Computers and Communications N.V.

IP Hoge Bunders
Ambachtsstraat 8
B-9700 Oudenaarde
Tel.: 32 (0)55 30 03 20

info@cac.be
www.cac.be

BTW: BE 0434.990.956

Nota rond General Data Protection Regulation (GDPR-wetgeving)

Computers and Communications N.V.

IP Hoge Bunders
Ambachtsstraat 8
B-9700 Oudenaarde
Tel.: 32 (0)55 30 03 20

info@cac.be
www.cac.be

BTW: BE 0434.990.956

1. GDPR IN MENSENTAAL

Wat is GDPR en wat wil dit zeggen voor mijn bedrijf?

U heeft ongetwijfeld al gehoord van de **GDPR**-wetgeving die ingaat op **25 mei 2018**. GDPR is de afkorting voor ***General Data Protection Regulation***. In het Nederlands spreken we van **AVG** of ***Algemene Verordening Gegevensbescherming,*** maar ook in België gebruiken we vaker de afkorting GDPR. Simpel uitgelegd is dit een verzameling van regels om de **gegevens van Europese burgers** beter te **beschermen**, maar wat houdt dit nu juist in? Hoe zorg ik ervoor dat mijn bedrijf aan deze wetgeving voldoet en dus geen strenge boetes krijgt? Lees verder om een antwoord te krijgen op al uw vragen.

2. WAT HOUDT GDPR IN?

De nieuwe GDPR-wetgeving introduceert eengemaakte regels over de **beveiliging én de opslag** van persoonlijke gegevens. Het gaat hier zowel om de persoonlijke gegevens van **klanten** als van uw eigen **werknemers**.
De wet geldt voor de hele Europese Unie en bestaat uit twee delen. Langs de ene kant hebt u de ***Regulation*** waar de **bedrijfswereld** zich aan moet houden en daarnaast hebt u de ***Directive*** die van toepassing is voor **overheidsdiensten** zoals politie en justitie. Een belangrijk onderscheid.

3. OVER WELKE GEGEVENS GAAT HET?

- **Persoonlijke gegevens** zoals naam, geslacht, geboortedatum, adres, …
- **Online gegevens** zoals zoekgeschiedenis, cookies, e-mail, …
- **Financiële gegevens** zoals bankrekening, inkomen, belastingen, …
- **Juridische informatie** zoals veroordelingen, boetes, …
- **Sociale media** zoals Facebook, LinkedIn, Twitter, …
- **GPS-gegevens** zoals reisinformatie, GPS, …
- **Medische gegevens** zoals vaccinaties, ziekenhuisinfo, …
- **Etnische gegevens** zoals culturele voorkeuren, religies, …
- **Winkelgedrag** zoals winkelaankopen, direct marketing, …

4. DE GEVOLGEN VOOR UW BEDRIJF EN HOE VOORBEREIDEN

De wetgeving gaat in vanaf **mei 2018** en geldt voor **iedereen die goederen of diensten aanbiedt in de Europese Unie**. Vanaf dan moet u als bedrijf dus kunnen aantonen dat u voldoet aan de nieuwe wet. Dit gaat zowel over de **manier van verzamelen** van persoonlijke gegevens als over het opslaan in datacenters of in een **cloud buiten de EU**. Voor de meeste bedrijven is dit een enorme aanpassing.

Gelukkig heeft de privacy commissie enkele richtlijnen opgesteld om uw bedrijf zo goed mogelijk voor te bereiden.

- ***Transparantie***: U moet op een begrijpelijke manier uitleggen hoe de data wordt verzameld en verwerkt.
- ***Recht om vergeten te worden***: Wanneer een persoon aan uw bedrijf vraagt om de persoonsgegevens te wissen dan bent u dit verplicht. Ook als de data al gedeeld werd met derde partijen.

IP Hoge Bunders
Ambachtsstraat 8
B-9700 Oudenaarde
Tel.: 32 (0)55 30 03 20
info@cac.be
www.cac.be
BTW: BE 0434.990.956

- ***Meldplicht***: Is er een datalek? U bent verplicht om dit binnen de 72 uur te melden, tenzij u kan aantonen dat het geen gevaar vormt voor de persoonsgegevens.
- ***Data-overdracht***: Burgers kunnen hun gegevens overdragen van de ene dienstverlener naar de andere. Voorbeeld: internetprovider.

5. WAT ZIJN DE SANCTIES?

Als u niet voldoet aan de GDPR-wetgeving dan hangen er **hoge boetes** boven uw hoofd. Bij een 'lichte schending' kan het gaan over 2% van uw jaarlijkse omzet. De maximale boete kan oplopen tot €20 miljoen of 4% van uw jaarlijkse omzet.

Toch zal het met die boetes waarschijnlijk niet zo'n vaart lopen, of toch niet wat betreft de vooropgestelde hallucinant hoge bedragen. Net zoals sommige bedrijven niet klaar zullen zijn, zal ook onze overheid de deadline van 25 mei 2018 niet halen. De privacy commissie is zich volop aan het omvormen tot de gegevensbeschermingsautoriteit (GBA). Van een puur adviserend orgaan zal ze evolueren naar een instantie die meldingen van datalekken ontvangt, klachten onderzoekt, boetes instelt en int. Maar die mensen zijn er nog niet.

Laat ons daarom GDPR niet langer gebruiken om bedrijven nodeloos bang te maken. Laat ons GDPR zien als een startsein om verder te denken dan persoonlijke gegevens en een goede beveiliging van data in het algemeen na te streven.

6. EEN TOEZICHTHOUDER BINNEN UW BEDRIJF

Omdat de GDPR-richtlijnen een grote impact hebben op uw bedrijf is het belangrijk om een **Data protector verantwoordelijke** aan te stellen. Deze persoon kent de nieuwe wetgeving en controleert of alles nauwkeurig wordt opgevolgd.

Als bedrijf is het belangrijk om na te denken hoe U intern met data omgaat en hierover een **DPIA** ofte ***Data Protection Impact Assessment*** uit te voeren. Dit is een instrument waarmee u de privacy risico's van **een gegevensverwerking in kaart kan brengen**. Hoewel wij een DPIA ten zeerste aanraden, is het enkel verplicht wanneer de gegevensverwerking een **hoog privacy risico** oplevert. Na het uitvoeren van de DPIA kan U als bedrijf aanpassingen doorvoeren of zich laten **adviseren** om de risico's te verkleinen of weg te werken.
Wanneer de regels niet worden nageleefd heeft het bedrijf de volledige aansprakelijkheid.

Vergeet ook niet alle medewerkers in te lichten inzake GDPR, zodat iedereen weet wat er nog moet gebeuren binnen het bedrijf om te voldoen aan de nieuwe wetgeving.
De Belgische Privacycommissie heeft een volledige stappenplan opgemaakt hoe met deze nieuwe regels om te gaan, u kan het hier downloaden.
Link naar de website van de Commissie voor de bescherming van de persoonlijke levensfeer:
https://www.privacycommission.be/nl/algemene-verordening-gegevensbescherming-0

Computers and Communications N.V.

IP Hoge Bunders
Ambachtsstraat 8
B-9700 Oudenaarde
Tel.: 32 (0)55 30 03 20

info@cac.be
www.cac.be

BTW: BE 0434.990.956

7. VOORKOMEN IS BETER DAN GENEZEN!

Kan ik mijn organisatie voor 100% beschermen tegen incidenten met privacygevoelige informatie?
Het antwoord daarop is: Nee.

Wij als C&C en DiAS DMS/CRM en DiAS FIN/ERP bieden U een basis om GDPR gevoelige info te lokaliseren en te bepalen hoe hiermee intern omgegaan kan/mag worden volgens uw interne procedures, maar het nemen van maatregelen kan de kans op grote schade fors verlagen. U bent dit niet alleen volgens de wet verplicht, maar zeker ook moreel gezien voor alle mogelijke betrokken.

Wij kunnen ons heel goed voorstellen dat u zich afvraagt of u voldoende maatregelen hebt genomen om datalekken te voorkomen. Bij vragen aarzel niet om ons te contacteren via e-mail naar dpm@cac.be .

Wij helpen graag!