Stappenplan voor de uitvoering van de AVG

Dit document moet samen met het werkdocument « GDPR: hoe alle voorschriften naleven? » gelezen worden. Welke zijn de eerste stappen om aan de nieuwe AVG (Algemene Verordening Gegevensbescherming - GDPR) te voldoen? Dit document probeert toe te lichten hoe de nieuwe reglementering uitgevoerd moet worden.

1. Een inventaris maken van alle gegevens en ze in het register opnemen

Een van de prioriteiten, en daar zijn alle waarnemers het over eens, is de noodzaak voor elke onderneming, ongeacht haar grootte of activiteitenterrein, om alle gegevens te inventariseren.

Voor elke onderneming betekent dit concreet een lijst opmaken van alle contacten van wie ze persoonlijke gegevens verzamelt, opslaat en gebruikt: klanten, reizigers, prospects, medewerkers, dienstverleners, leveranciers…

Het is ook te zien welke soort gegevens je verzamelt: identificatiegegevens (naam, adres, telefoonnummer…), locatiegegevens, facturatiegegevens, gevoelige informatie…?

Enkele mogelijk nuttige vragen om te stellen:

1) Welke gegevens bewaar je en waar sla je ze op?

2) Hoe kom je aan die gegevens? Van de mensen zelf of via derden?

3) Wie kan die gegevens raadplegen?

4) Weet je op welke datum de gegevens verzameld en op welke datum ze gewijzigd werden, en door wie?

5) Maak je al gebruik van *opt-in* (toelating geven) en *opt-out* (uitschrijven) ?

6) Speel je gegevens door aan derden? En zo ja, met welk doel?

7) Om welke reden(en) bewaar je die gegevens? En voor hoelang?

Zo'n eerste, niet-exhaustieve evaluatie helpt om te bepalen hoeveel werk je zult hebben om je met de bepalingen van dat nieuwe reglement in overeenstemming te brengen.

Als alle gegevens eenmaal in kaart zijn gebracht, zal je ze kunnen opnemen in het register. Op onze website vind je een model van zulk een register.

2. Weten wanneer je verantwoordelijke of onderaannemer bent

Waarom dat onderscheid? Omdat je rol en je aansprakelijkheden in die twee gevallen verschillen.

Wanneer je de verantwoordelijke voor de verwerking bent, haal je gegevens rechtstreeks binnen. Als onderaannemer krijg je gegevens van een verwerkingsverantwoordelijke. Voor meer informatie over die twee rollen: zie het document « GDPR: hoe alle voorschriften naleven? ».

Een voorbeeld: Wanneer je rechtstreeks gegevens verzamelt via een contactformulier op je website, ben je de ***verwerkingsverantwoordelijke****. Zoals wanneer een klant rechtstreeks met je in contact komt om naar de prijzen voor een reis te vragen.*

Wanneer je schoolvervoer uitvoert, ontvang je de gegevens van de leerlingen door toedoen van De Lijn of de TEC. In dat geval ben je ***onderaannemer (verwerker).***

Verwerkingsverantwoordelijke

- Wanneer je een onderaannemer kiest, moet je je ervan vergewissen dat hij zijn verplichtingen inzake gegevensbescherming kent en van plan is die verplichtingen ook na te komen;

- Wanneer je een opdracht aan je onderaannemer toevertrouwt, moet je die goed omschrijven;

- Je moet je er ook van vergewissen of het contract correct uitgevoerd wordt door de onderaannemer. Een langetermijncontract zal een geregelde controle vereisen.

Als onderaannemer

- Wanneer je onderaannemer bent, moet je gegevens conform de instructies van de verantwoordelijke gebruiken en de opgelegde vertrouwelijkheid respecteren;

- Er moet een gepaste veiligheid geïnstalleerd worden ter bescherming van de gegevens die je toevertrouwd werden;

- Bij een gegevenslek moet je de verwerkingsverantwoordelijke onmiddellijk op de hoogte brengen. Jij bent niet degene die de Privacy-commissie of de betrokken personen verwittigt;

- Wanneer de opdracht beëindigd is of de bewaartermijn afloopt, moeten de gegevens definitief verwijderd worden. Je moet die verwijdering bewijzen;

- De gegevens mogen enkel naar derden doorgespeeld worden met toestemming van de verantwoordelijke.

→ Om je te helpen, vind je modellen van clausules om toe te voegen in je contracten in de toolbox op onze website.

3. Geldige toestemming vragen

De vraag om toestemming is heel belangrijk en weinig veranderd met het nieuwe reglement. Het is een sleutelelement, want mensen moeten maximale controle hebben over de verwerking van hun gegevens.

Volgens de AVG moet de toestemming vrij, specifiek, op nuttige informatie gebaseerd en eenduidig zijn. De betrokkene moet ook duidelijke informatie gekregen hebben over de verwerking van zijn of haar gegevens.

Je moet een geldige toestemming vragen voor alle nieuwe gegevens die je verzamelt, maar ook voor alle gegevens die je al zonder toestemming verzameld hebt. Dat geldt natuurlijk niet voor gegevens die verzameld werden omdat:

- ze nodig zijn voor het uitvoeren van een contract;

- er een wettelijke verplichting geldt;

- het algemeen nut dat vereist;

- er een gewettigd belang speelt;

- er levensbelang op het spel staat.

Op grond van het *accountability*-principe moet een bewijs van de verkregen toestemming bewaard worden. Het zal hierbij gaan om een schriftelijk bewijs, hetzij digitaal, hetzij op papier. Zonder dat bewijs zal de toestemming niet als geldig beschouwd worden. De AVG beschrijft niet nader welke middelen gebruikt moeten worden. Er moet een mechanisme in werking gesteld worden waarmee het bewijs van de toestemming gemakkelijk teruggevonden kan worden.

4. Aan je IT-veiligheid denken

Je moet aangeven hoe en met welke platformen de gegevens beschermd worden tegen aanvallen van buitenaf, maar ook een spoor bewaren van de plaats waar al die gegevens uiteindelijk terechtkomen en waar de kopieën opgespoord kunnen worden. De veiligheidsaspecten van de gegevens moeten geanalyseerd worden: codering, pseudonimisering, beveiliging van de gegevensstromen, beveiligde toegang via een log-in en een paswoord…

Enkele vragen die je jezelf moet stellen:

1) Ik heb een antivirusprogramma, maar is het up-to-date?

2) Is mijn smartphone, waarop ik ook gegevens van mijn onderneming raadpleeg, correct geconfigureerd?

3) Ik maak back-ups, maar doe ik dat juist?

4) Heb ik een middel om een virus in een mail op te sporen?

5) Vergrendelen mijn werknemers hun werksessie wanneer ze hun werkpost verlaten?

6) Wanneer een werknemer mijn bedrijf verlaat, kan ik dan zijn toegang(en) tot het bedrijfsnetwerk snel afsluiten?

Neem voor al die aspecten contact op met je leverancier, je consultant of je IT-afdeling.

5. Je contracten en documenten aanpassen

Je bestaande contracten moeten gecontroleerd worden. Staan er clausules in over de bescherming van gegevens? Zo ja, zijn die nog up-to-date? Als er nog geen dergelijke clausules in staan, moeten er toegevoegd worden.

Elke contractonderhandeling zal vanaf heden aspecten moeten bevatten aangaande het beheren van persoonlijke gegevens. Vergewis je er nu al van of je met veilige partners werkt.

Er zullen ook nog verschillende documenten aangepast en/of opgemaakt moeten worden:

- **privacy beleid**: verplicht document waarin je de mensen informeert over de manier waarop je hun gegevens verwerkt. Je vindt een model op onze website. Dit document moet gemakkelijk toegankelijk zijn. Daarom wordt aangeraden het op je website te zetten.

- **intern beleid inzake de vertrouwelijkheid:** document waarin je uitlegt hoe je werknemers met de gegevens moeten omgaan bij de uitvoering van hun werk. Elementen zoals het gebruik van USB-sticks, het gebruik van een portable computer of het beheer van een mailbox (goede mailpraktijken) kunnen erin aan bod komen.

- **beleid inzake videotoezicht:** document waarin je de redenen vermeldt waarom je camera's hebt, welke beelden je bewaart, hoeveel camera's er zijn…

- **procedures in geval van gevaar voor verlies van gegevens:** je moet gegevenslekken binnen een korte termijn melden. Het is in dat verband nuttig om een schriftelijke procedure te voorzien. Een gegevenslek gaat om meer dan alleen maar een hacking. Het is ook de diefstal van een portable computer of het verlies van een USB-stick. Voor al die situaties moeten er aangepaste procedures voorzien worden zodat de gegevenslekken zo snel mogelijk gemeld worden.

- …

6. Het personeel inlichten

Ongeacht hoe groot de firma is, moet er verantwoordelijkheid worden opgenomen door één of meerdere personen die moeten zijn opgeleid en aantonen dat zij de nodige competenties hebben. Het is fout te denken dat slechts één persoon of enkele personen van de directie dat thema moeten beheersen. Abstractie maken van de bedienden houdt een risico in. Iedereen moet zich op zijn niveau bewust zijn van de implicaties en mogelijke risico's bij een slechte bescherming van de gegevens. Het personeel sensibiliseren is van primordiaal belang, zowel vóór als na de inwerkingtreding van het nieuwe reglement.