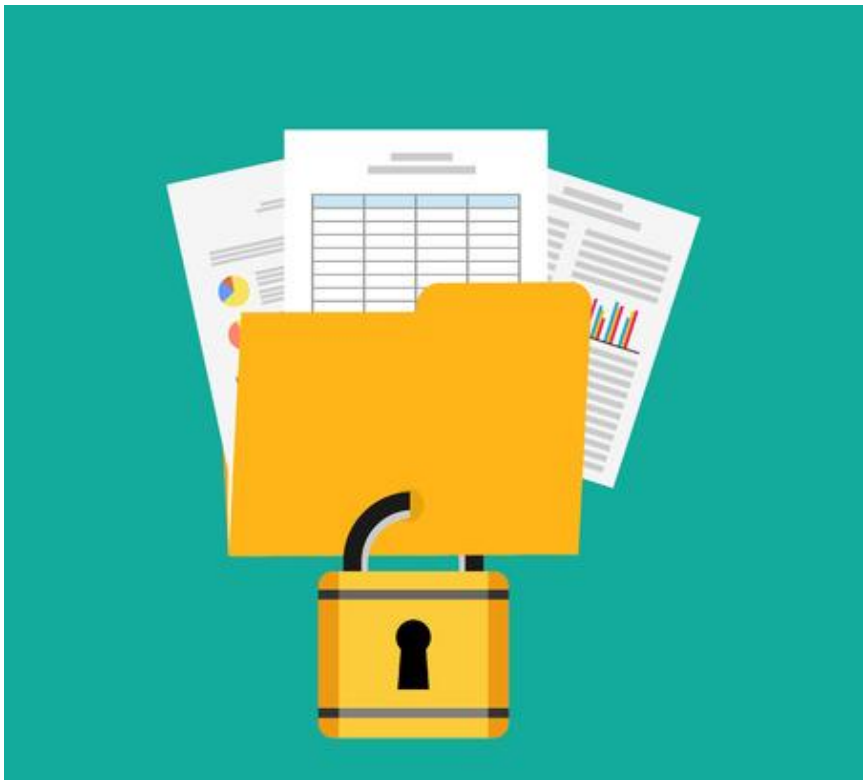

ANTWOORDBLAD PERSOONSGEGEVENS

TRAINING DIGITALE VAARDIGHEDEN
MODULE INFORMATIEBEVEILIGING EN PRIVACY

ANTWOORDBLAD PERSOONSGEGEVENS

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

Opdracht 1

a. In onderstaande tabel staat de indeling op classificatieniveau dikgedrukt weergegeven.

Document	Omcirkel de juiste classificatie
Cliënt-dossier	Openbaar - Bedrijfsvertrouwelijk - **Vertrouwelijk** - Geheim
Financieel jaarverslag	**Openbaar** - Bedrijfsvertrouwelijk - Vertrouwelijk - Geheim
Beleidsdocument	Openbaar - **Bedrijfsvertrouwelijk** - Vertrouwelijk - Geheim
Werkprocedure	Openbaar - **Bedrijfsvertrouwelijk** - Vertrouwelijk - Geheim
Persoonsgegevens medewerker	Openbaar - Bedrijfsvertrouwelijk - **Vertrouwelijk** - Geheim
Offerte	Openbaar - Bedrijfsvertrouwelijk - **Vertrouwelijk** - Geheim
Plannen voor reorganisatie	Openbaar - Bedrijfsvertrouwelijk - Vertrouwelijk - **Geheim**

Opdracht 2

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

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

b. In het voorbeeld van de verzekeringsgegevens worden gewone persoonsgegevens opgevraagd.

c. Deze opdracht heeft betrekking op je eigen werkzaamheden binnen je organisatie en is afhankelijk van jouw persoonlijk gedeelde informatie.

Opdracht 3

a. In de voorgestelde situatie wordt gevraagd naar *gewone* persoonsgegevens.

b. Er zijn zes grondslag(en) om deze *gewone* persoonsgegevens volgens de wet te mogen gebruiken. Alle zes de grondslag(en) staan in het Informatieblad Persoonsgegevens.
In de voorgestelde situatie moet je aan grondslag 1 of 2 voldoen:
1) Je moet de cliënt om toestemming vragen voor het gebruiken van zijn persoonsgegevens.
2) Je hebt de gegevens nodig voor het uitvoeren van de zorgovereenkomst tussen de cliënt en je organisatie.

c. Hieronder staan twee mogelijke negatieve gevolgen voor een cliënt wanneer zijn gegevens op straat komen te liggen:

- Kans op stigmatisering (vooroordelen of misvattingen over cliënten) of uitsluiting.
- Kans op misbruik van persoonsgegevens, bijvoorbeeld door identiteitsfraude.

Opdracht 4

a. De volgende organisaties mogen om een kopie van een identiteitsbewijs vragen om hiermee aan hun identificatieplicht te voldoen:

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

Opdracht 5

a. 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 veilig om er groot op te schrijven dat het een kopie betreft, voor wie deze kopie bedoeld is, en de datum. Was jou dat allemaal gelukt in de 'KopieID' app?

Opdracht 6

a. Je antwoorden hangen af van de organisatie waar je werkzaam bent. Vergelijk jouw antwoorden eens met die van een collega of bespreek ze met je leidinggevende.

Opdracht 7

a. Een aantal incidenten die in dit filmpje naar voren komen:

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

Opdracht 8

a. 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.

In het filmpje kan iemand het BSN van een ander terughalen. Dit is een persoonsgegeven van gevoelige 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.

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.

Opdracht 9

a. Beide situaties moeten door jou intern gemeld worden, omdat het gaat om een ernstig datalek.

b. Afhankelijk van hoe dit geregeld is in jouw organisatie moet je het datalek melden bij je leidinggevende, een interne service-desk of bij de Functionaris Gegevensbescherming (FG). Het is belangrijk dat je je 'fouten' bij het lekken van persoonsgegevens durft te delen met de daarvoor aangestelde persoon. Stop het niet in de doofpot, maar voorkom dat anderen soortgelijke fouten maken. Je leidinggevende, collega's of FG kunnen je juist ondersteunen.

c. Het is niet aan jou om te bepalen of het datalek ernstig is. De FG bepaalt dat en zet de melding mogelijk door naar de Autoriteit Persoonsgegevens. Bij iedere vorm van mogelijke datalekken is het belangrijk om deze via de juiste 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 de FG er melding van bij de Autoriteit Persoonsgegevens.
In situatie 2 is het verstandig als de FG het datalek meldt bij de Autoriteit Persoonsgegevens. De aard en de omvang van het datalek is hierin vooral doorslaggevend.

Weet je niet precies welke regels worden gehanteerd bij jouw organisatie als het gaat om een datalek? Check dan de procedure Meldplicht Datalekken van jouw organisatie!

Opdracht 10

a. In het filmpje komt het voorbeeld van een offline datalek naar voren in de vorm van een kindertekening. Op de achterzijde staan gegevens van een cliënt van de vader van het kind dat de tekening heeft gemaakt. De juf wil hem vervolgens op het prikbord in school hangen.

b. Andere voorbeelden van een offline-datalek zijn:

1. Een dossier van een cliënt in een zorgcentrum wordt in de container gegooid, in plaats van vernietigd door een papierversnipperaar.
2. Een dossier is verstuurd naar de printer, maar dit is bij de printer blijven liggen.

Opdracht 11

a. Vergelijk onderstaande antwoorden met je eigen antwoorden:

Onderwerp	Wat ik kan doen
Wachtwoorden	*Wachtwoorden veranderen als er de mogelijkheid bestaat dat iemand deze heeft gezien.*
Clean desk	Bij het gebruik van een dossier, deze direct terug doen in de kast en niet op mijn bureau laat liggen.
Phishing mails	Als ik een e-mail krijg met een externe link, deze controleren door mijn muis erop te houden.
Vertrouwelijke gesprekken	Geen vertrouwelijke gesprekken voeren in het bijzijn van collega's die er niets mee van doen hebben.
Vertrouwelijke documenten	Documenten die ik opsla het juiste classificatieniveau geven (vertrouwelijk of geheim).
PC-gebruik	Mijn PC vergrendelen als ik deze verlaat zodat niemand anders er toegang toe heeft.
Privé	Met mijn gezins-en andere familieleden geen vertrouwelijke informatie bespreken.

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