Stappenplan Algemene verordening gegevensbescherming (AVG)

Vanaf 25 mei 2018 is de Algemene verordening gegevensbescherming (AVG) een feit. Deze nieuwe privacywet geeft personen **meer privacyrechten** en organisaties **meer verantwoordelijkheden**. Dat laatste geldt ook voor organisaties binnen het MKB. Elke organisatie, die persoonsgegevens verwerkt, valt onder de werking van de AVG. Persoonsgegevens zijn gegevens, die (direct of indirect) te herleiden zijn tot een specifiek individu, denk aan: NAWTE-gegevens, zakelijke contactgegevens, leeftijd, geslacht, bankgegevens, maar ook foto's, videobeelden en IP-adressen. De nieuwe privacywetgeving ziet niet alleen toe op digitale gegevens, maar ook gegevens op papier.

De Autoriteit Persoonsgegevens ("AP") houdt toezicht op de naleving van de privacywet en kan hoge geldboetes uitdelen. Daarnaast zorgt een datalek voor de nodige negatieve aandacht en kan het imagoschade opleveren. Genoeg reden om goed voorbereid te zijn op de AVG. TouchPro helpt je in 5 stappen in de goede richting.

Stap 1: Documenteer alle systemen, aanwezige data en stel bewaartermijnen vast

Breng allereerst in kaart welke categorieën gegevens er binnen jouw organisatie aanwezig zijn. Dat kan je het eenvoudigst doen aan de hand van alle systemen en (web)applicaties die je in gebruik hebt. Bedenk vervolgens waarvoor je deze gegevens nodig hebt. Heb je de gegevens vastgelegd om uitvoering te geven aan de bestaande klantrelatie of voor marketingdoeleinden? Waarvoor bewaar je de gegevens nog? Is dat vanwege de fiscale bewaarplicht, uit het oogpunt van klachtenafhandeling of onverhoopte juridische onenigheid? Probeer je database(s) op te schonen en vervolgens opgeruimd te houden door het vaststellen van passende bewaartermijnen.

Stap 2: Breng in kaart met welke partijen je gegevens uitwisselt/deelt en waarom

Ga vervolgens na binnen welke bedrijfsprocessen er data wordt uitgewisseld of gedeeld met derde partijen. Bedenk ook waarom die data-uitwisseling plaatsvindt? Verkrijgt deze partij gegevens bij de uitvoering van haar dienstverlening (HRM, ICT, Marketing) aan jullie organisatie? Dan is deze partij een zogenaamde verwerker. Maak passende afspraken met verwerkers over de omgang met de data, de bewaartermijnen en hoe te handelen in het geval van een datalek. **Leg dit contractueel vast**.

Stap 3: Bedenk wat je gaat (en moet) doen in geval van een datalek

Organisaties zijn verplicht om een protocol datalekken te hebben, zodat zij in staat zijn tijdig te voldoen aan de **Meldplicht Datalekken**. Ernstige datalekken moeten namelijk binnen 72 uur, na het ontdekken daarvan, gemeld worden aan de AP. Denk bij ernstig aan een lek met veel of hele gevoelige data. Naast de meldplicht hebben organisaties een protocolplicht. Alle beveiligingsincidenten moeten intern geregistreerd worden met daarbij de genomen afwegingen, melden of niet en waarom niet. De verloren smartphone, een verkeerd verzonden bericht (verkeerde ontvanger) en de e-mail met ontvangers in de CC in plaats van de BCC, betreffen ook beveiligingsincidenten. Het versturen of afgeven van persoonsgegevens aan een verkeerde ontvanger was in 2017 het **meest voorkomende type datalek**. Zorg ervoor dat je (medewerkers) weten waar én dat zij (ook) dit type incidenten dienen te melden.

Stap 4: Informeer je medewerkers over de nieuwe privacywetgeving

Stap 4 ligt in het verlengde van de vorige stap, het creëren van bewustwording. Zorg ervoor dat de relevante mensen in je organisatie op de hoogte zijn van de nieuwe privacyregels. Zo voorkom je ook,

dat onwetende medewerkers op onveilige wijze gegevens verspreiden. De AP biedt instrumenten die organisaties kunnen helpen om de nieuwe privacywetgeving na te leven: **hulpbijprivacy.nl** en de **AVG-regelhulp**. Het gericht trainen en instrueren van je personeel op het gebied van privacy en data security kan ook door middel van het aanbieden van **e-learnings** of workshops.

Stap 5: Informeer je klanten

Last but not least. Het belangrijkste uitgangspunt van de AVG is transparantie. Organisaties dienen open en eerlijk te zijn over de gegevens, die zij vastleggen en waarom. Dit gebeurt doorgaans in een **privacy statement**. Daarin leg je (kort gezegd) uit wat je verzamelt, hoe en waarom. De gegevens, die je als organisatie noodzakelijkerwijs nodig hebt voor de uitoefening van je dienstverlening mag je verzamelen zonder toestemming. Voor het toesturen van nieuwsbrieven via de e-mail of het vastleggen van (privacy)gevoelige gegevens is vaak toestemming nodig. Zorg dat de verkregen **toestemming** voldoende specifiek is, zodat voor je klant duidelijk is waarvoor toestemming wordt gegeven. Zorg ook dat de toestemming (te allen tijde) weer in te trekken is.

Na het doorlopen van de bovengenoemde 5 stappen ben je als organisatie niet 100% privacy compliant. Wel heb je als organisatie met deze 5 stappen een goede basis voor de nieuwe privacywetgeving.