De GDPR in 10 stappen

Stap 3- Breng uw beveiligingsmaatregelen in kaart

De GDPR in 10 Stappen

Stap 3 – Breng uw beveiligingsmaatregelen in kaart

Inleiding

In de vorige 2 stappen heeft u in kaart gebracht welke gegevens u juist verwerkt en hoe u die verwerkt. In stap 3 gaan we meer in detail bekijken op welke manier u de gegevens die u verwerkt, beveiligt. Persoonsgegevens moeten immers beschermd worden tegen ongeoorloofde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.

De GDPR verplicht u als verwerkingsverantwoordelijke en de verwerker om in dat verband 'passende technische en organisatorische maatregelen te nemen'. Bij de beoordeling van het passende beveiligingsniveau wordt rekening gehouden met de risico's van de verwerking, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

TO DO

Vooraleer u de vragen hieronder beantwoordt, maakt u best een overzicht van de volgende twee vragen:

- Waar houdt u uw gegevens bij? Het kan zijn dat u bepaalde gegevens bijhoudt in een Excel of Acces bestand, maar het kan ook zijn dat u gegevens bijhoudt in een Cloud – oplossing of specifieke software (mailingprogramma's, boekhoudpakketten,…), of gewoon op papier.

- Controleer daarnaast ook wie juist toegang heeft tot die gegevens. Als u gegevens bijhoudt op papier; wie kan dan allemaal in de kast waar die papieren bewaard worden? Wie heeft een account op het boekhoudprogramma waar u mee werkt?

Beveiliging in functie van …

Welke beveiligingsmaatregelen u dus precies moet nemen, hangt af van een aantal factoren:

- ✓ De risico's die aan de verwerking verbonden zijn:
  Hoe groter het risico, hoe beter de beveiliging moet zijn. Die risico's hangen dan weer af van de omstandigheden van de verwerking: de aard, omvang, context en doeleinden van de verwerking.
  - Zo zal bijvoorbeeld 'controle op online communicatiemiddelen bij werknemers', of 'track & trace' meer risico's inhouden voor de betrokkenen dan het doeleinde 'klantenbeheer' en dus een betere bescherming vragen.
  - hou er ook hier weer rekening mee dat de verwerking van gevoelige gegevens een hoger beschermingsniveau zal vragen. Desgevallend neemt u contact op met een IT-leverancier om te weten welke mogelijkheden er zijn.

- Ook de omvang van de verwerking speelt een rol. Of er sprake van enkele honderden klanten dan wel van tienduizenden klanten zal mee de te nemen maatregelen bepalen.

✓ De stand van de techniek:
Bij het bepalen van de maatregelen om de risico's te beheren en beheersen moet rekening worden gehouden met de stand van de techniek. Dat betekent dat wat vandaag een goede beveiligingsmaatregel is, dat morgen niet meer noodzakelijk is.

✓ De uitvoeringskosten:
Bij het bepalen van de maatregelen om de risico's te beheren en beheersen mag rekening worden gehouden met de uitvoeringskosten. Die kosten worden mee bepaald door de context. Zo is het duidelijk dat de kosten inzake beveiliging voor een gemiddelde KMO heel wat lager zullen zijn dan de kosten voor de beveiliging van een (middelgroot) ziekenhuis. Dat betekent ook dat niet noodzakelijk altijd de duurste oplossing moet worden gekozen.

Wat met certificeringsnormen, zoals ISO 27000?

Inzake beveiliging kan een beroep worden gedaan op bepaalde certificeringsnormen, zoals ISO 27000. Ondernemingen die deze certificering kunnen voorleggen, mogen ervan uitgaan dat de genomen beveiligingsmaatregelen passend zijn.
Hou er wel rekening mee dat (op dit ogenblik) deze certificeringsnormen vooral gericht zijn op de technische aspecten van informatieveiligheid en niet zozeer op het ruimere kader van de bescherming van persoonsgegevens. Dat betekent dat ze slechts een gedeeltelijke oplossing bieden op het vlak van de (globale) naleving van de GDPR.

Praktisch – voorbeelden van beveiligingsmaatregelen

Hieronder worden een aantal voorbeelden gegeven van mogelijke beveiligingsmaatregelen. Zoals gezegd, volstaat het niet om deze lijst gewoon over te nemen: u moet steeds in functie van de gegevens die u verwerkt, nagaan welke maatregelen passend zijn.

Technische maatregelen

- Gegevens via een algoritme tijdelijk onleesbaar maken ('versleuteling')
- Toegang tot gegevens enkel mogelijk maken via een combinatie van 2 of meer persoonlijke elementen, zoals gebruikersnaam + paswoord of identiteitskaart + paswoord; …) ('dubbele authenticatie')
- Periodieke back-ups
- Logging (het bijhouden van wie welke gegevens opzoekt)
- Firewalls
- Virusscanners
- Software die attendeert op het dreigend verstrijken van een bewaartermijn.
- …

Ten aanzien van bijzondere categorieën van persoonsgegevens is het zeker aangewezen om beroep te doen op bepaalde technische maatregelen zoals logging, versleuteling, dubbele authenticatie. Indien u veel gevoelige gegevens verwerkt, doet u best beroep op een IT-leverancier om de mogelijkheden te bekijken.

Organisatorische maatregelen

- Het afsluiten van de kasten waarin papieren dossiers worden bewaard
- Het afsluiten van de archiefruimte
- Het afsluiten van de gebouwen en/of de ruimtes waar zich de servers bevinden
- Een stelsel van gebruikers- en toegangsbeheer
- Een vertrouwelijkheidsverklaring die moet worden ondertekend door alle medewerkers die persoonsgegevens (mogen) verwerken
- Het sensibiliseren van medewerkers (creëren van informatieveiligheidsbewustzijn) via allerlei richtlijnen
    - Richtlijnen over het opnemen van persoonsgegevens op draagbare informatiedragers zoals USB-stick of laptops
    - Richtlijnen over het afdrukbeleid
    - Richtlijnen over het meedelen van gegevens aan derden
    - Richtlijnen over de omgang met vragen om informatie
- Het opstellen van duidelijke procedures voor het tijdig en doeltreffend behandelen van informatiebeveiligingsincidenten
- …

Beperking interne toegang als onderdeel van beveiliging

Elke onderneming moet ervoor zorgen dat enkel die medewerkers die de gegevens nodig hebben voor de uitoefening van hun taken of voor de behoeften van hun dienst, er toegang toe hebben. Dit wordt omschreven als het beginsel “need to know”.

Dit beginsel heeft een dubbele reikwijdte, zowel personeel als qua voorwerp.

- Eerst en vooral geeft het aan wie toegang mag hebben.
- daarnaast bepaalt het ook tot welke gegevens die personen toegang mogen hebben.

Bijvoorbeeld: de medewerkers van de dienst “loonadministratie” moeten (mogen) geen toegang hebben tot de detailgegevens van de evaluatie of afwezigheid van een werknemer. Het volstaat dat zij toegang hebben tot het resultaat of feit als zodanig om hun taken te kunnen uitoefenen.

Gegevens doorgeven aan derden

Beveiliging betekent niet alleen beperking van de interne toegang (eigen medewerkers), maar ook beperking van personen buiten de onderneming die toegang krijgen tot de gegevens. U moet er met andere woorden zorg voor dragen dat gegevens enkel worden meegedeeld of doorgegeven aan derden die daartoe gerechtigd zijn.
Als gegevens ter beschikking worden gesteld van derden die daartoe niet gerechtigd zijn, is of kan er sprake zijn van een beveiligingsinbreuk of een gegevenslek.

In de volgende gevallen zal het doorgeven van gegevens aan een derde geen probleem stellen:

- ✓ De doorgifte wordt voorgeschreven of opgelegd door de wetgever
- ✓ De doorgifte gebeurt aan een verwerker die passend is en waarmee een verwerkersovereenkomst is gesloten

- ✓ De doorgifte is verenigbaar met het doeleinde waarvoor de gegevens oorspronkelijk zijn verzameld en/of verkregen
- ✓ De doorgifte is gesteund op de uitdrukkelijke toestemming van de betrokkenen waar het over gaat.

Indien u gegevens doorgeeft aan derden, en u zich niet op één van deze gronden kan beroepen, kan het nuttig zijn om de doorgifte als een afzonderlijk 'doeleinde' op te nemen.

Bijvoorbeeld: een onderneming die zijn klantenbestand wil verkopen of verhuren aan een andere onderneming, moet hiervoor de uitdrukkelijk toestemming hebben van de betrokken klanten.

Let op: doorgifte van gegevens aan derden is in principe verboden in de volgende gevallen:

- De verantwoordelijke is onderworpen aan een beroepsgeheim of vertrouwelijkheidsplicht
- De doorgifte is verboden op grond van de wet- of regelgeving
- De doorgifte is niet verenigbaar met het doeleinde waarvoor de gegevens oorspronkelijk zijn verzameld en/of verkregen en kan niet worden gesteund op de uitdrukkelijke toestemming van de betrokkenen.

Doorgifte aan derde landen

De GDPR geldt enkel voor landen die behoren tot de Europese Economische Ruimte (EER)[1]. Om de veiligheid van persoonsgegevens te waarborgen, bepaalt de GDPR echter dat u persoonsgegevens enkel in bepaalde gevallen kan doorgeven aan landen buiten deze EER (men spreekt dan van 'derde landen').

U zal misschien denken dat dit een 'ver van uw bed' – show is, en dat u geen gegevens doorgeeft aan landen buiten de EER. Nochtans doet u dat misschien sneller dan u denkt. Indien u heeft vastgesteld dat u bepaalde gegevens bijhoudt in een Cloud-oplossing of een specifieke software, is het niet gegarandeerd dat de leverancier van die oplossing zijn servers binnen de EER heeft staan. Staan die servers buiten de EER, dan geeft u wel degelijk gegevens door aan een derde land.

U doet er dan ook best aan om aan deze leveranciers na te vragen waar zij hun servers hebben staan. Van grote internationale spelers zal u waarschijnlijk geen antwoord krijgen, maar zelf moeten gaan zoeken in hun privacybeleid of algemene voorwaarden[2].

Indien u vaststelt dat er effectief een doorgifte is aan een derde land (bijvoorbeeld omdat de servers buiten de EER liggen), dan moet u een aantal zaken nagaan:

1) Voor 12 landen heeft de EU beslist dat zij veilig genoeg zijn om gegevens aan door te geven zonder dat u daar toestemming voor moet vragen aan de Gegevensbeschermingsautoriteit[3]. U vindt deze landen op https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en.
2) Voor wat betreft de VS moet u nagaan of uw leverancier voorkomt op de Privacy Shield list. Is dat het geval, dan mag u gegevens doorgeven zonder dat u daar toestemming voor moet vragen aan de Gegevensbeschermingsautoriteit.

Kan u geen beroep doen op één van deze twee mogelijkheden, dan mag een doorgifte aan een derde land enkel gebeuren als u extra maatregelen neemt. Die maatregelen zijn echter heel technisch en ingewikkeld.

[1] Dit zijn de Lidstaten van de E.U., aangevuld met IJsland, Noorwegen en Liechtenstein.
[2] Voor Facebook bijvoorbeeld: https://www.facebook.com/about/privacyshield
[3] Dit is de nieuwe naam van de vroegere 'privacycommissie'.

Omdat ze enkel nodig zullen zijn in specifieke situaties, geven we ze mee als bijlage aan deze stap. Als u echter beroep kan doen op één van de twee bovenstaande gronden (lijst van 12 landen of de Privacy Shield List), kan u de bijlage gewoon negeren en naar Stap 4 gaan.

Checklist

- ❑ Ik heb nagekeken of mijn beveiliging voldoende is, rekening houdend met het soort gegevens, de kostprijs, en de mogelijke risico's.
- ❑ Voor gevoelige gegevens voorzie ik een extra beveiliging.
- ❑ Ik weet welke medewerkers toegang hebben tot welke gegevens, en beperk de toegang tot de medewerkers die dat nodig hebben.
- ❑ Ik heb nagekeken of ik gegevens doorgeef aan derde landen, en of ik desgevallend de nodige waarborgen heb inzake veiligheid.

Bijkomende maatregelen bij doorgifte aan derde landen

Wat hieronder staat geldt enkel wanneer u gegevens doorgeeft aan landen buiten de EER die niet voorkomen op de lijst van 12 landen, of aan een Amerikaans bedrijf dat niet voorkomt op de Privacy Shield List!

In dat geval mag een doorgifte alleen plaatsvinden mits de verwerkingsverantwoordelijke of verwerker passende waarborgen bieden én de betrokkenen over afdwingbare rechten en doeltreffende rechtsmiddelen beschikken.
Die passende waarborgen kunnen worden geboden door een aantal instrumenten die op het niveau van de Europese Unie zijn uitgewerkt, zoals:

- Bindende bedrijfsvoorschriften (of Binding Corporate Rules).
  Dit instrument is bedoeld voor doorgiftes van persoonsgegevens tussen de leden van een concern of groepering van onderneming die gezamenlijk een economische activiteit uitoefenen.
- Standaardbepalingen inzake gegevensbescherming die door de Europese Commissie zijn vastgesteld. Hieronder vallen met name de overeenkomst voor doorgifte door een verantwoordelijke voor de verwerking naar verantwoordelijke voor de verwerking (model 2004/915/CE (ENG) en de overeenkomst voor doorgifte door een verantwoordelijke voor de verwerking naar een verwerker (model 2010/87/EU (ENG).
- Standaardbepalingen inzake gegevensbescherming die door een (nationale) toezichthoudende autoriteit zijn vastgesteld en door de Europese Commissie zijn goedgekeurd.
- Desgevallend, een goedgekeurde gedragscode of een goedgekeurd certificeringsmechanisme, samen met bindende en afdwingbare toezeggingen van de verwerkingsverantwoordelijke of verwerker in het derde land om de passende waarborgen toe te passen

Het zal niet altijd evident zijn voor een KMO om met de ontvanger in een derde land een instrument af te sluiten dat passende waarborgen biedt. Indien inderdaad blijkt dat zo'n instrument niet mogelijk is, kan een doorgifte plaatsvinden onder één van de twee volgende mogelijkheden:

Mogelijkheid 1: Specifieke afwijkingen

Het zal niet altijd evident zijn voor een KMO om met de ontvanger in een derde land een instrument af te sluiten dat passende waarborgen biedt.
Als de voorgaande trap niet kan worden toegepast, kan een doorgifte plaatsvinden mits een van de volgende voorwaarden is vervuld (waarbij we er van uit gaan dat geval de doorgifte niet regelmatig en stelselmatig plaats vindt, maar eerder incidenteel (of occasioneel) en niet repetitief):

- Uitdrukkelijk toestemming (na informatie over de risico's die eraan verbonden zijn)
- Uitvoering van een overeenkomst waarbij de betrokkene partij is of nemen van precontractuele maatregelen op verzoek van de betrokkene
- Sluiting of uitvoering van een in het belang van de betrokkene gesloten overeenkomst tussen de verwerkingsverantwoordelijke en een andere natuurlijke persoon of rechtspersoon
- Instelling, uitoefening of onderbouwing van een rechtsvordering
- Bescherming van de vitale belangen van de betrokkene of andere personen, indien de betrokkene lichamelijk of juridisch niet in staat is zijn toestemming te geven

Mogelijkheid 2: dwingende gerechtvaardigde belangen

Als de voorgaande stappen niet mogelijk zijn en enkel dan, kan de doorgifte mogelijks worden gebaseerd op de dwingende gerechtvaardigde belangen van de verwerkingsverantwoordelijke.
Voorwaarden zijn:

- Doorgifte is niet mogelijk op basis van de voorgaande trappen
- Doorgifte is niet mogelijk op basis van adequaatheidsbesluit
- Doorgifte is niet mogelijk op basis van passende waarborgen
- Geen van de specifieke afwijkingen is mogelijk
- Doorgifte is niet repetitief
- Doorgifte betreft een beperkt aantal betrokkenen
- Doorgifte is noodzakelijke voor dwingende gerechtvaardigde belangen verantwoordelijke die niet ondergeschikt zijn aan belangen of rechten en vrijheden van betrokkene
- Verwerkingsverantwoordelijke heeft alle omstandigheden in verband met doorgifte beoordeeld en op basis daarvan passende waarborgen geboden

Bijkomend maatregelen zijn

- Verantwoordelijke moet de toezichthoudende autoriteit informeren
- Verantwoordelijke moet de betrokkene informeren, in het bijzonder over de doorgifte en de dwingende gerechtvaardigde belangen

Deze voorwaarden en maatregelen geven aan dat de toepassing van deze mogelijkheid eerder uitzonderlijk zal zijn.