

De AVG / GDPR naleving in vogelvlucht – Hoe VESA Network Solutions kan voldoen aan uw behoeften

Verkoopt uw organisatie goederen en services aan klanten van de Europese Unie (EU)? Houdt u gegevens over afzonderlijke verkopen of klantvoorkeuren bij voor EU-inwoners? Verzamelt u klantinformatie, waaronder gedrags-gegevens? Als u een van deze vragen met 'Ja' hebt beantwoord, is uw organisatie een van de vele organisaties die zal worden beïnvloed door de nieuwe Algemene Verordening Gegevensbescherming (AVG).



VESA Network Solutions helpt u beter te begrijpen wat u nú kunt doen om te verzekeren dat u de AVG naleeft tegen de deadline van **25 mei 2018**.

De AVG is ook wel bekend onder de Engelse naam: **General Data Protection Regulation (GDPR)**. De Wet bescherming persoonsgegevens (Wbp) geldt dan niet meer.

Wat is de AVG?

De AVG legt regels op voor organisaties die goederen en services bieden aan mensen in de Europese Unie (EU) of die gegevens over EU-inwoners verzamelen en analyseren, waar ter wereld ze dan ook zijn gevestigd.



Deze voorschriften omvatten:

Verbeterde persoonlijke privacyrechten met flexibeler beheer voor individuen om hun persoonlijke gegevens te bekijken en bewerken.

Grotere plicht om gegevens te beschermen, waaronder strengere richtlijnen voor vertrouwelijkheid en gegevensbewaring en transparantere beleidsregels voor gegevensverwerking.

Verplichte melding van gegevenslekken, personeelstraining in privacy en aanwijzing van een Data Protection Officer (in grotere organisaties).

Aanzienlijke sancties voor niet-naleving, waaronder hoge boetes wanneer een organisatie al dan niet met opzet de voorschriften niet naleeft.

Hoe ondersteunt VESA Network Solutions de AVG?

Wacht niet totdat de voorschriften in mei 2018 worden afgedwongen.



Begin de AVG-naleving door u te concentreren op vier belangrijke stappen:

1. Traceren

De eerste stap op weg naar AVG is het beantwoorden van de vraag of de AVG op uw organisatie van toepassing is en zo ja in welke mate.

2. Beheren

De AVG geeft de betrokkenen meer zeggenschap over de manier waarop hun persoonsgegevens worden verzameld en gebruikt.

3. Beveiligen

Organisaties worden zich weliswaar steeds bewuster van het belang van informatiebeveiliging, maar de AVG legt de lat nog een stuk hoger.

4. Rapporteren

De AVG stelt nieuwe normen aan transparantie, verantwoordingsplicht en verslaglegging.

U bent kortom verplicht:

1. Persoonsgegevens te beschermen
2. Melden van een beveiligingsincident bij Autoriteit Persoonsgegevens en betrokkene
3. Passende maatregelen te nemen
4. Reparatie lek en voorkomen verdere verspreiding
5. Registratie bijhouden van beveiligingsincidenten



Advies van VESA Network Solutions:

1. Eisen stellen aan betrouwbaarheid;
2. Technische en/of organisatorische maatregelen treffen;
3. Controle hierop inbouwen;
4. Beveiligingsmaatregelen periodiek onder de loep nemen of ze nog wel in lijn zijn met de techniek en zo nodig aanpassen;



5. Regel u privacy goed - Bekijk [hier](#) "PRIVACY GOED GEREGLD".
6. Handel datalekken goed af door procedures – Bekijk [hier](#) "PROCEDURE MELDING DATALEKKEN".