

Hoe voldoe in aan de GDPR/AVG met Aangetekend Mailen?

Wat is de General Data Protection Regulation (GDPR)/AVG?

Vanaf 25 mei 2018 is de General Data Protection Regulation (GDPR) als nieuwe Europese verordening van kracht, in Nederland bekend als de AVG (Algemene Verordening Gegevensbescherming).

Dankzij de AVG is de bescherming van persoonsgegevens in alle landen van de EU op dezelfde manier geregeld en gelden in elke lidstaat dezelfde regels.

Voldoet u al aan deze wetgeving?

Wat betekent dit nu eigenlijk voor bedrijven?

1. Uw activiteiten vallen veel sneller onder de privacywet;
2. Uw privacyverklaring moet nóg transparanter;
3. Alle datalekken moeten intern worden gedocumenteerd;
4. U moet alle verwerkingen van persoonlijke gegevens documenteren, ook de triviale zoals uw personeelsadministratie of nieuwsbrief;
5. U moet met al uw leveranciers en afnemers een zogeheten verwerkersovereenkomst sluiten;
6. Zitten er risico's aan een verwerking, dan moet u een complete privacy impact assessment (PIA) uitvoeren;
7. U moet zo min mogelijk privacygevoelige informatie verzamelen en deze zo snel mogelijk weer vernietigen;
8. Uw software en diensten moeten van de grond af aan rekening houden met privacy ('privacy by design');
9. Uw informatiebeveiliging moet op orde zijn én blijven;
10. U dient intern privacybeleid te publiceren waarin staat wie welke rol heeft bij de omgang met persoonsgegevens;
11. U moet kunnen omgaan met verzoeken van personen, zoals een verzoek om inzage of correctie van hun gegevens;
12. De boetes voor het overtreden van de AVG kunnen oplopen tot 20 miljoen euro of 4% van de wereldwijde jaaromzet.

Waarom is een standaard e-mail niet veilig genoeg?

Bij het versturen en ontvangen van een normale e-mail zijn meerdere partijen betrokken: de mailserver of internet service provider van de verzender, de mailserver of internet service provider van de ontvanger en eventuele anti-spam en antivirus partijen. Van de meeste van deze partijen heeft u hoogstwaarschijnlijk geen weet hoe ze hun beveiliging hebben ingericht.

Geen enkele garantie

Er is geen enkele garantie af te geven dat alle stappen in het e-mailproces door middel van veilige verbindingen hebben plaatsgevonden. Sommige mailservers versleutelen het transport, andere mailservers doen dat niet. Daarnaast kan de ontvangende partij de e-mail na ontvangst wijzigen, waardoor je als verzender met lege handen staat bij de bewijsvoering. Je kunt namelijk niet aantonen dat de inhoud is gewijzigd.

E-mail is een open systeem, zonder controle van de identiteit van de verzender. Hierdoor kunnen verzenders zich anders voordoen: men denkt een veilige e-mail te krijgen, maar dat is niet zo. Hierdoor kunnen er naast spam vervelende extra zaken bij een e-mail zitten zoals virussen.

Waarom is beveiligde e-mail belangrijk?

Bedrijven en organisaties die persoonsgegevens en bijzondere gegevens versturen via e-mail moeten maatregelen treffen waardoor die gegevens beschermd zijn tegen ongewenste inzage of ongewenste veranderingen. Een standaard e-mail is onvoldoende beschermd tegen ongewenste inzage of ongewenste veranderingen en voldoet daarmee dus niet aan de GDPR/AVG.

Waarom past Aangetekend Mailen volledig binnen de GDPR/AVG?

De AVG verplicht om privacygevoelige informatie beveiligd te versturen om datalekken te voorkomen en/of snel te traceren. Het versturen van privacygevoelige informatie per email is nu eenmaal gemakkelijk en brengt daarom ook de meeste risico's voor u en uw organisatie mee. Tijdens het versturen van een 'gewone' mail heeft u geen grip op het zendproces, zo kan de mail gehackt worden of per ongeluk aan de verkeerde persoon afgeleverd worden. Om te voorkomen dat u onbewust en onopgemerkt te maken krijgt met een datalek, kunt u voor dit soort gevoelige informatie de dienst Aangetekend Mailen inzetten.

Medewerkers kunnen op een eenvoudige manier vanuit hun vertrouwde mailomgeving privacygevoelige

informatie beveiligd en rechtsgeldig versturen. Tijdens het transport van uw vertrouwde gegevens wordt het bericht tussen afzender en ontvanger beveiligd, zodat alleen de geautoriseerde afzender en de daadwerkelijke ontvanger bij het bericht kunnen. Over de bijlage(n) wordt een 'fingerprint' berekend waarmee er ook zeker gesteld kan worden wat er tussen beide partijen is gecommuniceerd en samen met de uitgebreide track & trace wordt dit op een biljet weergegeven welke toegankelijk is via een dashboard.

Met Aangetekend Mailen voldoet ook uitgaande correspondentie dan ook aan alle eisen van de GDPR/AVG.