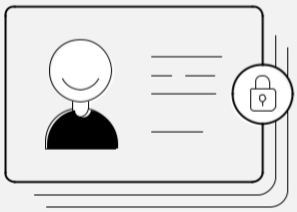
Tele service

Mobile Device Management noodzaak voor AVG

Algemene Verordening Gegevensbescherming



Mobile Device Management noodzaak voor AVG

De AVG heeft grote gevolgen voor bedrijven die bedrijfs- en persoonsgegevens beheren en verwerken. Elke organisatie binnen de EU die met gevoelige informatie werkt valt hieronder. Denk hierbij aan organisaties die met de volgende dataset aan gegevens werken.

- **Klantgegevens**
- **Transactiegegevens**
- **Werknemersgegevens**
- **Patiëntgegevens**

Deze wetgeving is leidend voor iedere organisatie, ongeacht grootte of aantal records. Organisaties moeten rekening houden met de gevolgen van een datalek. Wanneer er niet wordt voldaan aan de regelgeving, kan dit boetes opleveren tot maximaal 20 miljoen euro of 4% van de wereldwijde omzet. Maar misschien is de imagoschade nog wel groter, de risico's zijn enorm.

Beveiligen van mobiele toestellen is van groot belang voor AVG

Organisaties beschermen al jarenlang hun computers, servers en het netwerk met firewalls, virusscanners en ga zo maar door. Binnen de muren van het kantoor zit het vaak wel goed met de veiligheid van bedrijfsgegevens. Maar de laatste jaren is er een sterke groei van bedrijfsgegevens dat ook over mobiele toestellen verloopt, zoals smartphones, tablets en laptops die zich buiten het beveiligde bedrijfsnetwerk bevinden. Het verandert onze manier van werken, maar ook de manier hoe bedrijfsgevoelige gegevens te beschermen.

Hackers richten zich ook steeds meer op deze mobiele toestellen. Niet zo gek ook, aangezien dit veelal de zwakke plekken binnen het bedrijfsnetwerk zijn en dus een makkelijke ingang om bij gevoelige gegevens te komen.

De behoefte om gegevens op mobiele toestellen beter te beschermen groeit vanuit verschillende oogpunten. De noodzaak vooral door de wetgeving AVG dit beter te organiseren. Er wordt namelijk verwacht dat organisaties 'volgens de laatste

stand der techniek’ er alles aan doen om gevoelige bedrijfs- en persoonsgegevens te beschermen. Dus ook op mobiele toestellen. Eén van de grootste oorzaken van een datalek is verlies of diefstal van een mobiel apparaat. Organisaties moeten hier dus iets mee, maar hoe doet u dit eigenlijk?

Technische en organisatorische maatregelen

De AVG verplicht organisaties persoonsgegevens te beschermen met ‘passende technische en organisatorische maatregelen’. Maar over welke maatregelen hebben we het nu precies?

In artikel 32 staan wel enkele typen maatregelen omschreven die organisaties ‘waar passend’ kunnen inzetten:

- **Encryptie**
- **Borgen BIV (Beschikbaarheid, Integriteit en Vertrouwelijkheid)**
- **Bedrijfscontinuïteit**
- **Toegangscontrole**
- **Controle effectiviteit maatregelen**

Een Mobile Device Management (MDM) oplossing ondervangt deze punten. Het kan versleuteling meegeven aan bijvoorbeeld e-mailberichten, bestanden en mappen. Met een MDM-oplossing kunt u verloren telefoons traceren en op afstand de gegevens wissen van de telefoon. Zo blijven de mobiele persoonsgegevens onder controle en gewaarborgd.

Maar u kunt deze persoonsgegevens ook weer snel beschikbaar stellen, binnen security spreken we hier over bedrijfscontinuïteitplannen en incident-responsemanagement.

Persoonsgegevens mogen alleen toegankelijk zijn voor personen die van de ‘verwerkingsverantwoordelijke’ de opdracht hebben gekregen om ze te verwerken. Processen voor autorisatie en authenticatie moeten die toegang beperken.

Binnen een Mobile Device Management oplossing kunt u rechten toewijzen en wachtwoorden afdwingen voor zowel het toestel als specifieke bedrijfsapplicaties die erop staan.

Mobile Device Management een noodzaak

Met een MDM-oplossing kunt u uw gehele mobiele vloot aan toestellen effectief controleren, toegangsniveaus bepalen, versleutelen en waarborgen in één centrale beheeromgeving. Maar nog belangrijker, het geeft uw organisatie volledige grip en controle over de diversiteit aan mobiele toestellen.

Een oplossing voor het beheren van uw mobiele apparaten is dan geen luxe maar een must. Met een MDM-oplossing kunnen alle apparaten efficiënt en veilig worden beheerd. Een MDM-oplossing zorgt niet alleen voor het uitrollen van restricties, maar u kunt ook op afstand de instellingen van apparaten wijzigen en beveiligen. In het ergste geval van verlies of diefstal kan een apparaat compleet gewist worden. Zo voorkomt u mogelijke datalekken en geeft zekerheid en controle in het mobiliseren van bedrijfsprocessen.

Weten hoe Mobile Device Management u helpt AVG-proof te worden?

Maak een vrijblijvende afspraak met uw accountmanager

Tele service

Hoofdkantoor
's Gravenweg 320
2905 LB Capelle a/d IJssel
T 088 - 833 00 00

Business Center
Molenbaan 30
2908 LM Capelle a/d IJssel
T 088 - 833 00 00

Vestiging Boxtel
Bosscheweg 139 E
5282 WV Boxtel
T 088 - 833 00 90