Huidige uitdagingen en oplossingen rondom beveiliging

Gegevensprivacy en compliance

Cyberbeveiliging is de grootse bedreiging voor het voortbestaan en het succes van moderne organisaties. De afgelopen jaren zijn grote gegevenslekken regelmatig in het nieuws geweest. Dit is de nieuwe realiteit voor organisaties.

In het nieuws verschijnen regelmatig berichten over retailers, verzekeringsmaatschappijen, banken en technologiebedrijven die gehackt worden. Volgens schattingen zijn er alleen al in 2014 meer dan een miljard persoonlijke records aangetast. En die negatieve trend zet zich gestaag door.

Tegelijkertijd is de compliancedruk hoger dan ooit tevoren. Hoewel gegevensprivacywetgeving lang niet nieuw is, zet de komst van de Algemene Verordening Gegevensbescherming (AVG), ook wel bekend als de General Data Protection Regulation (GDPR), organisaties flink onder druk. De AVG treedt in mei 2018 in werking en verplicht alle soorten organisaties te voldoen aan nieuwe beveiligingsniveaus van persoonsgegevens. Als organisaties er niet in slagen om hun systemen en gegevens op de juiste manier te beveiligen, worden ze met torenhoge boetes bestraft.

RICOH
imagine. change.

De situatie

U staat onder druk om uw gegevensrecords op orde te krijgen en uw informatie te beveiligen

Alle soorten organisaties beschikken over gegevens die criminelen graag zouden willen bemachtigen. U heeft namelijk een aanzienlijke hoeveelheid persoonlijke en financiële gegevens van uw medewerkers in uw bezit. En u beschikt ook over contactgegevens van klanten, waar oplichting of fraude mee kan worden gepleegd. Als u met grootzakelijke klanten werkt, kunt u via hun beveiliging ook een onbewuste snelkoppeling vormen.

Ondertussen zijn hackers niet uw enige zorg. Net als elke andere organisatie die over persoonsgegevens van EU-burgers beschikt, moeten uw gegevensprocessen vóór mei 2018 op orde zijn voor AVG-controle. Uw informatiebeheerprocessen dienen aan de strikte nieuwe AVG-normen voor 'adequate beveiliging' te voldoen. Bent u niet compliant, dan staan u aanzienlijke financiële sancties en reputatieschade te wachten. En ook uw bedrijfscontinuïteit komt in het gedrang.

Dus hoe houdt u uw gegevens op orde en veilig? Zodanig dat compliance eenvoudig kan worden aangetoond, maar gegevens niet in de handen van criminelen vallen. Hoe houdt u klantgegevens veilig en behoudt u hun vertrouwen? Hoe kunt u efficiënt werken aan AVG-compliance terwijl de bedrijfsactiviteiten gewoon doorgaan?

RICOH
imagine. change.

De bedreigingen

Als moderne organisaties succesvol willen zijn, is gegevensprivacy cruciaal. Door te voldoen aan de strenge compliancenormen, wordt gevoelige informatie beschermd tegen verlies, diefstal of aanvallen.

Non-compliance heeft grote financiële gevolgen

Organisaties kunnen een boete krijgen tot 20 miljoen euro of 4% van de jaarlijkse wereldwijde omzet voor het overtreden van de AVG.[1]

Kans op reputatieschade

De kosten voor non-compliance of gegevensdiefstal omvatten niet alleen financieel verlies, maar kunnen ook ingrijpende gevolgen hebben voor de bedrijfscontinuïteit en tot reputatieschade leiden.

Ongestructureerde gegevens: een beveiligings- en compliancerisico

85% van de bedrijfsgegevens is 'ongestructureerd' en bevindt zich waarschijnlijk op de persoonlijke apparaten van medewerkers of als papieren exemplaren in kasten. Dit maakt overzicht in hoe de informatiestromen binnen uw organisatie lopen onmogelijk.[2] Deze ongestructureerde informatie verhoogt uw potentiële risico op gegevensverlies, diefstal of aanvallen. Bovendien bemoeilijkt het de rapportage en het vastleggen van gegevensprocessen.

Geen verschil tussen klein en groot

Niet alleen grote organisaties zijn gevoelig voor gegevenslekken. 60% van de kleine en middelgrote bedrijven (MKB) hebben in het afgelopen jaar een gegevenslek gemeld.[3] En voor het MKB wordt met compliance geen uitzondering gemaakt. De AVG is van toepassing op alle organisaties die gegevens van EU-burgers opslaan of verwerken, ongeacht waar de organisatie is gevestigd.

1. De EU GDPR-portal 'Frequently Asked Questions about the incoming GDPR' kunt u op www.eugdpr.org/gdpr-faqs.html vinden.
2. 'A Guide to Improving Document Efficiency', Ricoh whitepaper, oktober 2013.
3. Quocirca Enterprise MPS Study, 2017. Onderzoekspopulatie: 240 organisaties van meer dan 500 werknemers uit verschillende sectoren in het Verenigd Koninkrijk, Frankrijk, Duitsland en de Verenigde Staten.

RICOH
imagine. change.

De oplossingen

Structureer uw (digitale) documentomgeving

Als u met papieren documenten blijft werken, brengt u uw organisatie mogelijk in gevaar. En het vormt niet alleen een beveiligingsrisico. Het bemoeilijkt compliance en het verlies van belangrijke klantdossiers kan vergelijkbare gevolgen hebben als diefstal. Als u precies weet waar uw documenten zich bevinden, kunt u ze gemakkelijker beveiligen en openen wanneer u ze nodig heeft. **Ontdek hoe u uw documenten efficiënt digitaliseert, organiseert en beveiligt met de Print Security Optimisation-services van Ricoh.**

Verdubbel de gegevensbeveiliging

Stel dat u weet wie, waarom, hoe en welke persoonsgegevens binnen uw organisatie worden opgeslagen en verwerkt. Dan is het aanscherpen van de beveiliging van deze gegevens een belangrijke stap op weg naar AVG-compliance. Ricoh beschikt over de hoogste certificeringsniveaus binnen de sector. **Onze MFP's beschikken over ingebouwde beveiligingsfuncties die de circulerende gegevens binnen uw organisatie beschermen.**

Verwijder onnodige gegevens

Een belangrijke vereiste van de AVG is dat uw organisatie informatie alleen behoudt zolang dit nodig is. Wanneer u gegevens verwijdert die u niet langer nodig heeft, dient u ervoor te zorgen dat deze informatie effectief en veilig wordt verwijderd. Dit geldt ook voor de achtergebleven gegevens op apparaten aan het einde van hun levensduur. **Met de gecertificeerde en controleerbare Ricoh Data Cleansing Service worden gegevens aan het einde van de levensduur of het contract veilig van uw printer/MFP verwijderd.**

Beschouw AVG-compliance als kans

Hoe intimiderend of ongemakkelijk het ook lijkt, de AVG biedt ook kansen. Het verplicht u om uw bestaande gegevensbeheerprocessen grondig te herzien en zwakke punten in de beveiliging te identificeren en aan te pakken. U gaat de verwerking van persoonsgegevens controleren, vastleggen en beoordelen. Zo bereikt u niet alleen AVG-compliance, maar verbetert u uw informatiebeveiliging ook aanzienlijk. En u bent veel beter bestand tegen cyberaanvallen. **Ontdek hoe Ricoh u kan helpen om uw informatie te beveiligen en wet- en regelgeving na te leven.**

Vraag een expert

Ga naar **www.ricoh.nl** of neem contact met ons op. Ontdek hoe we u kunnen begeleiden op weg naar gegevensbeveiliging volgens de best practices en naleving van wet- en regelgeving.

Ricoh Nederland
Magistratenlaan 2
5223 MD 's-Hertogenbosch

073 645 11 11

www.ricoh.nl

RICOH
imagine. change.