Crowe

ACA IT-Solutions, onderdeel van Crowe

Whitepaper:

GDPR (AVG Privacywet)

Ben jij voorbereid op de Europese privacywetgeving?

ACA IT-Solutions, onderdeel van Crowe

GDPR (AVG Privacywet)

De nieuwe Europese privacywet vereist grondige voorbereiding
Automatisering en digitalisering maken het (bedrijfs)leven een stuk makkelijker. Technologische ontwikkelingen volgen elkaar in rap tempo op. Anderzijds brengt dit ook risico's met zich mee. Bijvoorbeeld op het vlak van security en privacy. Regelmatig komt het voor dat persoonlijke gegevens van bijvoorbeeld klanten of medewerkers op straat komen te liggen of in verkeerde handen terecht komen.

Voor de Nederlandse overheid en de Europese Unie is bescherming van privacygevoelige gegevens een belangrijk punt. Daarom wordt de Wet bescherming persoonsgegevens (Wbp) vervangen door een meer allesomvattende, Europese variant die toegesneden is op het digitale tijdperk. Deze wet heet de General Data Protection Regulation (GDPR) en is nu al van kracht, maar zal vanaf 25 mei 2018 ook actief worden gehandhaafd door de Autoriteit Persoonsgegevens (AP). Dit betekent dat alle organisaties die persoonsgegevens verzamelen, bewerken of verwerken vanaf die datum GDPR compliant moeten zijn. Organisaties en hun medewerkers zullen zich daarom grondig moeten voorbereiden.

AUTORITEIT PERSOONSGEGEVENS

> *De GDPR-wetgeving is een belangrijke leidraad voor organisaties. De drijfveer moet zijn om altijd en overal veilig en respectvol met data en persoonsgegevens om te gaan.*
>
> Maarten de Rooij, IT Business Professional ACA IT-Solutions

GDPR-compliancy wordt voor iedere organisatie van levensbelang
De nieuwe wet is in het leven geroepen om de persoonlijke gegevens van individuen binnen de EU beter te beschermen en afspraken hieromtrent te harmoniseren. Op die manier kunnen Europese burgers er van op aan dat hun gegevens in alle EU-lidstaten op dezelfde manier worden behandeld en beveiligd. Voor vrijwel alle instanties en bedrijven heeft dit effect op de manier van documenteren van persoonsgegevens. Ook de definitie van wat een persoonsgegeven is wordt met de GDPR uitgebreid en specifieker gemaakt. Mede door deze verbreding van het begrip 'persoonsgegeven' beschikt vrijwel iedere organisatie over privacygevoelige informatie die onder de GDPR valt. Denk aan klantgegevens (ook zakelijke e-mailadressen), kopieën van legitimatiebewijzen, creditcard- en/of bankgegevens, werknemersgegevens, etc. Om ervoor te zorgen dat deze informatie adequaat wordt opgeslagen, gebruikt en beheerd, kent de GDPR tientallen richtlijnen en voorschriften.

ACA IT-Solutions, onderdeel van Crowe

Maatregelen GDPR niet vrijblijvend

Het voldoen aan de GDPR en het nemen van maatregelen is allerminst vrijblijvend. Het gebrek aan een sluitend privacybeleid vergroot namelijk de kans op een datalek. De Autoriteit Persoonsgegevens kan datalekken ten gevolge van nalatigheid fors bestraffen. De sancties variëren van waarschuwingen en bindende maatregelen, tot een maximale boete van 20 miljoen euro of 4% van de wereldwijde jaaromzet. Dit kan de draagkracht van een bedrijf te boven gaan en leiden tot een faillissement.

Dit is echter niet de enige reden om te zorgen dat de organisatie voldoet aan de privacy wetgeving. Een datalek en slecht beleid op dit vlak kunnen leiden tot enorme reputatieschade. De Autoriteit Persoonsgegevens zal in bepaalde gevallen, zeker als zich vaker datalekken voordoen bij een organisatie, incidenten publiekelijk bekend maken. Ook dienen de getroffenen van een datalek te worden geïnformeerd, wat mogelijk kan leiden tot negatieve media aandacht.

Basisprincipes van de GDPR

De GDPR-wetgeving heet in Nederland AVG (Algemene Verordening Gegevensbescherming, vervanger van de Wbp) en bestaat uit maar liefst 99 artikelen. In beginsel is er sprake van diverse basisprincipes die voor elke organisatie gelden:

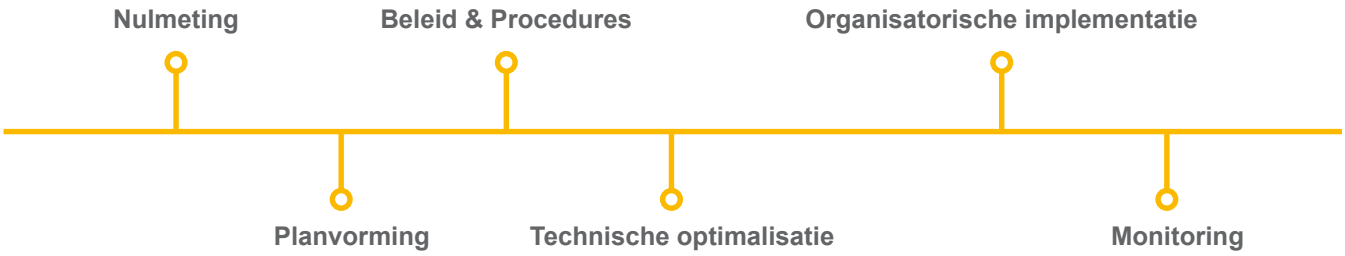
- ***Rechtmatigheid, eerlijkheid en transparantie*** **–** Persoonlijke data dienen op een rechtmatige, eerlijke en transparante manier verwerkt te worden in relatie tot personen waar de data betrekking op hebben.
- ***Integriteit en vertrouwelijkheid*** – Er dient sprake te zijn van adequate beveiliging van persoonlijke data, inclusief maatregelen tegen ongeautoriseerde of onrechtmatige verwerking en tegen onopzettelijk verlies, vernietiging of beschadiging.
- ***Data minimalisering*** **–** Alleen data opslaan en gebruiken die noodzakelijk is en uitsluitend beschikbaar is voor medewerkers die de data nodig hebben voor bedrijfsdoeleinden.
- ***Afbakening van het doel*** **–** Persoonlijke data mogen uitsluitend worden gebruikt voor duidelijke en rechtmatige doelen.
- ***Afbakening van de opslag*** **–** Persoonlijke data worden niet langer opgeslagen dan noodzakelijk is.

ACA IT-Solutions, onderdeel van Crowe

De oplossing: beveiligingsbeleid realiseren, uitvoeren en monitoren

De nieuwe wet gaat enorme impact hebben op de werk- en handelswijze in organisaties. Samengevat dienen ‘passende technische en organisatorische maatregelen’ genomen te worden voor de bescherming van privacy. Daar komt veel bij kijken. De oplossing voor een gedegen privacy beleid is drieledig:

1. Een goede beveiliging van de ICT-omgeving. De ICT-Security van jouw bedrijfsomgeving dient zo te zijn ingericht dat risico’s worden gemeden.
2. Van organisaties wordt verwacht dat er beleid en procedures worden gemaakt. Ook dienen documenten opgesteld te worden die afspraken met derden vastleggen (verwerkersovereenkomsten).
3. Beleid en procedures opvolgen. Dat vereist organisatorische aanpassingen. Alle medewerkers dienen op de hoogte te zijn van de do’s & dont’s en hiernaar te handelen.



Totaalaanpak van ACA IT-Solutions

Om als organisatie volledig GDPR-compliant te worden, zijn op technisch en organisatorisch vlak diverse stappen noodzakelijk. ACA IT-Solutions heeft specialisten in dienst die je gedurende het gehele traject begeleiden. Zowel uitvoerend, adviserend als beleidsmatig. Stapsgewijs nemen wij je mee in het proces om GDPR-compliant te worden en te blijven. Wij ondersteunen je met het maken van beleid en procedures. Bovendien helpen we om betrokkenheid en awareness te creëren bij jouw medewerkers.

Naast de organisatorische facetten is ook de beveiliging van de ICT-omgeving een belangrijke factor. Ook op technisch vlak kunnen wij je perfect ondersteunen. Wij hebben ruim 30 jaar ervaring met advies, ontwerp, installatie, beheer en ondersteuning (24x7) van ICT-omgevingen. Hiermee is ACA IT-Solutions een betrouwbare partner voor veel verschillende typen organisaties, van MKB tot Enterprise.

Advies & ondersteuning

Bij ACA IT-Solutions, onderdeel van Crowe, draait alles om de drie-eenheid Beleid, Techniek en Mens. Elk vraagstuk is een samenspel van deze elementen. Dat leidt tot innovatieve IT-bedrijfsoplossingen, waarbij continuïteit, beschikbaarheid en veiligheid essentieel zijn. Daarmee bereiken onze klanten een onderscheidend resultaat.

Contact

Wil je meer informatie of een afspraak maken? Neem dan contact met ons op via onderstaande contactgegevens.

Adresgegevens
ACA IT-Solutions, onderdeel van Crowe
Beukenlaan 40-50
5651 CD Eindhoven

Contactgegevens
040 - 8 800 100
info@aca-it.nl
www.aca-it.nl

ACA IT-Solutions, onderdeel van Crowe

Hoe *privacyproof* is jouw organisatie?
Gebruik onderstaande checklist en controleer of het privacy- en ICT-beleid van jouw organisatie aan de privacywetgeving voldoet. Deze checklist kan dienen ter ondersteuning en geeft een indicatie van de eisen.

Zijn de volgende verplichte onderwerpen al geregeld?

Hebben alle medewerkers een privacyreglement ontvangen? . . . . . JA NEE
Is voor alle medewerkers een actieplan beschikbaar bij een datalek? . . . . . JA NEE
Is bekend wie toegang heeft tot privacy- en persoonsgevoelige informatie? . . . . . JA NEE
Is privacygevoelige informatie zonder medeweten buiten de organisatie opgeslagen? . . . . . JA NEE
Is er een verantwoordelijke bij gebruik sociale media door medewerkers? . . . . . JA NEE
Heeft je veiligheidsfunctionaris een reglement voor intern privacy- en ICT-beheer? . . . . . JA NEE
Is er toestemming om persoonsgegevens van klanten op te slaan? . . . . . JA NEE
Is er toestemming voor de publicatie van beeldmateriaal van medewerkers? . . . . . JA NEE
Zijn alle medewerkers geïnformeerd over de geldende Wet bescherming persoonsgegevens? . . . . . JA NEE
Worden privacygevoelige gegevens, die niet noodzakelijk zijn voor de organisatie, tijdig verwijderd? . . . . JA NEE
Is een stappenplan voor de uitvoering van het privacybeleid voor medewerkers beschikbaar? . . . . . JA NEE
Is er een protocol voor melding, registratie en verwerking van beveiligingsincidenten? . . . . . JA NEE
Is de privacybescherming geregeld wanneer een medewerker de organisatie verlaat?. . . . . JA NEE
Is er een verwerkersovereenkomst naar alle externe bewerkers gestuurd?. . . . . JA NEE
Is bepaald wie toegang heeft tot privacygevoelige gegevens (zowel in- als extern)?. . . . . JA NEE
Is het meldingsnummer van de Autoriteit Persoonsgegevens in de records verwerkt? . . . . . JA NEE
Voldoen alle externe bewerkers aan de criteria van de privacywetgeving? . . . . . JA NEE
Zijn alle externe bewerkers verzekerd tegen aansprakelijkheid bij datalekken? . . . . . JA NEE
Zijn de juiste wettelijke stappen gevolgd voor invoering ICT-gebruiksbeleid? . . . . . JA NEE
Is er een sluitend ICT-gebruiksreglement voor medewerkers? . . . . . JA NEE
Voldoen eigen devices van medewerkers (mobiles, tablets, laptops) aan de ICT-Security eisen? . . . . . JA NEE
Wordt gecontroleerd of medewerkers op eigen devices (BYOD) geen illegale software hebben?. . . . . JA NEE
Is er een overzicht van uitgevoerde technische maatregelen beschikbaar?. . . . . JA NEE
Zijn de preventieve maatregelen bij de medewerkers onder de aandacht gebracht?. . . . . JA NEE

Heb je meerdere vragen met nee beantwoord of twijfelt u hieraan?
Neem geen risico en neem contact met ons op. Wij komen graag bij je langs voor een vrijblijvend adviesgesprek.