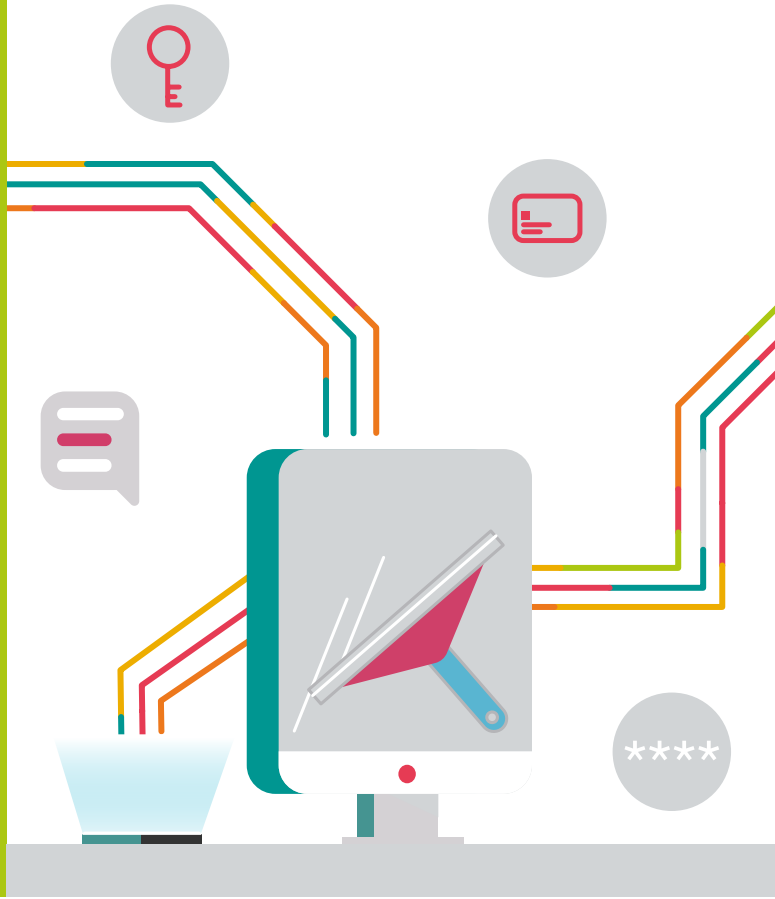
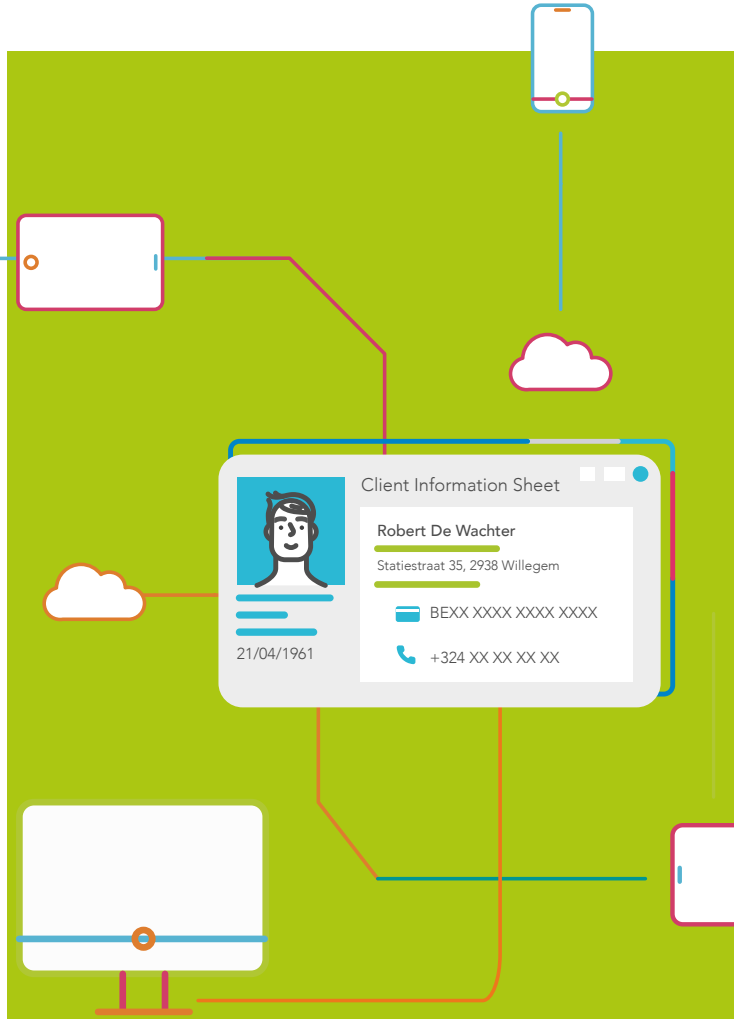
GDPR
DATA CLEAN-UP

GEGEVENSBESCHERMING
IS OOK JOUW TAAK.
TIJD VOOR EEN
GROTE SCHOONMAAK!



CYBER SECURITY
COALITION.be



In deze brochure maken we je wegwijs in het opruimen van persoonsgegevens die je bij de uitoefening van je job bewaart – op je laptop, gsm of in een cloud.

Waarom is een schoonmaak zo belangrijk?

Persoonsgegevens zijn overal.
Je zou ervan versteld staan hoeveel persoonsgegevens je in het kader van je werk op verschillende apparaten en in verschillende toepassingen of apps bijhoudt (bijvoorbeeld op je laptop, smartphone of tablet voor professioneel gebruik, evenals op USB-sticks en externe harde schijven). Dagelijks verzenden en bewaren we persoonsgegevens in onze mailboxen, op apps, in een cloud …

Een reëel en groot risico
Persoonsgegevens zijn net zoals andere data gevoelig voor verlies, diefstal of schending van de vertrouwelijkheid. Wanneer een organisatie persoonsgegevens verliest of wanneer deze gegevens gestolen worden, kan dit zeer ernstige gevolgen hebben. Een datalek heeft niet enkel gevolgen voor de betrokken personen (schending van de privacy), maar ook voor het bedrijf zelf (imagoschade, boetes, klantenverlies). Bovendien is het wettelijk verplicht om persoonsgegevens te verwijderen wanneer het doel van de verwerking is bereikt.

Iedereen is betrokken
Gegevensbescherming is de verantwoordelijkheid van je bedrijf of organisatie. Maar als medewerker kun jij ook een belangrijke bijdrage leveren.
Door correct om te gaan met persoonsgegevens bescherm je anderen en help je je organisatie om haar goede reputatie te behouden.
Behandel persoonsgegevens van anderen zoals je zou willen dat er met jouw gegevens wordt omgegaan.

Gegevensbescherming: een korte inleiding

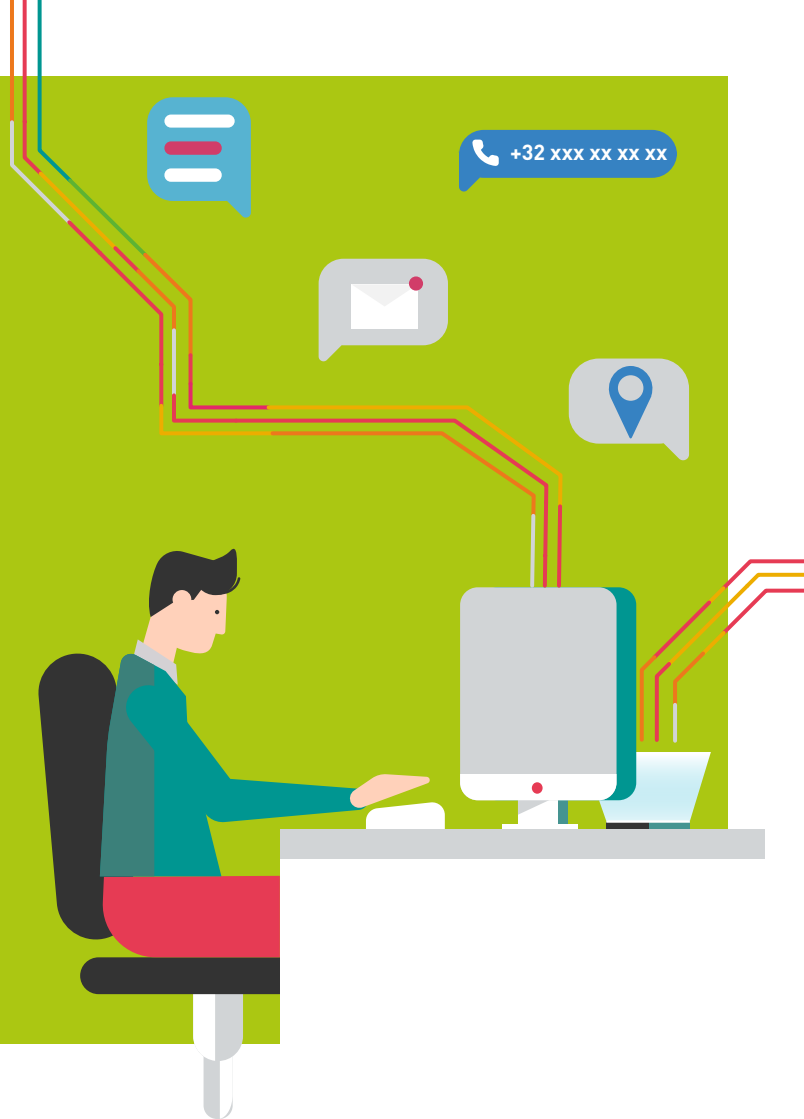
GDPR
Sinds 25 mei 2018 is de GDPR (General Data Protection Regulation) van toepassing. Deze Europese regelgeving verplicht alle ondernemingen en organisaties de nodige maatregelen te nemen om persoonsgegevens te beschermen.

Basisprincipes
De GDPR bepaalt dus hoe we op een rechtmatige en veilige manier persoonsgegevens verzamelen, verwerken en bewaren. Enkele van de basisprincipes zijn dat persoonsgegevens alleen verzameld mogen worden voor welbepaalde, gerechtvaardigde doeleinden én dat we deze gegevens niet langer dan noodzakelijk mogen bewaren. Bovendien moeten we ervoor zorgen dat persoonsgegevens op een veilige manier worden verwerkt.

Wat verstaan we onder persoonsgegevens?
Dit zijn alle gegevens die een persoon identificeren of op basis waarvan een persoon rechtstreeks of onrechtstreeks geïdentificeerd kan worden. De naam, het telefoonnummer en het e-mailadres zijn voor de hand liggende voorbeelden, maar ook betalingsinformatie, foto's, evaluaties en locatiegegevens zijn persoonsgegevens.

Daarnaast is er een specifieke categorie van gevoelige gegevens die bijzondere aandacht vragen. Het gaat dan bijvoorbeeld om medische gegevens, politieke opvattingen, religieuze overtuigingen ...

Om welke personen gaat het dan?
De GDPR is van toepassing op alle persoonsgegevens die in jouw organisatie verzameld, verwerkt en bewaard worden. Het kan onder meer gaan om gegevens van klanten, prospecten, medewerkers en leveranciers.



Hoe begin je eraan?

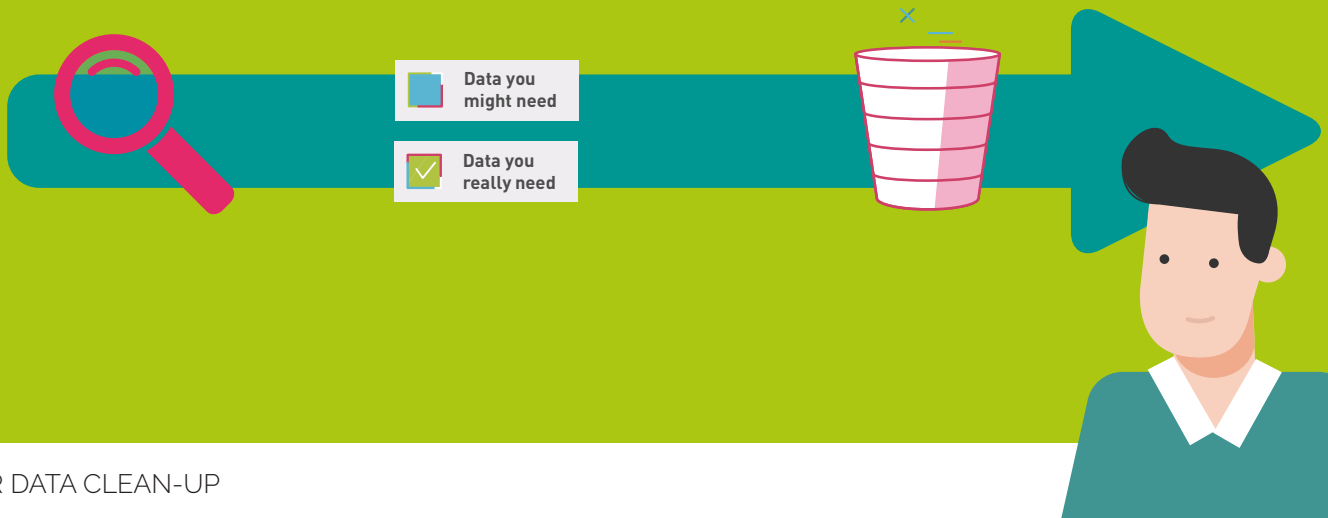
Helemaal klaar voor de schoonmaak van persoonsgegevens?

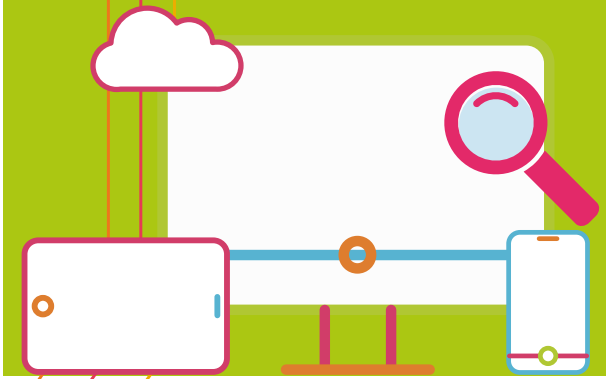
Met ons stappenplan kun je meteen aan de slag!

Stap 1
identificeer en lokaliseer

Stap 2
maak je vertrouwd met de bewaartermijnen

Stap 3
kom in actie





Stap 1: identificeer en lokaliseer

Vooraleer je kunt starten met de schoonmaak is het belangrijk om na te denken over welke persoonsgegevens je bewaart bij de uitoefening van je job en waar je deze bewaart.

- **Identificeer de persoonsgegevens** die je bewaart. Dit kunnen onder andere gegevens zijn van klanten, leveranciers, collega's, sollicitanten... Denk aan voor de hand liggende persoonsgegevens, zoals namen, e-mailadressen en telefoonnummers, maar vergeet niet dat ook foto's, IP-adressen ... als persoonsgegevens worden beschouwd. Afhankelijk van de sector waarin jouw organisatie actief is, bewaar je misschien ook gevoelige gegevens als medische informatie.

  – Het **verwerkingsregister** van je organisatie kan hierbij een hulpmiddel zijn. Dit bevat een inventaris van alle activiteiten rond gegevensverwerking binnen je organisatie. Dit document is verplicht voor elke onderneming met meer dan 250 medewerkers of in het geval van risicovolle verwerkingen.

- **Ga na waar je deze persoonsgegevens bewaart.** De meeste organisaties maken gebruik van opslagsystemen die **lokaal of in een cloud** worden gehost. Denk aan de centrale schijfruimte, een CRM-systeem, een intranet, wiki of ander online samenwerkingsplatform enz. Vergeet je professionele mailbox niet en denk na over welke andere applicaties je gebruikt in je job. Mogelijk bewaar je persoonsgegevens **lokaal op je professionele toestellen**, zoals je laptop, smartphone, een USB-stick of externe harde schijf.

- Ga na of je deze persoonsgegevens ook op **andere systemen of apparaten** bewaart. Exporteer je soms documenten vanuit een applicatie of maak je kopieën van documenten die persoonsgegevens bevatten? Waar en hoe bewaar je back-ups?

! Vermijd duplicatie van persoonsgegevens.
Dit verhoogt namelijk het risico op incidenten, zoals ongeoorloofde toegang door anderen.

- Ga na welke regels je organisatie hanteert met betrekking tot het dupliceren van persoonsgegevens (beleid inzake bewaartermijnen, Bring Your Own Device policy, ...).
- Gegevens die voor gebruiksgemak worden gedupliceerd, moeten vlak na gebruik worden verwijderd, aangezien de bewaarperiode alleen betrekking heeft op het oorspronkelijke bestand.

  – Voorbeeld: Een medewerker exporteert e-mailadressen van klanten uit het centrale CRM-systeem naar een Excelbestand, om deze lijst vervolgens te uploaden in een e-mailmarketingprogramma. Zodra deze actie is voltooid, moet hij de geëxporteerde lijst verwijderen.

- Check ook of je persoonsgegevens voor professioneel gebruik bewaart op je **eigen apparaten die voor professionele doeleinden** worden toegestaan. Ook op deze apparaten moet je een data clean-up uitvoeren!

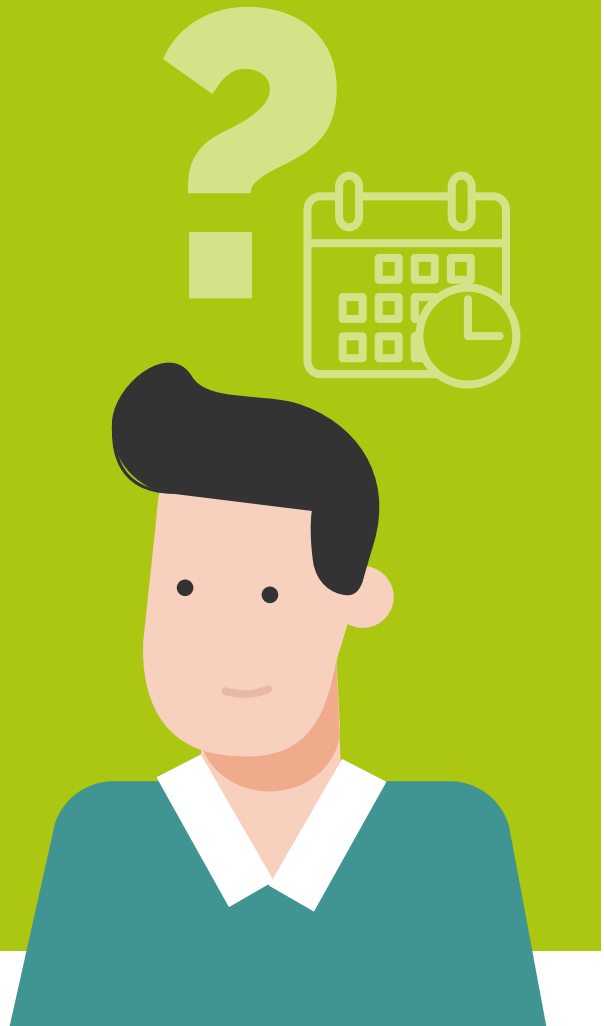
Stap 2: maak je vertrouwd met de bewaartermijnen

Nu je de door jou bewaarde persoonsgegevens in kaart hebt gebracht, is het belangrijk om te weten of je ze nog mag bijhouden. Als basisregel geldt dat je persoonsgegevens maar zo lang als strikt noodzakelijk mag bewaren. Maar hoelang is dat dan? Sommige bewaartermijnen zijn bij wet bepaald, andere zijn door je organisatie vastgelegd. Zodra je de geldende bewaartermijnen kent, weet je welke persoonsgegevens je al zeker kunt verwijderen in de volgende fase.

Bewaartermijnen in jouw organisatie of bedrijf
Informeer je over de bewaartermijnen die jouw organisatie heeft vastgelegd voor elke verwerking van persoonsgegevens.

- Elke verwerking heeft een geïdentificeerde duurtijd of moet op zijn minst voldoen aan criteria die bepalen wanneer het doel is bereikt.
- Organisaties moeten hun bewaartermijnen op regelmatige basis herzien. Het einde van een bewaartermijn kan worden getriggerd door bepaalde gebeurtenissen.

  – Voorbeeld: Een organisatie moet de persoonsgegevens van een sollicitant verwijderen zodra het duidelijk is dat die persoon niet zal worden aangeworven. Indien de organisatie het cv van de sollicitant toch wil bewaren, bijvoorbeeld voor het aanleggen van een wervingsreserve, dan moet ze de sollicitant hierover informeren en hem het recht geven zich hiertegen te verzetten.



- Sommige bewaartermijnen zijn gebaseerd op wettelijke verplichtingen en werden vastgelegd in de **Belgische wet**.

Waar kan ik deze informatie terugvinden?
De info over de bewaartermijnen die jouw organisatie heeft vastgelegd, kun je terugvinden in de **privacyverklaring of in de richtlijnen voor de bescherming van persoonsgegevens**. Neem voor toelichting contact op met de verwerkingsverantwoordelijke of DPO binnen je organisatie.

Onthoud!
- Als je geen wettelijke verplichting hebt, bewaar dan **alleen de persoonsgegevens die echt nodig zijn om je werk te doen** en zorg ervoor dat die taak binnen de toegestane gebruiksdoelen valt. Vraag bij twijfel advies aan de verwerkingsverantwoordelijke of DPO van je organisatie.
- Houd geen onnodige kopieën van persoonsgegevens bij.

Stap 3: kom in actie

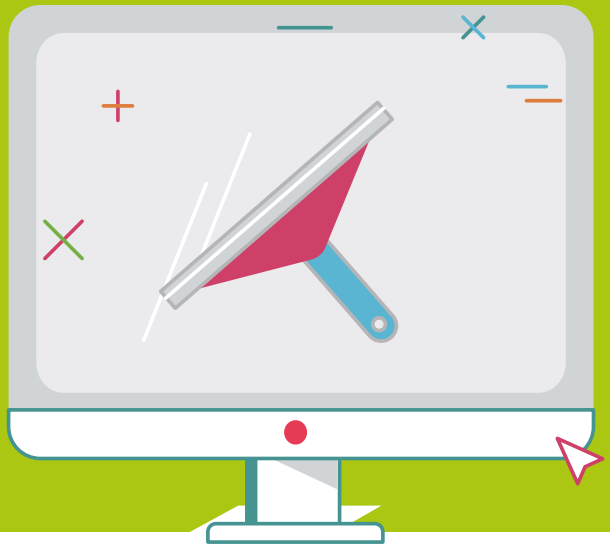
Nu je de bewaartermijnen kent, kun je aan de slag gaan. In deze stap ga je de persoonsgegevens verwijderen of veilig opslaan.

Verwijder alle persoonsgegevens waarvan de bewaartermijn is verstreken of die niet meer noodzakelijk zijn voor de uitvoering van je job.

- Als jouw organisatie over centrale IT-systemen beschikt, heeft je IT-afdeling daarin mogelijk al **automatische archivering of verwijdering** geïmplementeerd om aan de bewaartermijnen te voldoen.

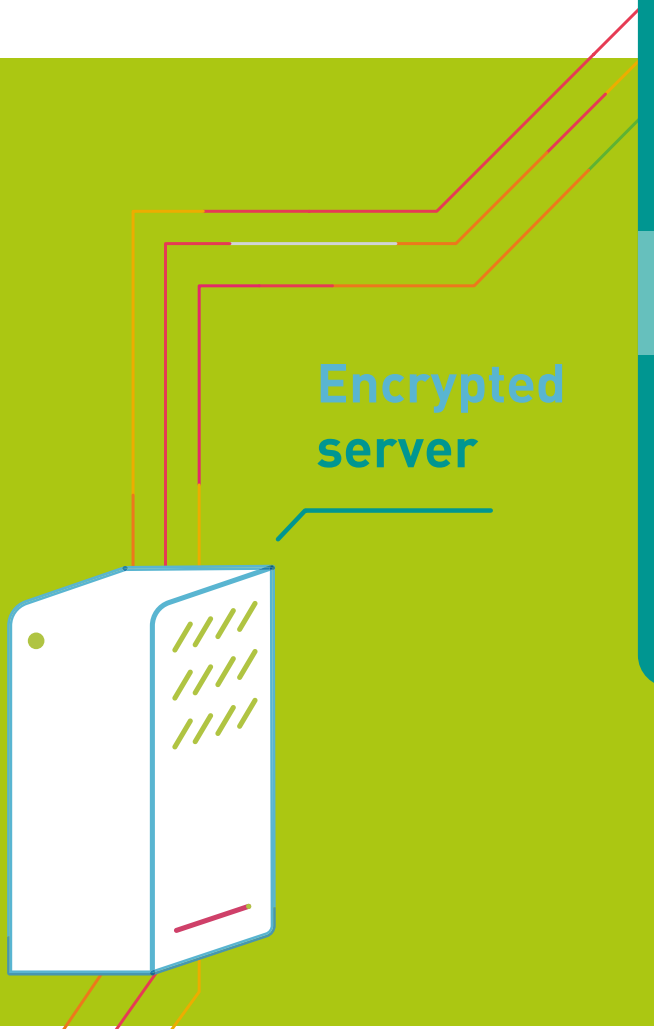
  – Voorbeeld: camarabeelden mogen maximaal één maand worden bewaard. Het systeem herkent de datums en verwijdert automatisch beelden die ouder zijn dan een maand.

- Indien de systemen die je gebruikt geen automatisch verwijderingsproces toestaan, controleer dan of er een **manuele procedure** is die je regelmatig kunt toepassen.
- Zorg ervoor dat **gedupliceerde persoonsgegevens** worden verwijderd, tenzij ze als back-up voor de organisatie moeten dienen.
- Vergeet niet om ook persoonsgegevens te verwijderen die je op je **persoonlijke apparaten** hebt opgeslagen.



In specifieke gevallen mag je persoonsgegevens archiveren.

- In sommige gevallen moet je bepaalde persoonsgegevens toch nog bewaren, ook al heb je ze niet meer nodig om je job uit te oefenen. Denk bijvoorbeeld aan gegevens die noodzakelijk zouden kunnen zijn in het geval van een claim (juridische procedure) of een boekhoudkundige verantwoording. Zorg ervoor dat je die persoonsgegevens **veilig archiveert en de toegang ertoe beperkt**. Vraag bij twijfel advies aan de DPO van je organisatie.



Bewaar de persoonsgegevens die nog noodzakelijk zijn op een veilige manier.

- In de eerste plaats moet de **toegang tot de persoonsgegevens worden beperkt** tot personen die de gegevens nodig hebben voor hun werk.

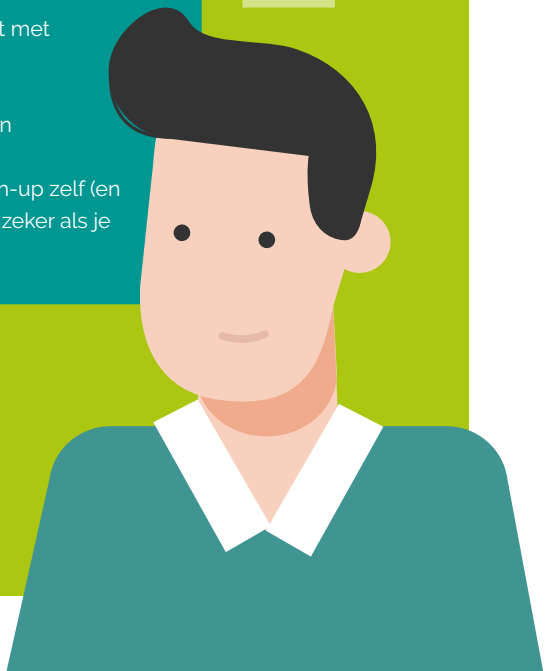
  – Voorbeeld: arbeidsovereenkomsten alleen toegankelijk maken voor de hr-afdeling door ze op een specifieke, afgeschermde plaats te bewaren.

- Om te voorkomen dat onbevoegde personen toegang krijgen tot je apparaten of tools bij verlies / diefstal moet je de toegang tot je apparaten of tools beveiligen. Dat kan onder meer door een **sterk wachtwoord** te gebruiken.
- Wil je deze gegevens langer dan de vereiste bewaartermijn bewaren, bijvoorbeeld voor statistische doeleinden of testdoeleinden, dan is het noodzakelijk om ze te **anonimiseren**.

Praktische tips

Het opruimen van persoonsgegevens kost tijd en moeite. We geven je nog enkele handige tips:

- **Ga systematisch te werk.** Volg het driestappenplan en voorzie voldoende tijd om elke stap uit te voeren.
- **Werk samen met je collega's**. Werk je binnen een groot bedrijf, dan kun je de data clean-up ook organiseren met de collega's van jouw afdeling.
- **Begin met één apparaat of tool.** Start bijvoorbeeld met het opruimen van je professionele mailbox.
- **Ruim ook je persoonlijke apparaten op**. Gebruik je bijvoorbeeld je persoonlijke smartphone voor zakelijke doeleinden, verwijder dan ook oude professionele foto's en persoonsgegevens die je hebt gedeeld in berichtenapps enz.
- **Gebruik sterke wachtwoorden**. Bescherm de persoonsgegevens die je nog nodig hebt met sterke wachtwoorden.
- **Vermijd het gebruik van USB-sticks of externe harde schijven voor de opslag van persoonsgegevens**. Indien je ze toch gebruikt, zorg dan altijd voor een versleuteling van de gegevens.
- **Als er ook privébestanden op je professionele apparaten staan,** moet je de data clean-up zelf (en in je eigen belang) uitvoeren, bijvoorbeeld in "Mijn documenten" of "Mijn afbeeldingen", zeker als je daar gevoelige gegevens bewaart.



Lijst van interessante websites

gegevensbeschermingsautoriteit.be

edpb.europa.eu

Safeonweb.be

CYBER SECURITY
COALITION.be

www.cybersecuritycoalition.be

Deze brochure kwam tot stand dankzij de medewerking van Belnet, MIVB, de Hoge Raad voor de Zelfstandigen en de KMO en AG Insurance.