Whitepaper Informatiebeveiliging

AVG-compliance

Een introductie tot informatiebeveiliging

www.sharp.nl | www.sharp.be

SHARP
Be Original.

Inhoud

Introductie

Veel mkb-bedrijven worstelen met de naleving van de Europese wet Algemene verordening gegevensbescherming (AVG), met name als het gaat om de bescherming van persoonlijke gegevens.

De Algemene verordening gegevensbescherming (AVG) heeft verschillende uitdagingen met zich meegebracht voor bedrijven in Europa en daarbuiten.

Hoewel de grootste focus van de AVG ligt op de bescherming van online gegevens, is de regelgeving ook van toepassing op hoe bedrijven met data omgaan en opslaan. Dat betekent dat ze moeten nadenken over wat er gebeurt met de data die ze vastleggen (via scannen of elektronische input), opslaan en bewaren, verwerken, delen, printen, kopiëren, faxen en archiveren.

De AVG introduceert onder meer begrippen als persoonlijk identificeerbare informatie, gegevensbescherming, gegevensvernietiging, gegevensverwerkers, verwerkings-verantwoordelijken, gegevens-beschermingsautoriteit (zie de AVG-begrippenlijst op pagina 8).

Er bestaan veel publicaties die zich richten op hoe de AVG moet worden geïnterpreteerd, wie erbij betrokken zijn en hoe de regelgeving moet worden opgenomen in bedrijven. Maar er zijn slechts enkele documenten, artikelen of whitepapers beschikbaar over hoe de AVG moet worden vertaald naar het bedrijfsleven en alle bijbehorende processen en activiteiten, met name de activiteiten die gerelateerd zijn aan persoonlijke gegevens.

Door zakelijke gebruikers (medewerkers), bedrijfsprocessen (workflows en best practices) en bedrijfsmiddelen (hardware en software) aan elkaar te koppelen, heeft Sharp drie aparte gebieden van zakelijke beveiliging gedefinieerd die samen de algemene gegevensbescherming naar een hoger niveau kunnen tillen, om zo te voldoen aan de AVG.

- **Netwerkbeveiliging**
  Is gerelateerd aan elk netwerk dat door een organisatie wordt gebruikt, beheerd door een IT-afdeling. De focus ligt op alle verbonden randapparatuur omtrent printen, scannen en faxen.

- **Outputbeveiliging**
  Is gerelateerd aan zowel de geprinte als gescande output van MFP's en/ of printers. Onder deze categorie vallen hardcopy, afgedrukte documenten en afbeeldingen van documenten die worden verstuurd van een pc naar een printer (inclusief via speciaal aangewezen printservers), scans (inclusief scan-naar-map, scan-naar-email en scan-naar-cloud) en verstuurde faxdocumenten.

- **Documentbeveiliging**
  Is gerelateerd aan informatie afkomstig van papieren documenten via het scanproces of elektronische afbeeldingen van de documenten die zijn opgeslagen in bedrijfsarchieven, zoals e-mails, elektronische bestanden, formulieren, etc.

Sharp kan bedrijven helpen bij de naleving van de AVG door tools en best practices te introduceren en toe te passen op bedrijfsprocessen die rechtstreeks verbonden zijn met netwerk-, output en documentbeveiliging.

Achtergrond

De AVG is de grootste verandering in gegevensbescherming van de afgelopen twintig jaar. Maar er zijn nog steeds veel vragen over – en nog weinig antwoorden.

De AVG introduceert nieuwe eisen en definieert de boetes voor een gebrek aan middelen en preventieve maatregelen om tegen datalekken te beschermen (1). Maar er wordt weinig informatie gegeven over wat bedrijfseigenaren, IT-beheerders en gebruikers nodig hebben om aan de AVG te voldoen. Elk bedrijf moet zelf bepalen wat het nodig heeft.

Het belangrijkste punt van de introductie van de AVG was het beter behere`n en beschermen van de verwerking van persoonlijk identificeerbare informatie. Dat houdt in dat alle persoonlijke informatie in uw bedrijfssystemen op de juiste wijze moet worden beheerd – van klant- en bedrijfscontactgegevens opgeslagen in uw bedrijfsapplicaties, tot en met alle netwerkinstellingen, documentmanagement- en printmanagementaccounts en personeelsdocumentatie.

Er bestaan twee lagen binnen de AVG-naleving:

- **De persoonlijke laag**
  Alle zaken die gerelateerd zijn aan de gebruiker, inclusief hun gedrag, manier van werken en hoe bedrijfssystemen en -regels op ze worden toegepast.

- **De organisatorische laag**
  Alle bedrijfsprocessen binnen een organisatie (inclusief papieren en elektronische workflows), middelen (inclusief de middelen die mensen helpen delen en communiceren op elektronische of papier gebaseerde wijze), de cultuur en hoe het bedrijf reageert op marktuitdagingen.

De introductie van strategieën en tools op organisatorische niveau maakt het beheer mogelijk van de verwachte verandering in eindgebruikersgedrag en hoe eindgebruikers werken en alle beschikbare bedrijfsgegevens verwerken. Dit leidt tot meer inzicht in hoe zowel documenten als gebruiker identificeerbare informatie moet worden verwerkt (2).

Daarom focust Sharp zich op de organisatorische laag (processen, oplossingen en hardware) en kan het bedrijven helpen uitgebreide, essentiële beveiligingsbeleid te creëren.

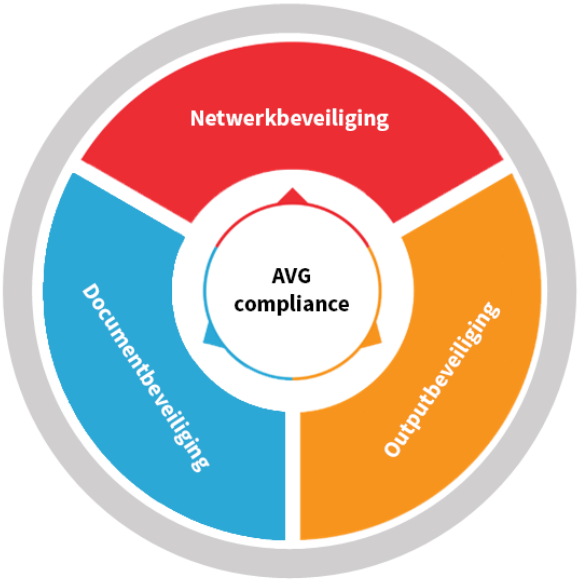
Met het oog op de drie categorieën voor algemene gegevensbescherming heeft Sharp drie mogelijke risico's in kaart gebracht die tot een AVG-overtreding kunnen leiden als er niks mee gedaan wordt.

- **Netwerkgerelateerde risico's**
  - Het verplaatsen van gegevens van papieren naar elektronische bestanden en weer terug naar papier.
  - De behoefte om MFP's en printers op dezelfde manier te beveiligen als servers en de behoefte aan een geplande en gemeenschappelijke printbeveiligingsbeleid.
  - De behoefte om apparaten te monitoren en beheren voor het naleven en – zo nodig – updaten van het beveiligingsbeleid op basis van eventuele nieuwe kwetsbaarheden.
  - De behoefte om gegevens veilig en tijdig te verwijderen.

- **Outputgerelateerde risico's**
  - De behoefte om toegang tot MFP's en printers te beveiligen, de output te beheren en vertrouwelijke gegevens te routeren.
  - Het beheer van het aantal en de typen output – kopieën, printjes, faxdocumenten, scans (inclusief scan-naar-email en scan-naar-map).
  - De behoefte aan een auditspoor en inzicht in wat er is vastgelegd en geprint.

- **Documentgerelateerde risico's**
  - Gebrek aan definitie van en inzicht in de documentlifecycle binnen het bedrijf. Dit omvat alle stappen van documentcreatie tot en met -vernietiging.
  - Ongestructureerde documentopslagsystemen die ervoor zorgen dat documentmanagementsystemen (DMS) het risico lopen op aanvallen en potentiële datalekken.
  - Vaak terugkomende handmatige opdrachten die gelinkt zijn aan (elektronische en papieren) documenten, waarbij een per ongeluk verkeerd toegevoegde bestemming kan leiden tot datalekken.
  - Ongecontroleerd delen van bedrijfskritische documenten.
  - Risico op gegevenscorruptie zonder versiebeheer.

Beveiligingsframework Sharp



Aanbevelingen

Met behulp van onze uitgebreide aanpak van bedrijfsbeveiliging garandeert Sharp naleving van de strengste regelgevingen en creëren we oplossingen die bedrijven helpen efficiënter te werken.

Sharp streeft naar AVG-naleving in elk aspect van informatiebeveiliging door zich te focussen op de drie hoofdcategorieën van bedrijfsbeveiliging: netwerkbeveiliging, outputbeveiliging en documentbeveiliging. We dekken de organisatorische aspecten van gegevensverwerking en gegevensbescherming met ons uitgebreide portfolio van Optimised Products en Solutions, en de daar aan gerelateerde Sharp Managed Services.

Door een sterke basis te creëren voor de organisatorische laag van een bedrijf beïnvloeden we het gedrag van eindgebruikers. Dit, in combinatie met onze met aandacht ontworpen en goed beveiligde systemen, helpt bedrijven met de naleving van de AVG en biedt de juiste tools voor het meten van risico's, voorkomen van cyberaanvallen en genereren van accurate gebruikersinzichten.

Sharp Managed Services dekt elk aspect van databeveiliging, inclusief hoe bedrijfssystemen omgaan met persoonlijk identificeerbare informatie. Zo helpen we organisaties te voldoen aan de AVG.

Hieronder vindt u een samenvatting van hoe Sharp u kan helpen te voldoen aan de AVG.

Algemene verordening gegevensbescherming (AVG) en Sharp		
Beveiligingsaspect	Producten en oplossingen	Naleving via
Netwerkbeveiliging	• Sharp MFPs • Sharp Printers • Sharp Remote Device Manager	• Gebruikerstoegangbeheer • Poortbeheer • Protocolbeheer • Network Services-beheer • Gegevensversleuteling • Gegevensoverschrijving
Outputbeveiliging	• Job Accounting II • SafeQ • Drivve Image	• Toegangsbeheer • Functionaliteitsbeperkingen • Gegevenslogboek- / auditrapportages • Gegevenslogboekretentie en -aanpassing
Documentbeveiliging	• Cloud Portal Office • Drivve Image	• Databasetoegangsbeheer • Gebruikersrechtenbeheer • Versiebeheer • Auditspoor • Documentretentie, incl. documentvernietiging • Auditlogboek

Conclusie

Sharp kan elke organisatie helpen effectieve beveiligingsmaatregelen en managementmethodes te introduceren voor AVG-naleving.

Het begrijpen, plannen, aanpassen en inzetten van de maatregelen en functies die nodig zijn voor AVG-naleving kan veel tijd in beslag nemen. Daarnaast kan dit proces implementatieproblemen veroorzaken, zeker gezien elk bedrijf anders is.

Sharp adviseert bedrijfseigenaren en IT-managers de whitepapers in onze bibliotheek door te lezen voor hulp bij de drie onderwerpen netwerkbeveiliging, outputbeveiliging en documentbeveiliging: [www.sharp.nl/informatiebeveiliging].

Deze whitepapers omschrijven de risico's en oplossingen en introduceren:

- Beveiligde netwerkapparatuur van Sharp.
- Beveiligingssoftware van Sharp die zakelijke datavastlegging en -output helpt te beschermen.
- Beveiligingssoftware van Sharp die elektronische documenten helpt te beschermen.

Daarnaast bieden de Sharp Managed Services-teams advies en helpen ze robuuste beveiligingsmaatregelen te creëren.

Ook introduceren ze tools die relevant zijn voor elk bedrijfstype en -behoefte.

Om mogelijke kwetsbaarheden in andere delen van uw bedrijf te voorkomen, kunnen we daarnaast helpen nog meer beveiligingsmaatregelen te introduceren. Met deze maatregelen uit het Sharp-portfolio levert u een 360-graden beveiliging voor elk onderdeel van uw bedrijf:

- Documentbeveiliging.
- Netwerkbeveiliging.
- Outputbeveiliging.
- AVG-naleving.

AVG-begrippenlijst (3)

Verantwoordelijkheid – de gegevensverantwoordelijke is verantwoordelijk voor naleving van de gegevensbeschermingsprincipes. Zij moeten de stappen kunnen aantonen die het bedrijf neemt om naleving te garanderen.

Datalek – een beveiligingsincident waarbij persoonsgegevens onbedoeld of met opzet vernietigd zijn, verloren zijn geraakt, gewijzigd zijn, verstrekt zijn of toegankelijk zijn gemaakt.

Verwerkingsverantwoordelijke – 'verantwoordelijke' verwijst naar een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt.

Recht op vergetelheid – (ook bekend als het recht om vergeten te worden) geeft het datasubject het recht om te verzoeken dat de gegevensverantwoordelijke zijn of haar persoonlijke gegevens verwijdert.

Gegevensverwerker – 'verwerken' verwijst naar elke activiteit, of set activiteiten, die wordt uitgevoerd met betrekking tot persoonlijke gegevens of sets persoonlijke gegevens. Verwerken bestaat uit geautomatiseerde of handmatige activiteiten. Verwerken omvat de volgende activiteiten: verzamelen, registreren, organiseren, gebruiken, structureren, opslaan, aanpassen, binnenhalen, raadplegen, vernietigen en meer. De dataverwerker kan een organisatie of externe leverancier zijn die de persoonlijke gegevens beheert en verwerkt uit naam van de verantwoordelijke. Dataverwerkers moeten voldoen aan specifieke wettelijke verplichtingen, zoals het bijhouden van persoonlijke dossiers, en zijn aansprakelijk in het geval van een beveiligingsincident.

Gegevensbeschermingsautoriteit – de nationale autoriteit die de gegevensprivacy beschermt.

Functionaris voor de Gegevensbescherming (Data Protection Officer of DPO)– een aangewezen persoon die erop toeziet dat de policy's en procedures van de AVG worden geïmplementeerd en nageleefd.

Datasubject – iemand van wie de persoonlijke gegevens worden verwerkt door een verantwoordelijke of verwerker.

Persoonlijke gegevens – directe en indirecte informatie die verband houdt met een persoon en kan worden gebruikt om de persoon te identificeren. Dit omvat hun naam, identiteitsnummer, locatie of online gegevens zoals een IP-adres.

Verwerken – verwijst naar elke activiteit in relatie tot persoonlijke gegevens, van initiële verzameling tot en met de uiteindelijke vernietiging. Verwerken omvat het organiseren, wijzigen, raadplegen, gebruiken, verstrekken, combineren en bewaren van gegevens – op elektronische dan wel handmatige wijze.

Bronnen

1. https://www.emerce.nl/achtergrond/negen-maanden-avg-tot-nu-toe-gebeurd
2. “CEO Survey”, PwC, 2017
3. “GDPR Glossary of Key Terms”, High Speed Training, februari 2018

SHARP

Be Original.