard is. Vervolgens zet hij/zij mogelijk de melding door naar de Autoriteit Persoonsgegevens. Het is dus niet aan jou om te bepalen of het datalek ernstig is. Bij iedere vorm van mogelijke datalekken is het belangrijk om deze via de procedure van je organisatie te melden. Twijfel je of er sprake is van een datalek? Meld het altijd intern!

   In situatie 1 neemt de FG contact op met degene die de e-mail heeft ontvangen en vraagt hem de e-mail te verwijderen zonder te openen. Daarnaast maakt hij/zij een melding bij de Autoriteit Persoonsgegevens.
   In situatie 2 is het verstandig dat de FG het datalek meldt bij de Autoriteit Persoonsgegevens. De aard en de omvang van het datalek is hierin doorslaggevend.

Sommige organisaties hebben een FG, andere niet.
Ben je werkzaam bij 's Heeren Loo?
's Heeren Loo heeft als grote zorgaanbieder een FG aangesteld. Daardoor is de FG degene die datalekken meldt bij de Autoriteit Persoonsgegevens. Dit doe je dus niet zelf! Verder 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!

Antwoord: Opdracht 14

a. Voorbeeld van een offline datalek in het filmpje:
   - Kind maakt tekening op papier met op de achterzijde gegevens van cliënt van vader.

b. Andere voorbeelden van een offline-datalek zijn:
   - Dossier van een cliënt in een zorgcentrum wordt in de container gegooid, in plaats van vernietigd door een papierversnipperaar.
   - Een dossier is verstuurd naar de printer, maar dit is bij de printer blijven liggen.