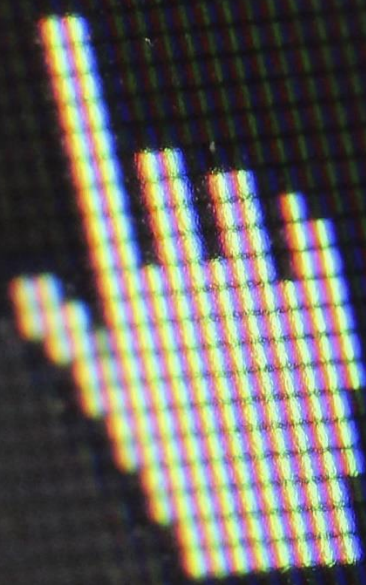


Security



HOE KUNT U ZICH VOORBEREIDEN OP DE GDPR?

Volg de 10 stappen
van de Autoriteit
Persoonsgegevens

In Nederland controleert de Autoriteit Persoonsgegevens (AP) of de huidige en toekomstige privacywetgeving wordt nageleefd. De AP heeft ook een faciliterende rol om bedrijven te ondersteunen bij de implementatie van de GDPR. Daartoe heeft de AP onder andere een 10-stappenplan opgesteld.

STAP 1 BEWUSTWORDING

Zorg ervoor dat de relevante mensen in uw bedrijf zich bewust zijn van wat de nieuwe privacyregels inhouden. Zij moeten inschatten wat de impact van de GDPR is op de huidige processen en goederen, en welke aanpassingen nodig zijn om aan de nieuwe wet te voldoen. Natuurlijk dient vervolgens iedereen binnen de organisatie op de hoogte te zijn van de nieuwe regels en werkwijze.

STAP 2 RECHTEN VAN BETROKKENEN

Onder de GDPR krijgen mensen van wie u persoonsgegevens verwerkt, zoals klanten en medewerkers, meer en betere privacy-rechten. Zoals het recht op inzage en het recht op correctie en verwijdering. Onder de nieuwe wet moet u er ook voor zorgen dat alle mensen van wie u gegevens verzamelt, deze makkelijk van u kunnen krijgen en kunnen doorgeven aan een andere organisatie (recht op dataportabiliteit).

STAP 3 OVERZICHT VERWERKINGEN

Documenteer welke persoonsgegevens u verwerkt en waarom u dit doet, waar ze vandaan komen en met wie u ze gedeeld heeft. Middels de verantwoordingsplicht schrijft de GDPR voor dat u moet kunnen aantonen dat uw bedrijf volgens deze wet handelt. Het verwerkingsregister is bovendien

noodzakelijk als klanten, medewerkers of andere relaties hun privacyrechten uitoefenen. Dit is het geval wanneer zij willen dat u hun gegevens aanpast of verwijderd. Dit zal u vervolgens ook moeten doorgeven aan de organisaties waarmee u deze gegevens hebt gedeeld.

STAP 4 DATA PROTECTION IMPACT ASSESSMENT (DPIA)

Wanneer het verwerken van persoonsgegevens een hoog privacyrisico kan hebben, dan kunt u verplicht zijn om een Data Protection Impact Assessment (DPIA) uit te voeren. Hiermee kunt u vooraf bepalen wat de risico's zijn en passende maatregelen nemen. Wanneer het niet lukt om dit risico te verkleinen, bent u verplicht om met de Autoriteit Persoonsgegevens te overleggen, voordat u begint met de verwerking.

STAP 5 PRIVACY BY DESIGN & PRIVACY BY DEFAULT

De GDPR hanteert de uitgangspunten 'Privacy by Design' en 'Privacy by Default'. Privacy by Design houdt in dat u al bij het ontwerp van producten of diensten rekening houdt met de bescherming van de persoonsgegevens. Zo mag u niet méér gegevens verzamelen, en niet langer, dan voor een specifieke doel nodig is. Privacy by Default betekent dat u technische en organisatorische maatregelen neemt, waardoor standaard alléén die persoonsgegevens verwerkt worden die noodzakelijk zijn.

STAP 6 FUNCTIONARIS VOOR DE GEGEVENSBESCHERMING (FG)

Als u bijzondere persoonsgegevens verwerkt, zoals gegevens over iemands gezondheid,

politieke opvatting, geloofsovertuiging of strafrechtelijke verleden, dan bent u onder de GDPR mogelijk verplicht om een Functionaris voor de gegevensbescherming (FG) aan te stellen. Een FG is een interne privacy-toezichthouder voor toepassing en naleving van de GDPR.

STAP 7 MELDPlicht DATALEKKEN

De meldplicht datalekken die sinds 1 januari 2016 geldt, blijft onder de nieuwe GDPR merendeels hetzelfde. Wel worden de registratie-eisen vanaf 28 mei 2018 strenger. Alle datalekken dienen te worden gedocumenteerd, zodat de AP kan controleren of u aan deze meldplicht voldoet.

STAP 8 VERWERKERSOVEREENKOMSTEN

Heeft u gegevensverwerking uitbesteed? Dan dient u te evalueren of de maatregelen die u in het contract met deze verwerker hebt afgesproken voldoen aan de GDPR. Is dat niet het geval? Dan dient u deze aan te passen aan de nieuwe wet.

STAP 9 LEIDENDE TOEZICHTHOUDER

Heeft u vestigingen in andere EU-landen? Of heeft uw gegevensverwerking invloed in meerdere EU-landen? Dan hoeft u nog maar aan één privacy-toezichthouder verantwoording af te leggen, de leidende toezichthouder. Zorg wel dat u weet onder welke toezichthouder uw bedrijf valt.

STAP 10 TOESTEMMING

Als u toestemming nodig heeft van de mensen van wie gegevens worden verwerkt, moet u nagaan of deze toestemming overeenkomstig de GDPR is. Dat geldt zowel voor de manier waarop u toestemming vraagt, als de manier waarop u deze krijgt en registreert. Onder de nieuwe Europese privacywet dient u dit allemaal aan te kunnen tonen. Ook moet het voor mensen net zo eenvoudig zijn om hun toestemming weer in te trekken, als dat ze deze aanvankelijk hebben gegeven.

.

A.B. Software & Consultancy

Dé **Exact** partner voor de industrie

☎ 088 - 456 1234

💻 www.absc.nl

