Stappenplan GDPR

(General Data Protection Regulation)

De General Data Protection is een nieuwe privacywet binnen de Europese Unie. De GDPR is vanaf 28 mei 2018 op elke organisatie, groot of klein, binnen alle branches van toepassing. De wet is bedoeld om privacyrechten van personen te waarborgen en beveiligen. Sigmax gelooft dat de GDPR een belangrijke stap voorwaarts is naar meer duidelijkheid over individuele privacyrechten, en het naleven hiervan. Maar Sigmax ziet ook dat door de GDPR organisaties veranderingen moeten doorvoeren. Veel bedrijven weten niet goed waar ze moeten beginnen. Sigmax helpt u graag het GDPR-traject te overwinnen.

Wat zijn de belangrijkste onderdelen van GPDR?

- Transparantie over verwerking en gebruik van persoonsgegevens.
- Beperken van verwerking van persoonsgegevens tot specifieke, legitieme doeleinden.
- Beperken van verzameling en opslag persoonsgegevens tot beoogd gebruik.
- Individuen in staat stellen om persoonsgegevens te laten corrigeren of om te laten verwijderen.
- Persoonsgegevens niet langer opslaan dan nodig is voor beoogd gebruik.
- Persoonsgegevens beveiligen met de juiste beveiligingsmethoden.

Stap 1: Identificeren

Stel vast welke persoonsgegevens er zijn en waar ze zijn opgeslagen

De eerste stap richting GDPR-compliance is beoordelen tot op welke hoogte de GDPR geldt voor uw bedrijf. Deze analyse begint met achterhalen welke gegevens uw bedrijf heeft en waar ze zijn opgeslagen.

Wat zijn persoonsgegevens?

Familie en demografische informatie. Religieuze overtuigingen en afkomst zijn gevoelige gegevens.

Vingerafdrukken en genetische informatie.

Vrijetijdsbestedingen en hobby's. Politieke meningen zijn gevoelige gegevens.

Gedragspatronen en interesses.

Reisgeschiedenis en locatiegegevens.

Financiële informatie. Lidmaatschappen zijn gevoelige gegevens.

Online gedragspatronen en gebruikte apparaten.

Medische gegevens. Gezondheids-informatie is gevoelige data.

Privé en werk informatie. Seksuele geaardheid is gevoelige data.

Stap 2: Beheren

Controleer hoe persoonsgegevens worden gebruikt en benaderd

De GDPR biedt personen op wie de gegevens betrekking hebben, meer controle over de manier waarop hun persoonlijke gegevens worden vastgelegd en gebruikt.
Betrokkenen kunnen bijvoorbeeld een verzoek indienen bij uw bedrijf om hun gegevens te delen, te verplaatsen naar andere services, fouten erin te corrigeren of om te verbieden dat bepaalde gegevens voor bepaalde doeleinden worden gebruikt. In sommige gevallen moet voldaan worden aan deze verzoeken binnen een vastgestelde periode.

Gegevenscontrole

Om aan de wensen van betrokkenen te voldoen, moet u weten welke types gegevens er binnen uw organisatie worden verwerkt, hoe dat gebeurt en voor welke doeleinden. De eerder aangegeven inventarisatie van gegevens is een goede eerste stap om te zetten. Is de inventarisatie afgerond, dan is de volgende belangrijke stap het ontwikkelen en implementeren van een gegevensbeheerplan. Dit plan ondersteunt bij het opstellen van beleid, rollen en verantwoordelijkheden voor de toegang, beheer en gebruik van persoonlijke gegevens. Tevens zorgt het ervoor dat activiteiten op het gebied van gegevensverwerking voldoen aan de GDPR. Met een gegevensbeheerplan heeft u de zekerheid dat uw organisatie tegemoet komt aan de eis van de betrokkenen om gegevens te verwijderen of te verplaatsen.

Sigmax ONE Identity

Met Sigmax ONE Identity zijn risico's op fouten, misbruik en administratieve rompslomp door een wildgroei aan wachtwoorden verleden tijd. Met deze cloud-oplossing is de toegang tot bestanden centraal achter de schermen geregeld. Iedere professional logt nog maar één keer in heeft vervolgens toegang tot een werkomgeving met alle applicaties waar hij/zij bij moet kunnen.

Sigmax ONE Identity

Stap 3: Beveiligen

Stel beveiligingscontroles in om kwetsbaarheden en gegevensschendingen te voorkomen, en erop te reageren

Organisaties zijn steeds meer doordrongen van het belang van informatiebeveiliging. Maar door de GDPR wordt de lat op dit gebied nog hoger gelegd. De nieuwe wet verplicht organisaties om de juiste technische en organisatorische maatregelen te nemen zodat persoonlijke gegevens beveiligd zijn tegen verlies en ongeautoriseerde toegang of openbaarmaking.

Uw gegevens beveiligen

Gegevensbeveiliging is een complexe zaak. Er zijn veel risico's waar rekening mee gehouden moet worden: een fysieke inbreuk, frauduleuze werknemers, hackers of onopzettelijk verlies. Met het opstellen van risicobeheerplannen en door risicobeperkende maatregelen te nemen, zoals wachtwoordbeveiliging, auditlogs en encryptie, kunt u voldoen aan de geldende wetten en regels.

Sigmax ONE Secure

Sigmax ONE Secure is een op maat voor u samengestelde mix van beveiligingsoplossingen waarmee u altijd en overal veilig werkt. Sigmax ONE Secure wordt als een totaaloplossing geïmplementeerd en volledig door Sigmax voor u beheerd. Beheer niet langer losse componenten, maar kies voor beveiliging die perfect aansluit op de unieke behoeften van uw organisatie.

Sigmax ONE Secure

Heeft u een mogelijke breuk ontdekt!?

1. Beoordeel de impact en ernst van de gebeurtenis.
2. Voer een technisch onderzoek uit en bepaal uw strategie voor de stappen 3 en 4.
3. Stel een herstelplan op de kwestie op te lossen. Stappen voor crisisbeheersing, zoals het in quarantaine plaatsen van besmette systemen, moeten direct worden uitgevoerd parallel aan de diagnose. Nadat het directe gevaar is geweken, moeten er wellicht risicobeperkende maatregelen worden ingesteld voor de lange termijn.
4. Maak een evaluatierapport van de incidentgegevens waaruit blijkt hoe uw beleid, procedures en processen wilt veranderen, zodat de gebeurtenis niet nogmaals plaatsvindt. Deze stappen komen overeen met Artikel 31 van de GDPR die verplicht om de omstandigheden van de inbreuk, het effect ervan en de uitgevoerde oplossingen vast te leggen.

Stap 4: Rapporteren

Onderneem actie op gegevensverzoeken, rapporteer inbreuk op gegevens en bewaar vereiste documentatie

Met de komst van GDPR worden er nieuwe standaarden gezet op het gebied van transparantie, accountability en het bijhouden van gegevens. U zult niet alleen transparanter moeten worden over hoe u omgaat met persoonsgegevens, maar ook over hoe u actief documentatie bijhoudt over processen voor persoonsgegevens en het gebruik ervan.

Bijhouden van records

Organisaties die werken met persoonlijke gegevens moeten overzichten bijhouden van hun verwerkingsdoelen, de categorieën waarbinnen de verwerkte gegevens vallen, de identiteit van externe partijen met wie de gegevens zijn gedeeld, of (en welke) andere landen persoonlijke gegevens ontvangen en de wettelijke basis van dergelijke overdrachten, organisatorische en technische beveiligingsmaatregelen en de bewaartijd van gegevens binnen verschillende datasets.

Rapportagetools en documentatie van cloudservices

Wat geldt voor andere databases en systemen waarmee persoonlijke gegevens worden verwerkt, geldt ook voor cloudservices: het is verplicht om nauwkeurig vast te leggen hoe deze services worden gebruikt en betreffende personen in uw organisatie moeten hiervan op de hoogte zijn.

Binnen uw organisatie moet duidelijk zijn welke persoonsgegevens door andere serviceproviders namens uw organisatie worden bewaard; via welke contractuele relatie deze serviceproviders worden gecontroleerd; en wat er gebeurt met de gegevens wanneer een servicerelatie wordt beëindigd.

Betrokkenen inlichten

Met de komst van de GDPR worden er ook strengere verplichtingen opgelegd aan gegevensverwerkers en op beheerders wat betreft het melden van inbreuken op persoonsgegevens die een risico opleveren voor de rechten en de vrijheden van een individu. Onder de nieuwe regelgeving, zoals staat vermeld in Artikelen 17, 31 en 32, moet de gegevensverwerker de gegevensbeheerder zonder oponthoud op de hoogte stellen van al zulk soort inbreuken op persoonsgegevens nadat ze zijn ontdekt.

Als de beheerder eenmaal van de schending weet, moet deze de relevante autoriteit voor gegevensbescherming binnen 72 uur op de hoogte stellen. Als de inbreuk leidt tot een hoog riscio voor de rechten en vrijheid van individuen, moet de beheerder ook de betreffende individuen op de hoogte stellen.

Grip op veiligheid

Het krijgen van grip start bij inzicht geven in de huidige situatie van veiligheid. Want pas als u weet welke risico's u loopt kunt u bepalen welke veiligheidsmaatregelen u moet treffen. Sigmax geeft u dat inzicht en biedt de ideale beveiligingsmix voor uw specifieke situatie. Behoefte aan dit inzicht? Laat een Security Scan uitvoeren.

Security Scan