GDPR: Hoe alle voorschriften naleven?

Inhoud

I. Wat was er vroeger en wat brengt de toekomst?

GDPR (General Data Protection Regulation of Algemene Verordening Gegevensbescherming) is een document van ruim 80 pagina's en 99 artikels dat in mei 2016 werd goedgekeurd. De Europese wetgever gaf de voorkeur aan een verordening boven een richtlijn om in de hele Unie zoveel mogelijk dezelfde toepassing ervan te verkrijgen. In tegenstelling tot een richtlijn wordt een verordening immers niet aan de situatie in de diverse lidstaten aangepast via de omzetting in nationale wetten. Een verordening is dus rechtstreeks van toepassing.

Niemand kan dus nog doen of deze tekst, die vanaf mei 2018 van kracht zal zijn, niet bestaat. Deze verordening is er gekomen om burgers meer controle over hun gegevens te geven door de spelers die deze gegevens verwerken voor hun verantwoordelijkheid te plaatsen.

De tijd dat men de bescherming van persoonsgegevens gemakkelijk over het hoofd kon zien is bijna voorbij. Veel spelers hebben er nu belang bij om een klacht in te dienen, zoals ontevreden klanten, uw concurrenten, uw werknemers, de Privacycommissie, …

De nieuwe verordening **bevestigt grotendeels de bestaande principes**. De verplichting om gegevens te beschermen bestaat al bijna 20 jaar, aangezien de eerste richtlijn al van 1995 is. Maar het klopt ook dat niemand er echt aandacht aan heeft besteed en dat de voorzien sancties zeer zelden werden toegepast. De regels zijn dus niet nieuw, maar ze werden versterkt en in bepaalde opzichten aangepast. Als u niet op de eerste trein bent gesprongen, is het nu kwestie van de tweede niet te missen!

Er zal nu immers **een ruime waaier aan strengere sancties worden opgelegd.** Tot nu waren er alleen strafrechtelijke geldboeten voorzien. Het risico dat ze zouden worden toegepast, was klein, want dan moest er eerst een strafrechtelijke procedure voor een rechtbank worden ingeleid. Maar nu kan de Privacycommissie u zeer hoge administratieve boeten opleggen en ze kan dit veel gemakkelijker doen dan vroeger. Voor de zwaarste gevallen voorziet de verordening in een plafond van 20 miljoen euro of 4% van de totale omzet als boete.

Naast een stevige boete riskeert u ook een tijdelijke opschorting of zelfs een definitieve stopzetting en het verbod om nog gegevens te verwerken. Zonder de potentiële imagoschade en het verlies aan geloofwaardigheid van uw bedrijf te vergeten.

Deze verordening legt dus talrijke verplichtingen op, maar sommige delen van de GDPR zullen een grotere impact op bepaalde organisaties hebben dan op andere. GDPR is dus geen revolutie, maar eerder een evolutie naar een nieuwe situatie.

II. Wat is de verwerking van persoonsgegevens eigenlijk?

Misschien beseft u het niet, maar bij veel van uw dagelijkse activiteiten doet u eigenlijk aan de verwerking van persoonsgegevens. Elk bedrijf verwerkt op grote schaal persoonsgegevens, soms zonder het te beseffen.

"Persoonsgegevens" is de term die wordt gebruikt voor alle informatie op basis waarvan iemand rechtstreeks of onrechtstreeks kan worden geïdentificeerd (identificeerbaar), zoals de naam, het adres, het rijksregisternummer, de loongegevens, het online profiel, de gegevens van een elektronische verbinding, het IP-adres, een kandidatuur, beelden van een bewakingscamera, de aankoopgeschiedenis, klikgedrag, lokalisatiegegevens, enz.

Als autocar- of autobusbedrijf verwerkt u vooral gegevens van uw werknemers, uw klanten en uw leveranciers.

Het begrip **"verwerking"** wordt zo ruim geïnterpreteerd, dat **vrijwel elke manipulatie van persoonsgegevens als verwerking wordt beschouwd.** Denk onder andere aan het verzamelen, registreren, opslaan, updaten, wijzigen, raadplegen, gebruiken, verzenden, distribueren, wissen, extraheren, enz. van gegevens. Verwerking begint bij het verzamelen van gegevens en eindigt bij het wissen ervan.

Een voorbeeld: Het betreft dus gegevens die u dagelijks verzamelt via een online formulier op uw website, een contactformulier waarin de gebruiker alleen een e-mailadres vermeldt, een inlichtingenfiche of een inschrijvingsformulier. Andere courante verwerkingen zijn personeels- en loonbeheer, downloads van de tachograaf, geolocalisatie van de chauffeurs, een telefoongids van een bedrijf, de boekhouding, klantenbeheer, bewaking (video, alarm, toegangscontrole, …).

De voorwaarde is dat de verwerking minstens gedeeltelijk moet zijn geautomatiseerd of, als dat niet het geval is, dat de persoonsgegevens bestemd zijn voor opname in een bestand.

Een voorbeeld: Tijdens uw professionele activiteiten houdt u de visitekaartjes van uw contacten bij. Als u deze kaartjes gewoon op een hoopje in een bureaulade bewaart, gaat het niet om gegevensverwerking en telt de bescherming van de GDPR niet. Maar als u daarentegen de kaartjes gestructureerd ordent, bijvoorbeeld alfabetisch, om een persoon en zijn gegevens gemakkelijker terug te vinden, dan is dit de verwerking van persoonsgegevens en moeten specifieke juridische regels worden gevolgd.

De enige uitzondering is verwerking die in het kader van strikt persoonlijke, privé-activiteiten plaatsvindt, dus zonder enige band met uw professionele of commerciële activiteiten. *Een voorbeeld: de contactenlijst van uw persoonlijke gsm (dus niet van de gsm die u voor uw werk gebruikt!).*

III. Welke spelers zijn belangrijk?

Verantwoordelijke voor de verwerking

Elk bedrijf, elke zelfstandige, al wie professioneel bezig is, bewaart persoonsgegevens, van klanten, leveranciers, werknemers, enz.

Geen enkel bedrijf, ongeacht de grootte of sector ervan, geen enkele professional ontsnapt aan de gevolgen van de nieuwe reglementering. Natuurlijk verschillen de risico's en de omvang van de te nemen maatregelen van speler tot speler, maar alle bedrijven kunnen het slachtoffer van gegevensdiefstal of hacking worden.

In de GDPR-verordening draagt de verantwoordelijke voor de verwerking de grootste verantwoordelijkheid, hij of zij bepaalt de middelen en doeleinden van de verwerking. Het voornaamste criterium is zijn juridische en organisatorische capaciteit.

In de meeste gevallen **is de werkgever de verantwoordelijke voor de verwerking**. Maar ook meerdere verantwoordelijken voor de verwerking zijn mogelijk. Zij bepalen dan samen de doeleinden en middelen van de verwerking.

Toeleverancier - verwerker

U kan een externe verwerker aanstellen om bepaalde persoonsgegevens te verwerken. Deze verwerker is "*de natuurlijke persoon, de rechtspersoon, de feitelijke vereniging of het openbaar bestuur die persoonsgegevens verwerkt ten behoeve van de voor de verwerking verantwoordelijke*".

Voorbeelden van verwerkers: het kan gaan om een sociaal secretariaat, een tour-operator, een screeningbureau bij een aanwerving, een web- of marketingbureau, een archiveringsdienst voor e-filing, een overheid, een clouddienst, een bewakingsfirma, een verzekeringsmaatschappij of een extern IT-bedrijf.

Als u op een beroep doet op toeleveranciers voor de verwerking, controleer dan of zij voldoende garanties bieden dat de verwerking volgens de reglementering verloopt. Als verantwoordelijke voor de verwerking dient u de contracten met elke verwerker te analyseren: hoe uitgebreid is de verwerking, wat is de aard ervan, hoe lang duurt ze en wat zijn de doeleinden ervan, welke categorieën personen zijn betrokken, wat zijn uw rechten en verplichtingen, … In de contracten met uw toeleveranciers dient u de clausules die betrekking hebben op de GDPR aan te passen, onder andere betreffende het delen van verantwoordelijkheid of de verplichting om elke privacyschending te melden. Ga dus na of u met "veilige" partners werkt.

Voorbeeld: Een betrouwbare verwerker zal een gedragscode toepassen die door de Privacycommissie is goedgekeurd. Vraag minstens aan uw toeleverancier welk beleid inzake gegevensbescherming hij toepast.

De verwerking dient volgens uw instructies te verlopen; De verwerker dient zijn ingrepen te beperken tot de opdracht die u hem gegevens hebt. U dient uw instructies te documenteren, bijvoorbeeld via een lastenboek of bijlagen bij het contract. Als de verwerker zijn boekje te buiten gaat en de gegevens

(her)gebruikt voor andere doeleinden dan deze waarin het contract voorziet, dan wordt de verwerker zelf verantwoordelijk voor de verwerking en moet hij de gevolgen dragen die uit dit statuut voortvloeien, met name een grotere verantwoordelijkheid dragen.

Belangrijk om op te merken is nog dat een bedrijf tegelijkertijd zowel verwerkingsverantwoordelijke als verwerker kan zijn.

Taak: analyseer en herformuleer uw contracten met uw toelveranciers (verwerkers).

De Privacycommissie

De Privacycommissie is een onafhankelijke controle-instantie die waakt over de toepassing van de reglementering. De bevoegdheden van deze commissie werden nu uitgebreid. Voor de ergste gevallen kan zij nu gemakkelijker boeten eisen dan vroeger. Na een onderzoek of een klacht heeft de commissie nu ook de bevoegdheid om verscheidene maatregelen te nemen, zoals een waarschuwing, berisping, verzoek om de verwerking in overeenstemming te brengen met de bepalingen van de GDPR, een tijdelijke of definitieve verwerkingsbeperking, … Vooraleer er sprake kan zijn van boetes, moet er dus een heel proces doorlopen worden.

De Commissie publiceert bovendien interpreterende richtlijnen over bepaalde begrippen en principes van de verordening.

IV. Welke verplichtingen heeft de verantwoordelijke voor de verwerking?

Zodra u persoonsgegevens verzamelt, dient u een aantal verplichtingen na te leven. De verordening herneemt de bestaande verplichtingen van de richtlijnen en voegt er nieuwe toe.

1) Transparent zijn en informeren

Het transparantieprincipe is de basis van de hele reglementering. Als u persoonsgegevens verzamelt, dient u dat altijd transparant te doen, dat wil zeggen dat u de betrokken personen hiervan **in een duidelijke en begrijpelijke taal** op de hoogte dient te brengen.

U dient te vermelden welke soorten gegevens worden verzameld, voor welke doeleinden, hoe lang deze gegevens worden bewaard, aan wie deze gegevens kunnen worden doorgegeven en welke rechten uw klanten hebben in verband met hun gegevens.

Al deze informatie dient zich in een document te bevinden dat voor uw klanten beschikbaar is en dat zij op elk ogenblik kunnen raadplegen en opslaan. Ideaal plaatst u dit document op uw website, als dit mogelijk is. Het betreft de “Privacy Statement” of “Privacy Policy” (in het Nederlands ook de “Privacyverklaring” of het “Privacybeleid” genoemd).

Taak: Controleer en herwerk de informatie indien nodig en pas de Privacyverklaring aan of publiceer er een

2) Enkel geoorloofde verwerkingen uitvoeren

De onderneming mag enkel persoonsgegevens verwerken wanneer ze daarvoor een correcte juridische basis heeft. Enkel de hierna opgesomde gronden kunnen in aanmerking genomen worden:

De verordening behoudt **toestemming** als juridische basis, maar voegt er **striktere voorwaarden** aan toe. De toestemming moet vrij en specifiek zijn, gebaseerd op nuttige en eenduidige informatie die in een heldere en begrijpelijke taal is opgesteld. Elke verwerkingsverantwoordelijke moet kunnen aantonen dat er toestemming werd gegeven (de GDPR vermeldt "expliciete toestemming"). De betrokken persoon moet uitdrukkelijk zijn toestemming geven voor de verwerking van zijn gegevens en dit in alle vrijheid.

Om dit na te leven brengt u bijvoorbeeld een vakje aan dat de betrokkene moet aankruisen (opgelet: geen vooraf aangekruiste vakjes gebruiken!) wanneer hij uw verklaring van privacybescherming terugstuurt.

Personen van wie de gegevens worden verwerkt, hebben ook het recht om hun toestemming op elk ogenblik te herroepen. Deze herroeping heeft geen gevolgen voor het al dan niet geoorloofd zijn van de oorspronkelijke verwerking, maar alleen voor latere verwerkingen. Als de betrokkenen zijn toestemming herroept, mogen de gegevens dus niet langer worden verwerkt.

Taak: controleer de formulieren waarmee u persoonsgegevens opvraagt en herwerk ze eventueel.

De verwerking is geoorloofd als ze **noodzakelijk is voor de uitvoering van de overeenkomst.** *Voorbeelden:*

- *Om uw werknemers te betalen hebt u hun bankgegevens nodig.*
- *Om kinderen op te halen voor schoolvervoer hebt u een adres nodig. Maar u hoeft daarvoor in geen geval het beroep van de ouders te kennen.*

De verwerking kan ook nodig zijn om **een verplichting na te komen** die aan de verwerkingsverantwoordelijke wordt opgelegd door een wet, een decreet of een ordonnantie. *Voorbeeld: de inhouding van socialezekerheidsbijdragen of bedrijfsvoorheffing.*

Het **algemeen belang** vormt eveneens een rechtvaardigingsgrond voor gegevensverwerking. Die kan slechts worden ingeroepen door de overheid zelf of in het kader van de uitoefening van een opdracht van algemeen belang. Meestal zal deze grond in de private autobus- en autocarsector niet kunnen ingeroepen worden. Deze grond laat bijvoorbeeld wel toe aan De Lij of de TEC om een lijst met abonnees bij te houden.

Verwerking is eveneens mogelijk wanneer het **vitaal belang** van een persoon op het spel staat. In dit geval moet het gaan over zeer gewichtige zaken en moet er in het belang van de betrokken persoon gehandeld worden. *Bijvoorbeeld: een persoon heeft tijdens een autocarreis een medisch probleem en heb bedrijf*

moet de familie van de persoon bereiken om belangrijke medische gegevens aan dokters of verplegers te kunnen overmaken.

Het **gerechtvaardigd belang** vormt de laatste belangrijke juridische basis. Deze basis kan bijvoorbeeld gebruikt worden in het kader van direct marketing activiteiten. Wanneer men voor dergelijke activiteiten toestemming als basis zou willen inroepen, dan moet men bij het verzamelen van de informatie die toestemming bekomen of post factum toestemming vragen. Dat laatste zou bijvoorbeeld kunnen door een bericht te sturen naar alle betrokkenen en hen te vragen om te antwoorden dat ze effectief die reclame nog willen ontvangen (men heeft immers een expliciete toestemming nodig). In de praktijk zal dat allicht betekenen dat men nog zeer weinig klanten zal kunnen contacteren. In een dergelijk geval kan het gerechtvaardigd belang van de onderneming ingeroepen worden. Dit kan echter slechts voor zover de promotie betrekking heeft op producten of diensten die in de lijn liggen met wat de klant voordien al heeft aangekocht en onder bepaalde voorwaarden, met name:

- Er moet een evenwicht zijn tussen het belang van het bedrijf en van het individu. Vanuit dit oogpunt dient het bedrijf er zich van te gewissen dat de betroffen persoon geïformeerd is en zich rederlijkerwijze kan verwachten door een bedrijf voor commerciële doeleingen gecontacteerd te worden.
- Het belang moet reëel en specifiek zijn. Bijvoorbeeld: het bedrijf wil communiceren over de goederen en diensten die het aanbiedt ten einde de verkoop ervan te bevorderen.
- De verwerking van de gegevens (in dit geval het versturen van informatie over de diensten van het bedrijf) moet nodig zijn om het legitiem doel (optimalisatie van de verkoop) te bereiken. Dat betekent voornamelijk dat er geen alternatief voor handen is.

Bijvoorbeeld: een klant die reeds een autocarreis geboekt heeft kan geïnformeerd worden over nieuwe reizen die door het bedrijf aangeboden worden.

In dit geval is het belang van uw bedrijf de verkoop te bevorderen, maar is het eveneens in het belang van de klant om op de hoogte te blijven van het aanbod aan reizen waar hij of zij heel duidelijk interesse in heeft getoond. Men kan dus argumenteren dat er een evenwicht is tussen de belangen van het bedrijf en het individu.

Gevoelige gegevens - die betrekking hebben op ras, etnische afkomst, politieke, filosofische of godsdienstige overtuiging, lidmaatschap van een vakbond, gezondheid, seksuele voorkeur, begane overtredingen of strafrechterlijke veroordelingen - mogen in principe niet verwerkt worden, maar er zijn enkele uitzonderingen.

3) De veiligheid en wettelijkheid van de gegevensverwerking verzekeren

Zodra u persoonsgegevens verzamelt, dient u **technische en organisatorische maatregelen** te nemen om de gegevens maximaal te beveiligen en de reglementering na te leven. U kiest zelf welke maatregelen dat zijn, op basis van de aard van de gegevens, de hoeveelheid verzamelde gegevens, de doeleinden van de verwerking en de potentiële risico's bij een lek, verlies of diefstal van gegevens.

Technische maatregelen zijn maatregelen op het niveau van het IT-systeem van het bedrijf, bijvoorbeeld om intern de toegang tot de gegevens te beperken of om de gegevens te versleutelen, te anonimiseren[1] of te pseudonimiseren[2]. Organisatorische maatregelen zijn maatregelen in verband met het interne gegevensbeheer. Ze kunnen gaan van het opstellen van een intern beleid voor gegevensverwerking, met onder andere de bewustmaking en opleiding van uw werknemers die belast zijn met de gegevensverwerking, tot de beveiliging van het interne netwerk of de servers, de fysieke beveiliging van lokalen, het verbod om niet-gecontroleerde informaticanetwerken aan te sluiten, enz.

Taak: een audit van de informaticaveiligheid uitvoeren

4) Een register van de verwerkingsactiviteiten bijhouden

Het betreft een logboek/werkblad waarin u onder andere bijhoudt welke persoonsgegevens werden verwerkt, waarom, hoe lang ze worden bijgehouden, voor wie, aan wie ze worden overgedragen en hoe ze beschermd zijn. Dit register moet schriftelijk op de maatschappelijke zetel van het bedrijf aanwezig zijn.

Vanaf de inwerkingtreding van de verordening moeten **bedrijven met 250 of meer werknemers** een **register bijhouden van de verwerkingsactiviteiten die onder hun verantwoordelijkheid hebben plaatsgevonden**, op papier of elektronisch.

In **bedrijven met minder dan 250 werknemers** moet dit register ook worden opgesteld, maar alleen als de verwerking van persoonsgegevens een **risico kan inhouden voor de rechten en vrijheden van de betrokken personen, als de verwerking niet occasioneel gebeurt of als gevoelige gegevens worden verwerkt (zoals medische of gerechtelijke gegevens).**

Wat precies de draagwijdte is van het begrip "niet occasionele" verwerking moet nog worden verduidelijkt. Het is immers moeilijk om uit te maken wanneer een verwerking courant of occasioneel is. Volgende Privacycommissie zijn verwerkingen die niet als occasioneel worden beschouwd (en dus courant zijn) typisch verwerkingen van gegevens van klanten, personeel of leveranciers.

Een verwerking die risico's inhoudt voor de rechten en vrijheden van de betrokken personen heeft betrekking op situaties die bijvoorbeeld aanleiding kunnen geven tot discriminatie, diefstal, financieel verlies of identiteitsfraude.

Bijvoorbeeld: bij bepaalde bedrijven kunnen klanten zich registreren met een login en paswoord. Het opslaan van dat paswoord kan potentieel heel wat gevaren inhouden voor de rechten en vrijheden van de betrokken personen. Mensen gebruiken namelijk vaak hetzelfde paswoord voor uiteenlopende

[1] Het anonimiseren van informatie is een proces waarbij persoonsgegevens zo worden veranderd dat ze na de verwerking niet opnieuw identificatie mogelijk maken. Dit procedé dient onomkeerbaar te zijn, he anonieme karakter van de informatie mag achteraf niet kunnen worden ongedaan gemaakt.

[2]Pseudonimisering maakt het mogelijk om gegevens die personen rechtstreeks identificeren te scheiden van andere niet-relevante gegevens. Dit mechanisme produceert een identificatiesleutel om een link tot stand te brengen tussen de verschillende persoonsgegevens. Deze identificatiesleutels moeten veilig worden opgeslagen, met een robuuste toegangscontrole. De gegevens zijn bijgevolg niet anoniem, maar evenmin identificeerbaar. Een voorbeeld zijn de laatste vier cijfers van een Visa of MasterCard die zichtbaar blijven tijdens een online betaling.

doeleinden. Het is daarom allerminst ondenkbaar dat een hacker die het paswoord vanop uw server kan stelen dit paswoord kan gebruiken om bijvoorbeeld op een cloudservice van de betrokken persoon in te loggen om daar aan bankkaartgegevens te komen.

Om veilig en voorzichtig te werk te gaan, kan u maar beter alle verwerkingen die u uitvoert in kaart brengen. Wij adviseren u in elk geval om een register van de verwerkingsactiviteiten aan te leggen, want bij een controle kan het altijd nuttig zijn om te bewijzen dat u de privacy van uw klanten ter harte neemt en dat u op de hoogte bent van de nieuwe Europese reglementering.

Ga voor meer informatie over de inhoud en vorm van dit register naar deze websites:
http://economie.fgov.be/nl/modules/publications/general/cybersecurite-is_uw_bedrijf_er_klaar_voor.jsp en
https://www.privacycommission.be/nl/model-voor-een-register-van-de-verwerkingsactiviteiten.

Wij werken een vereenvoudigd register uit dat specifiek voor onze sector bruikbaar is en dat u binnenkort op onze website vindt.

Taak: een register opstellen

5) Informeren bij een inbreuk op de persoonsgegevens ("data breaches")

Als er zich een probleem met de gegevens voordoet, bijvoorbeeld bij een lek, verlies, diefstal of vernietiging (per ongeluk of na een niet-toegelaten binnendringing in het informaticasysteem van het bedrijf) van gegevens, dan moet de verwerkingsverantwoordelijke **binnen 72 uur nadat hij het probleem heeft opgemerkt de toezichtsautoriteit hiervan op de hoogte brengen**. Het kan *bijvoorbeeld gaan om: een gestolen laptop waarop zich persoonsgegevens bevonden of een e-mail met persoonsgegevens die per ongeluk naar het verkeerde adres werd gestuurd.*

De verwerkingsverantwoordelijke dient ook **de betrokken personen zo snel mogelijk te informeren** over de inbreuk op hun persoonsgegevens wanneer zij een belangrijk privacyrisico lopen. De inbreuk kan *bijvoorbeeld leiden tot identiteitsdiefstal, discriminatie, aantasting van hun reputatie, financieel verlies, enz.*

Taak: een crisisplan en een te volgen protocol opstellen

V. Wanneer bent u "accountable"? Strengere documentatieverplichting

Het principe van *accountability* houdt in dat u zich niet mag beperken tot het naleven van de principes en verplichtingen van de GDPR, maar dat u ook met kunnen aantonen dat u ze naleeft. Het is met andere

woorden een verplichting tot transparantie en verifieerbaarheid ten opzichte van de overheid. Concreet betekent dat dat u uw acties uitgebreid moet documenteren.

Vroeger volstond het om aan de Privacycommissie elke gegevensverwerking aan te geven. In de praktijk deden veel bedrijven deze aangiftes niet. Het systeem is nu dus veranderd.

Nu moet u kunnen aantonen dat u technische en organisatorische maatregelen hebt genomen die de naleving van de reglementering garanderen. U dient deze maatregelen te documenteren om aan te tonen dat u de nodige analyses hebt uitgevoerd, dat u aangepaste hulpmiddelen gebruikt, enz.

Een voorbeeld: Het volstaat niet om te verklaren "ik heb software aangekocht". U dient uit te leggen waarom u eerder een bepaald programma dan een ander hebt gekocht. En u dient de opvolging door middel van updates aan te tonen.

Gedragscharters, een governance-systeem, certificaties, enz. kunnen eveneens aantonen dat de ondernemer alles in het werk stelt voor de naleving en alle nodige maatregelen neemt.

Taak: aangepaste acties in deze zin ondernemen en elke actie documenteren

Vevolgens voert de verordening twee nieuwe principes in die u dient na te leven: de gegevensbescherming door ontwerp (**"Privacy By Design"**) en gegevensbescherming door standaardinstellingen (**"Privacy By Default"**).

Enerzijds komt *privacy by design* erop neer dat u vanaf het ontwerpen van een nieuw product, een nieuwe dienst of een nieuw project rekening dient te houden met de privacy van uw klanten. U dient dus producten en diensten te ontwikkelen die door hun aard zelf de privacy respecteren. *Een voorbeeld*: *vanaf het begin gegevens pseudonimiseren of het aantal gegevens beperken.*

Anderzijds bestaat *privacy by default* erin dat u er spontaan voor zorgt dat de privacy van uw klanten wordt gerespecteerd en dat u niet wacht tot die u dat uitdrukkelijk vragen. De bescherming van de privacy moet dus altijd in de grootst mogelijke mate worden gerespecteerd. U dient bij de gegevensverwerking rekening te houden met de specifieke doelstelling van een bepaalde verwerking. *Een voorbeeld: de standaardinstellingen van een website dienen niet toegankelijk gemaakt te worden voor een onbeperkt aantal individuen (sociale media).*

Taak: controleer de parameters die u bij elke verwerking toepast

Iedereen die persoonsgegevens verwerkt staat garant voor de confidentialiteit, beschikbaarheid en integriteit van de gegevens. Op basis van het register moet voor iedere verwerking van de gegevens een risico-analyse worden uitgevoerd. U kunt zelf kolommen toevoegen aan uw register en daarin specifieke risico's oplijsten samen met eventuele preventieve maatregelen die u genomen hebt.

Bij zo'n risico-anlyse dient u zich de volgende vragen te stellen:

- Indien u werkt met papieren dossiers, liggen die dan gewoon op uw bureau of zijn ze opgeborgen in een kast? Is die kast gesloten? Wie heeft er toegang toe?

- Indien u digitaal werkt, is uw computer dan beschermd met een paswoord? Wie kent dat paswoord? Worden de persoonsgegevens opgeslagen in een afgeschermde map beschermd met een paswoord? Laat ik mijn computer soms onbeschermd achter in de wagen?
- Indien u met een server werkt, wie heeft daar dan toegang toe? Is het nodig dat al mijn personeel daar toegang toe heeft? Maakt u back-ups? Waar zijn die dan opgeslagen?
- Indien u gegevens op een cloud opslaat, waar bevinden die zich dan en wie heeft er toegang toe? Heb ik van mijn dienstverlener voldoende garanties met betrekking tot gegevensbescherming gekregen?
- Indien u gegevens van bewakingscamera's opslaat, worden die dan bewaard? Wie kan die bekijken en onder welke voorwaarden?

Bijvoorbeeld: U beschikt over een lijst met personen die een autocarreis naar Spanje gemaakt, hebben. Eén van uw medewerkers heeft toegang tot de lijst en herkent de naam van zijn buur. Hij weet dat zijn buurman arbeidsongeschikt is en geen toestemming heeft om de woning te verlaten. Uw werknemer zou die informatie kunnen misbruiken om zijn buurman af te persen. Daarom mag deze lijst slechts beschikbaar zijn voor de mensen die de gegevens effectief nodig hebben in de uitoefening van hun functie. Ten einde dergelijke situatie te verkomen moet u anticiperen en de mogelijkheid van misbruik verhinderen. Dat is het doel van de risico-analyse.

Naast deze klassieke risico-analyse legt de GDPR nog meer verplichtingen op aan bedrijven/organisaties die bepaalde types van gegevens verwerken of waarbij gegevensverwerking een hoofddoel van het bedrijf vormt. Men spreekt in de verodening opnieuw over verwerkingen die risico's in houden voor de rechten en vrijheden van individuen zonder dit verder te specifiëren. Er worden enkele voorbeelden gegeven, zo heeft men het over systematische observatie van gegevens of grootschalige verwerking van gevoelige gegevens. In bepaalde gevallen moet men een formele risico-analyse maken en die presenteren aan de Privay Commissie.

Taak: ga vóór elke verwerking na of het nodig is om een impactanalyse uit te voeren

VI. Welke rechten hebben de betrokken personen?

De verordening herneemt de rechten die reeds in de richtlijn werden opgesomd en voegt er twee nieuwe aan toe: het recht op vergetelheid en het recht op overdraagbaarheid van de gegevens. Bij elk recht horen voorwaarden. U beschikt over een termijn van een maand om te reageren op een aanvraag.

Recht op inzage: De betrokken persoon heeft het recht om u op elk moment te vragen of u gegevens over hem hebt verzameld. Als dat het geval is, moet u deze persoon bepaalde inlichtingen kunnen geven: over welke gegevens gaat, aan wie werden deze gegevens doorgegeven, hoe lang worden ze bewaard en welke rechten heeft de persoon. Hij kan u ook vragen om hem een kopie van zijn gegevens in elektronisch formaat te bezorgen.

Recht op rectificatie: Op gewoon verzoek van de betrokkene dient u op elk ogenblik onjuiste of onvolledige gegevens te kunnen verbeteren of aanvullen.

Recht op beperking van de verwerking: In sommige gevallen kan de betrokken persoon vragen om de verwerking van zijn gegevens te beperken. Dit betekent dat de betrokken gegevens moeten "gemarkeerd" zijn in uw informaticasysteem en dat uw bedrijf ze gedurende een bepaalde periode niet meer mag gebruiken.

Recht op gegevenswissing (of 'recht op vergetelheid'): In bepaalde, door de verordening opgesomde gevallen heeft de betrokken persoon het recht om te eisen dat zijn gegevens zouden worden gewist. Het volstaat daarvoor dat hij zijn toestemming herroept en er geen andere wettelijke grond voor de verwerking is. In dat geval bent u verplicht om de gegevens te wissen binnen een redelijke termijn. *Een voorbeeld: op basis van het recht op vergetelheid kan men Google vragen om elke link te verwijderen die verwijst naar persoonsgegevens die online staan.* Maar er bestaan uitzonderingen op deze verplichting.

Recht op overdraagbaarheid van gegevens: Als de gegevensverwerking geautomatiseerd is en steunt op de toestemming van de persoon of als ze noodzakelijk is voor de uitvoering van een overeenkomst, dan kan de betrokken persoon u vragen om hem zijn gegevens te bezorgen "in een gestructureerde, gangbare en machineleesbare vorm". In bepaalde gevallen kan hij de verwerkingsverantwoordelijke zelfs vragen om de gegevens aan de nieuwe verwerkingsverantwoordelijke te bezorgen. *Een voorbeeld: een Facebook-gebruiker zou kunnen vragen om al zijn gegevens aan een ander sociaal medium te bezorgen of een klant van energiebedrijf Luminus zou kunnen vragen om zijn gegevens aan Engie te bezorgen. Een gebruiker van een e-maildienst zou kunnen vragen om alle e-mails die hij ontvangen en verstuurd heeft in een digitaal formaat te ontvangen, alsook de contactenlijst die hij heeft samengesteld.*

Het recht op overdraagbaarheid van gegevens heeft tot doel om personen opnieuw een bepaalde controle over hun gegevens te geven. Dit is de gecombineerde toepassing van de principes van toegankelijkheid, transparantie en wissing van gegevens. Het is duidelijk dat het recht op overdraagbaarheid technische implicaties heeft.

Taak: protocols uitwerken om binnen de termijn te voldoen aan aanvragen

VII. Wanneer moet men een functionaris voor gegevensbescherming aanstellen?

De GDPR geeft een belangrijke rol aan een nieuwe speler inzake de bescherming van persoonsgegevens: de functionaris voor gegevensbescherming, in het Engels aangeduid met Data protection officer (of DPO).

In een aantal gevallen is de aanstelling van een DPO verplicht, zowel voor de verwerkingsverantwoordelijken als voor de verwerkers, met name:

- wanneer zij een overheidsinstantie of overheidsorgaan zijn;

- als hun hoofdactiviteit ze ertoe brengt om een regelmatige en stelselmatige observatie op grote schaal van de betrokkenen uit te voeren;

- als hun hoofdactiviteit ze ertoe brengt om (nog steeds grootschalig) zogeheten "bijzondere" categorieën van gegevens of persoonsgegevens met betrekking tot strafrechtelijke veroordelingen en strafbare feiten te verwerken.

De gevallen waarin de aanstelling van een DPO verplicht is, zijn in vrij ruime bewoordingen omschreven en vatbaar voor interpretatie: hoe zit het onder andere met het begrip "regelmatige en systematische observatie" van de betrokken personen of vanaf wanneer gaat het om "grootschalige" verwerking? Deze begrippen zullen door de Privacycommissie moeten worden geïnterpreteerd.

De functionaris kan een personeelslid, maar ook een onafhankelijke dienstenleverancier zijn. Hij heeft de opdracht om te adviseren, te controleren en als aanspreekpunt te dienen voor de toezichtsautoriteit. Hij controleert dus binnen het bedrijf of de gegevens worden verwerkt zoals de reglementering het voorschrijft. Deze persoon moet in staat zijn om **onafhankelijk op te treden binnen het bedrijf.** Hij of zij rapporteert aan het hoogste managementniveau en kan niet ontslagen worden wegens redenen die verband houden met de uitoefening van de functie.

De DPO moet een specialist in de wetgeving op de privacybescherming zijn, maar ook grondig het bedrijf kennen, de werking ervan en de markt waarop het actief is. Belangenconflicten dienen vermeden te worden. *Een voorbeeld: in de meeste gevallen kan een IT-verantwoordelijke niet tegelijk ook DPO zijn, want dan zou hij de beschermingsmaatregelen moeten controleren die zijn eigen team heeft geïnstalleerd.*

De GDPR vermeldt niet over welk diploma of over welke certificaten een DPO moet beschikken en evenmin welke kennis en ervaring voorrang zouden moeten krijgen.

Ook andere bedrijven, die hiertoe niet verplicht zijn, mogen een DPO aanstellen. Dit is in elk geval sterk aan te raden.

Taak: indien nodig een DPO aanstellen

VIII. Conclusie

KMO's denken nog te vaak - ten onrechte - dat dit hen niet aangaat, omdat zij niet het doelwit van hackers zouden zijn. Maar wat gisteren misschien correct was, geldt vandaag niet meer. Hackers hebben nu immers meer belangstelling voor KMO's, want grote ondernemingen, die reeds aanvallen te verduren kregen, hebben maatregelen genomen, KMO's vaak nog niet.

Naleving van de GDPR betekent dat u een aantal maatregelen moet nemen en procedures invoeren en dat u hiervoor tijd, mensen en middelen moet vrijmaken. Deze obstakels zijn niet onoverkoombaar. Bekijk deze nieuwe reglementering als een commercieel of concurrentievoordeel waar u mee kan uitpakken bij uw klanten en partners. De vele mogelijkheden om klacht tegen u in te dienen en de maatregelen en

sancties die tegen u kunnen worden uitgesproken, zouden u moeten overtuigen om de reglementering volledig na te leven.

Ook als u alle mogelijke firewalls en virusscanners gebruikt, dient u nog de wettelijke verplichtingen na te leven. Dit is een kans om informatie en uw ICT beter te beschermen en een beheermethode in te voeren.

Wij zijn natuurlijk steeds tot uw beschikking voor alle vragen die u zich zou kunnen stellen! Aarzel niet om contact met ons op te nemen.