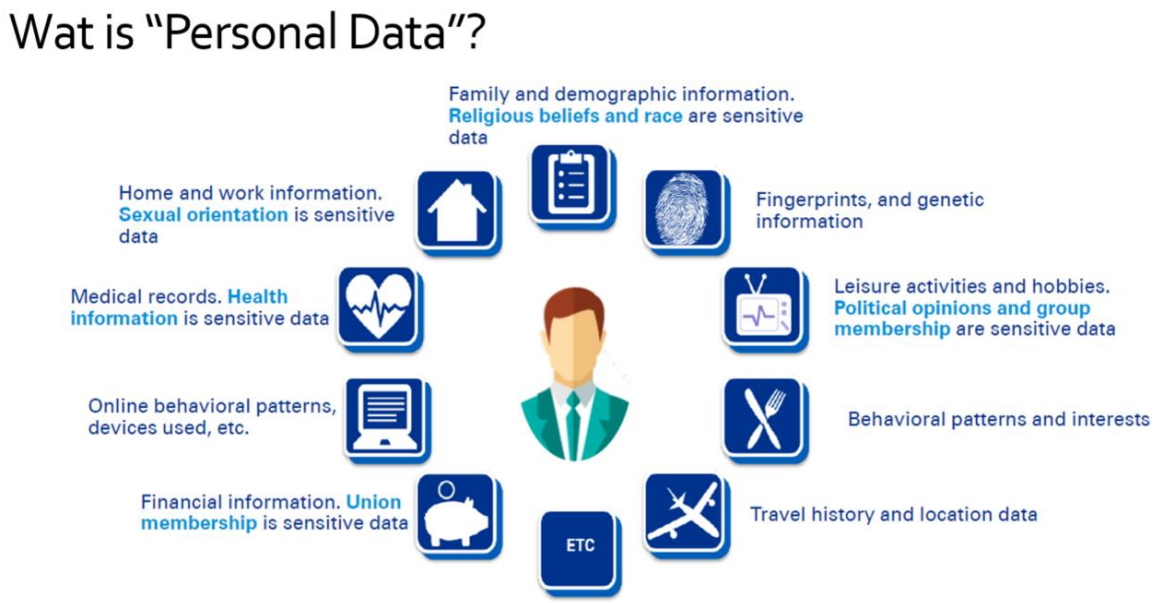
Ben jij klaar voor de nieuwe privacy wetgeving?

Bereid je nu al voor op de strengere verplichtingen omtrent registratie van persoonsgegevens. Naast de al langer bestaande Wet Bescherming Persoonsgegevens, is sinds januari 2016 de meldplicht datalekken van kracht. Op 25 mei 2018 worden de regels rondom persoonsgegevens nóg strakker getrokken met de nieuwe GDPR. Wat hiervan de consequenties zijn leest u hieronder.

De General Data Protection Regulation (GDPR) is de Europese verordening, omgezet in Nederlandse wetgeving, op het gebied van het verzamelen, verwerken en gebruiken van persoonsgegevens.
De GDPR is bedoeld om de privacy van Europese burgers beter te beschermen. Burgers krijgen in feite het recht om zelf te bepalen wie welke gegevens ("personal data") van ze mogen hebben en waar ze vervolgens voor gebruikt mogen worden. Een goede zaak, maar wel eentje met grote gevolgen die je als bedrijf niet mag onderschatten.



Expliciete toestemming vereist

Zo mag je niet meer zomaar allerlei persoonsgegevens verzamelen en verwerken. Je bent dan verplicht om per gebruiksdoel expliciet om toestemming te vragen. Je mag de data vervolgens alleen voor het omschreven doel gebruiken en dat moet je dan ook duidelijk en begrijpelijk omschrijven.

Voorbeeld Emailadres

Vraag je bijvoorbeeld of je een e-mailadres mag gebruiken om een maandelijkse nieuwbrief te versturen, dan heb je niet automatisch toestemming om meteen ook leuke aanbiedingen te doen.

Voorbeeld telefoonnummers

Onder de persoonlijke gegevens vallen ook telefoonnummers. Je kunt straks zonder explicite toestemming niet meer bellen (cold calling). Leg je telefoonnummers van klanten vast, dan vraag je toestemming voor het doel daarvan.

Voorbeeld Cookies

Ook voor het plaatsen van cookies is (meestal) toestemming nodig. In ieder geval informatie over het feit dat u cookies gebruikt en waarvoor.

Toestemming intrekken

Daarnaast mag iemand zijn toestemming ook weer intrekken, of kan om inzage gevraagd worden en moet je de gegevens dan in een begrijpelijk formaat kunnen aanleveren. In specifieke situaties kan zelfs geëist worden dat je iemands gegevens volledig verwijdert, het zogenaamde recht om vergeten te worden.

Herleidbare gegevens

Belangrijk om te weten, is dat de GDPR van toepassing is op alle persoonsgegevens en dat dit begrip flink wordt verruimd. Het gaat straks om alle gegevens die mogelijk tot een individuele persoon herleid kunnen worden. Denk aan een naam, IP-adres, telefoonnummer, kenteken, maar ook aan cookies en identifiers van apparaten. Als je niet aan de verplichtingen voldoet ben je strafbaar en kun je strafrechtelijk vervolgd worden. Een boete wil je echt niet riskeren, want die kunnen oplopen tot vier procent van je jaaromzet of maximaal twintig miljoen euro. Over de reputatieschade die je oploopt zullen we het maar niet hebben.

De wetgeving is van toepassing op alle Europese burgers en bedrijven, ongeacht waar hun data wordt opgeslagen. Maak je bijvoorbeeld gebruik van een clouddienst die de data mogelijk ergens buiten Europa opslaat, of een datacenter op een ander continent, dan moet je nog steeds aantoonbaar aan de verplichtingen van de GDPR voldoen.

Administratie en databescherming

Behalve dat expliciete toestemming nodig is, moet je er alles aan doen om de persoonsgegevens te beschermen. Ze mogen niet verloren gaan, beschadigd raken, door ongeautoriseerde mensen worden ingezien en ze moeten ook nog eens correct en actueel gehouden worden. Dat is een flinke administratieve last. Verder mag je geen gegevens verzamelen die je niet nodig hebt voor de omschreven doeleinden en mogen privacygevoelige gegevens niet op straat komen te liggen. Wat nu bijvoorbeeld al geldt in het kader van de meldplicht datalekken, blijft straks onder de GDPR ongeveer hetzelfde. Data protection officers zijn straks verplicht voor bedrijven met meer dan 25 medewerkers.

Per 1 mei 2018 moet je kunnen aantonen dat je aan de verplichtingen voldoet.

- Dat je expliciete toestemming hebt om bepaalde persoonsgegevens vast te leggen,
- Dat je kunt aantonen dat je deze toestemming heb ontvangen.
- Dat je er alles aan doet om deze gegevens optimaal te beschermen
- Dat je vooraf hebt uitgezocht welke acties nodig zijn mocht er onverhoopt iets misgaan.
- Dat je klanten inzicht kunt geven welke gegevens je waarvoor vastlegt.
- Dat je klantgegevens weer kunt wissen.

Gegevens in kaart brengen

Het is essentieel dat je bedrijfsbreed zorgvuldig in kaart brengt welke soorten data er allemaal verzameld, opgeslagen en verwerkt worden. Aan de hand van deze inventarisatie kun je vervolgens bepalen welke acties er uitgezet moeten worden om op tijd aan de verplichtingen van de GDPR te voldoen.

Voor welke gegevens moet je bijvoorbeeld nog toestemming vragen. Is elke datasoort alleen toegankelijk door geautoriseerde afdelingen en functionarissen. Zijn er persoonsgegevens die je niet nodig hebt en dus niet mag hebben. Kan data geaggregeerd en geanonimiseerd worden zodat het niet meer onder de GDPR valt. Worden gegevens niet te kort en ook niet te lang bewaard. Om welke

bedrijfssystemen, apparatuur van medewerkers, datacenters en cloud diensten gaat het. Maak je gebruik van externe partijen die namens jouw bedrijf privacygevoelige gegevens verwerken.

Privacy by design en privacy by default

Ook belangrijk om te weten, is dat privacy by design verplicht wordt. Alle systemen moeten zo ontworpen worden dat al vanaf de tekentafel alles aan de bescherming van de privacy wordt gedaan. Daarnaast geldt privacy by default. Dit houdt in dat als gebruikers zelf ergens privacyinstellingen kunnen aanpassen, deze standaard al de hoogste graad van bescherming moeten bieden. Je kunt dus niet alvast een paar vakjes aanvinken om jezelf meer mogelijkheden te geven, ook niet op zoiets als een inschrijfformulier.