Hoe EMM u helpt bij de naleving van de algemene verordening gegevensbescherming

Redelijke, verstandige beveiligingsstandaarden worden in tal van regio's overal ter wereld omgezet in wetgeving. De algemene verordening gegevensbescherming is sinds april 2016 van kracht in de EU en wordt op 25 mei 2018 volledig van toepassing. De algemene verordening gegevensbescherming zorgt voor één allesomvattend, geharmoniseerd juridisch systeem in de EU voor de bescherming van gegevens en privacy. De geldboetes en reputatieschade als gevolg van niet-naleving van de algemene verordening gegevens-bescherming zijn aanzienlijk. De maximumboete bedraagt meer dan 20 miljoen euro of 4% van de wereldwijde bedrijfsomzet.

De algemene verordening gegevensbescherming is van toepassing op verwerkingsverantwoordelijken en verwerkers in de EU en op verwerkingsverantwoordelijken en verwerkers buiten de EU wanneer zij persoonsgegevens van EU-burgers verwerken.

MobileIron

info@mobileiron.com
www.mobileiron.com
Tel: +1.877.819.3451
Fax :+1.650.919.8006

"EMM wordt cruciaal voor de naleving van de algemene verordening gegevensbescherming."

IDC (februari 2017)*

"Verwerkingsverantwoordelijke" wordt gedefinieerd als de organisatie die doel en methode van de gegevensverwerking bepaalt. "Verwerker" wordt gedefinieerd als de organisatie die de verwerking uitvoert namens en onder aanwijzing van de verwerkingsverantwoordelijke. In dit document gaan wij ervan uit dat de verwerker en de verwerkings-verantwoordelijke dezelfde entiteit zijn: de onderneming met werknemers of klanten in de EU.

Een allesomvattend en goed gestructureerd EMM-programma (Enterprise Mobility Management) is een belangrijk onderdeel van bedrijfsinitiatieven die zijn gericht op naleving van de algemene verordening gegevensbescherming. Dit document biedt ondernemingen een kader om de privacy, het beveiligingsbeleid ten aanzien van mobiele apparaten en handhavingsmodellen proactief te beoordelen. Dit document biedt geen juridisch advies. Elke onderneming dient ervoor te zorgen dat haar EMM-implementatie goed aansluit op haar interne juridische kader en nalevingskader.

De principes voor het verwerken van persoonsgegevens volgens de algemene verordening gegevensbescherming zijn gebaseerd op standaarden en consistent met nieuwe privacykaders in andere regio's.

De principes van de algemene verordening gegevensbescherming

Elke werkgever bewaart bepaalde persoonsgegevens. Het logische beginpunt voor de naleving van de algemene verordening gegevensbescherming is om een minimum aan noodzakelijke persoonsgegevens te bewaren en redelijke voorzorgsmaatregelen te treffen om de risico's voor burgers te beperken.

Hoewel Europa in de hele wereld vooroploopt op het gebied van gegevensbescherming en privacy, zijn de principes voor de verwerking van persoonsgegevens onder de algemene verordening gegevensbescherming gebaseerd op standaarden en consistent met nieuwe privacykaders in andere regio's. Deze principes zijn onder meer:

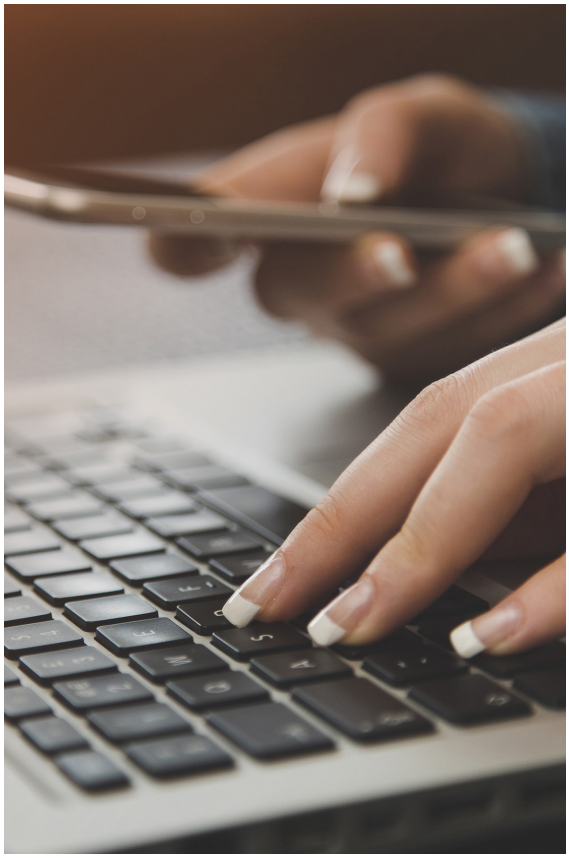
- **Rechtmatige, behoorlijke en transparante verwerking:** ondernemingen moeten geldige redenen hebben om persoonsgegevens te verwerken en moeten die informatie aan de betrokkene geven.
- **Doelbinding:** er moet een duidelijke en uitdrukkelijke reden zijn voor de verwerking van persoonsgegevens. De gegevens mogen alleen worden verwerkt voor het doel waarvoor de gegevens zijn verzameld.
- **Instemming:** de betrokkene van wie persoonsgegevens worden verwerkt, moet over het algemeen hiervoor zijn instemming geven.
- **Minimale gegevensverwerking:** de verwerkte gegevens moeten beperkt zijn tot wat strikt noodzakelijk is voor een specifiek doel. Toegang mag alleen worden gegeven aan degenen die die gegevens voor dat specifieke doel nodig hebben.

* "Market Analysis Perspective: Western Europe Enterprise Mobility, 2017" van IDC Europe, februari 2017.

- **Juistheid:** de gegevens moeten juist zijn en onjuistheden moeten gemakkelijk kunnen worden gecorrigeerd. Een betrokkene moet het recht hebben om een dergelijke rectificatie te vragen.
- **Opslagbeperking:** de gegevens mogen alleen worden bewaard zolang ze noodzakelijk zijn voor het beoogde doel.
- **Integriteit en vertrouwelijkheid:** de gegevens moeten worden verwerkt op een wijze die adequate beveiliging van de gegevens garandeert, waaronder voorkoming van ongeoorloofde verwerking en onopzettelijk verlies.
- **Verantwoordingsplicht:** de onderneming moet in staat zijn de naleving van bovenstaande principes en gerelateerde corrigerende maatregelen aan te tonen.

Een onderneming moet kunnen aantonen dat zij afdoende veiligheidsmaatregelen heeft genomen en dat naleving adequaat wordt gecontroleerd.

Privacy is geen bijzaak.



Gegevensbescherming door ontwerp en door standaardinstellingen – Artikel 25 van de algemene verordening gegevensbescherming

Privacy is geen bijzaak. Artikel 25 van de algemene verordening gegevensbescherming beschrijft het concept van "gegevensbescherming door ontwerp en door standaardinstellingen", ook bekend als "privacy door ontwerp en door standaardinstellingen".

Gegevensbescherming door ontwerp: de onderneming moet gegevens gedurende haar gehele operationele levenscyclus beschermen, van het eerste ontwerp van processen en systemen tot aan buitendienststelling ervan en gegevensvernietiging.

Gegevensbescherming door standaardinstellingen: de onderneming moet ervoor zorgen dat standaard alleen de benodigde hoeveelheid persoonsgegevens worden verzameld en verwerkt. De betrokkene moet zich niet hoeven af te melden om inwinning van aanvullende gegevens te voorkomen. De onderneming mag geen informatie verzamelen "voor het geval dat" zij die eventueel later wil gebruiken.

Stand van de techniek – Artikel 32 van de algemene verordening gegevensbescherming

Artikel 32 van de algemene verordening gegevensbescherming schetst het belang van het gebruik van de allerbeste actuele technologieën voor de ondersteuning van informatiebeheer:

*"Rekening houdend met de **stand van de techniek** ... treffen de verwerkingsverantwoordelijke en de verwerker passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen."*

Hoewel de algemene verordening gegevensbescherming geen specifieke technische implementaties voorschrijft, verwijst artikel 32 naar onder andere versleuteling, integriteit, beschikbaarheid en tests als voorbeeldmaatregelen, waarvoor de onderneming de meest geavanceerde oplossingen moet overwegen.

Een EMM-kader voor de algemene verordening gegevensbescherming

EMM-oplossingen, zoals MobileIron, zijn een belangrijke component van een beveiligingsprogramma dat aan de algemene verordening gegevensbescherming voldoet. Voor ondernemingen zonder effectieve EMM kan het een uitdaging zijn aan autoriteiten uit te leggen waarom zij geen geavanceerde, technische maatregelen hebben genomen om het risico van gegevensverlies te beperken.

Voor ondernemingen zonder effectieve EMM kan het een uitdaging zijn aan autoriteiten uit te leggen waarom zij geen geavanceerde, technische maatregelen hebben genomen.

Een EMM-kader voor de algemene verordening gegevensbescherming moet onder meer bestaan uit de volgende MobileIron-functionaliteit:

1. Met het MobileIron-platform kan de onderneming **gegevensversleuteling afdwingen** bij het apparaat door versleutelingsinstellingen voor het apparaat te bewaken en secundaire versleuteling aan te bieden voor zakelijke apps en bedrijfsgegevens.
2. Met het MobileIron-platform kan de onderneming **een duidelijke scheiding tot stand brengen tussen persoonsgegevens en bedrijfsgegevens** op het apparaat. De onderneming heeft geen toegang tot de inhoud van persoonlijke apps of persoonlijke e-mailaccounts. Elke onderneming moet ook beoordelen of toegang tot andere soorten persoonsgegevens, zoals app-inventaris of apparaatlocatie, een rechtvaardig beveiligingsdoel of operationeel doel dient. Als dat het geval is, moet dat doel duidelijk worden verwoord en gecommuniceerd, en moeten de maatregelen voor wat betreft gegevensbescherming door standaardinstellingen en instemming proactief worden geïmplementeerd.
3. Met het MobileIron-platform kan de onderneming **vertrouwde toegang tot bedrijfsservices afdwingen.** MobileIron Access biedt de onderneming inzicht in welke mobiele apparaten en apps verbinding proberen te maken met back-endservices. Ongeoorloofde toegang kan dan worden geblokkeerd. MobileIron Sentry beschermt het gegevensverkeer en kan dit indien nodig ook langs aanvullende beveiligings- en inspectiegateways routeren.
4. Met het MobileIron-platform kan de onderneming **auditlogs** raadplegen om te bepalen welke acties plaatsvonden voorafgaand aan een inbreuk op gegevens en welke acties daarna plaatsvonden. In bepaalde situaties bedraagt de verplichte melding krachtens de algemene verordening gegevensbescherming slechts 72 uur en is een snelle reactie vereist.
5. Met het MobileIron-platform kan de onderneming **maatregelen tegen gegevensverlies afdwingen.** Dankzij deze maatregelen kan de onderneming vertrouwelijke gegevens op een verloren apparaat op afstand wissen en ervoor zorgen dat zakelijke apps op een apparaat geen gegevens kunnen delen met ongeoorloofde apps. Deze maatregelen identificeren ook aanvallen op de integriteit van het besturingssysteem van het mobiele apparaat (jailbreaking of rooting). Als er sprake is van een nalevingsprobleem, kan de onderneming met het MobileIron-platform de juiste correctieve maatregelen nemen, zoals meldingen verzenden, bestanden in quarantaine plaatsen of gegevens wissen.

Onbeheerde mobiele apparaten maken geen deel uit van een grondige verdedigingsstrategie.

EMM implementeren voor de algemene verordening gegevensbescherming

Elke onderneming die wordt getroffen door de algemene verordening gegevensbescherming doet er verstandig aan haar bestaande EMM-implementatie en configuratiemodel onder de loep te nemen. Ten eerste identificeert een dergelijke inventarisatie hiaten waarin EMM onvoldoende wordt ingezet voor de naleving van de algemene verordening gegevensbescherming. Ten tweede vormt deze inventarisatie de basis voor het ontwerp en de implementatie van een duurzaam nalevingstoezicht- en correctieprogramma.

Hier is een beginpunt voor de implementatie van EMM als onderdeel van een beveiligings-programma dat aan de algemene verordening gegevensbescherming voldoet.

1. Plaats alle mobiele apparaten onder beheer als deze toegang hebben tot bedrijfsgegevens. Onbeheerde mobiele apparaten maken geen deel uit van een grondige verdedigingsstrategie die een redelijk niveau van gegevensbescherming biedt aan verloren of gecompromitteerde apparaten.
2. Pas actuele configuratieprofielen toe. Dwing beleid af voor wachtwoorden, versleuteling, beveiliging van apparaten, verbindingen en andere relevante zakelijke functies.
3. Distribueer alle zakelijke apps als beheerde apps via een app store van de onderneming, zodat de apps in een door de onderneming gecontroleerd beveiligingskader worden gebruikt.
4. Dwing adequaat beleid af om gegevensverlies te voorkomen en app-gegevens op het apparaat te beschermen.
5. Dwing voor alle zakelijke services vertrouwde toegang af. Blokkeer de toegang vanaf ongeoorloofde, onbeheerde of niet-conforme apparaten, apps en gebruikers. Sta niet toe dat vertrouwelijke gegevens worden opgeslagen op een apparaat buiten het zicht en de controle van de onderneming.
6. Stel gegevensbeschermingsbeleid en beveiligingsbeleid op en communiceer het beleid regelmatig in heldere bewoordingen naar werknemers.
7. Verzamel adequate auditlogs met informatie over inventaris en gebruik om in het geval van inbreuk op gegevens snel te kunnen reageren.

Conclusie

Een onderneming kan alleen adequate beveiliging bieden voor persoonsgegevens als zij kan aantonen dat zij afdoende EMM-controlemaatregelen en procedures heeft geïmplementeerd. Deze maatregelen moeten ervoor zorgen dat de persoonsgegevens die door de onderneming worden verkregen, worden beschermd tegen dreigingen van buitenaf en tegen ongeoorloofd gebruik of ongeoorloofde openbaarmaking. Het MobileIron-platform biedt een robuust kader voor de naleving van de principes van de algemene verordening gegevensbescherming: de minimalisering, integriteit en vertrouwelijkheid van gegevens evenals verantwoordingsplicht.