



© Copyright MERITIUS® Antwerpen

Verdienstelijk in recht

In dit nummer

GDPR: Wat moet u weten? Hoe kunnen wij u helpen?..... 1

GDPR: Hoe wordt u compliant? – Stappenplan..... 2

Onze diensten..... 3

GDPR: Wat moet u weten? Hoe kunnen wij u helpen?

Bryan ROUTH

1. WAT?

De General Data Protection Regulation (of Algemene Verordening Gegevensbescherming) is een Europese richtlijn die in werking treedt op 25/05/2018 en die betrekking heeft op het beheer en de beveiliging van persoonsgegevens.

Vanaf 25 mei zal uw organisatie moeten kunnen aantonen welke persoonsgegevens u verzamelt, hoe u deze data gebruikt en hoe u ze beveiligt. De GDPR houdt een overstap in naar een accountability-systeem. Alles zal dus gemotiveerd en gedocumenteerd dienen te worden teneinde dit te kunnen voorleggen in het geval van een controle.

2. WIE?

De GDPR is van toepassing op alle ondernemingen gevestigd in de Europese Unie, alsook op ondernemingen gevestigd buiten de Europese Unie die diensten aanbieden binnen de Europese Unie.

Alle KMO's vallen er dus onder.

3. WAAROM?

Sancties!

De GDPR voorziet in zware boetes voor overtredingen. Zo worden boetes voorzien tot €10.000.000 of 2 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit hoger is voor de lichtere overtredingen en tot €20.000.000 of 4 % van de totale wereldwijde jaaromzet in het voorgaande boekjaar, indien dit hoger is voor de zware overtredingen.

Dit zijn uiteraard maximumboetes en er zal rekening gehouden worden met uw inspanningen in het kader van de GDPR om de uiteindelijke boete te bepalen.

Verder is men ook aansprakelijk voor de scha-

de die door de betrokkenen wordt geleden en natuurlijk de imagoschade t.a.v. (potentiële) klanten en partners. De rapporten van de gegevensautoriteit zijn immers in principe openbaar en het risico dat de media de overtredingen oppikt is dan ook reëel.

De gegevensautoriteit kan ook een staking van de verwerkingen opleggen, hetgeen uiteraard een ernstig probleem voor de bedrijfsvoering kan zijn.

4. PERSOONSgegevens?

Het begrip persoonsgegevens in de richtlijn is zeer ruim. Het heeft betrekking op alle informatie over een natuurlijke persoon die het mogelijk maakt om deze op een directe en indirecte manier te identificeren (vb.: rechtstreeks werkmailadres, IP-adres, gegevens eenmanszaak,...).

Ook verwerken wordt zeer ruim gedefinieerd. Zo wordt ook het louter opslaan van gegevens gezien als verwerking.

5. HOE KUNNEN WIJ U HELPEN?

Het mag duidelijk zijn dat het toepassingsgebied van de GDPR zeer ruim is en u dus het nodige zal moeten doen om GDPR-compliant te zijn.

Om u te helpen de nodige stappen te nemen zal u hierbij een concreet stappenplan kunnen vinden, alsook een model van het gegevensregister zoals voorgeschreven door de gegevensautoriteit.

Verder bieden wij u ook de nodige modeldocumenten aan voor een vaste prijs.

Wij verzorgen ook presentaties op locatie en ook voor meer gedetailleerde en sectorspecifieke adviezen kan u bij ons terecht.



MERITIUS
ADVOCATEN - AVOCATS

GDPR: Hoe wordt u compliant? - Stappenplan

Bryan ROUTH

1. INFORMEREN

Informeer de oversten, kaderleden en de mensen die instaan voor de gegevensverwerking over de aankomende veranderingen. Zij zullen deze moeten invoeren, toepassen en zullen ook kunnen helpen bij het samenstellen van de lijsten van gegevens.

2. GEGEVENSREGISTER

Breng in kaart welke persoonsgegevens je bijhoudt, waarom je ze bijhoudt, waar deze vandaan komen en met wie je deze deelt. Breng dit samen in een gegevensregister. Eventueel dient u hiervoor een gegevens-audit te laten uitvoeren. Ga ook na hoelang je deze gegevens moet bijhouden.

Deel de verschillende gegevens in in types en identificeer de wettelijke grondslag voor elk type.

3. TOESTEMMING

Voor de types gegevens waarvoor je geen wettelijke grondslag hebt, heb je toestemming nodig. Zorg voor een wijze van toestemming vragen, verkrijgen en registreren die conform de GDPR is. De toestemming moet immers vrij, specifiek, geïnformeerd en ondubbelzinnig zijn en kan bovendien worden ingetrokken.

Voor minderjarige kinderen (-16 jaar) dient toestemming te worden gevraagd aan de ouder(s) of voogd(en). Zorg er dus voor dat je de leeftijd van de betrokkene kan nagaan.

4. RECHTEN VAN DE BETROKKENE

Incorporeer alle rechten waarop de betrokkene zich kan beroepen in de procedures van je bedrijf. Hou hierbij ook rekening met hoe persoonsgegevens kunnen worden verwijderd en hoe gegevens elektronisch zullen worden meegeëld binnen de voorgeschreven termijnen, zowel voor overdracht van de gegevens op vraag van de betrokkene, als voor de mededeling van persoonsgegevens aan de betrokkene. U zal zich dus o.a. volgende vragen dienen te stellen: Wie neemt de beslissing? Zijn je systemen hier toe uitgerust?

5. PRIVACYVERKLARING

Stel een privacyverklaring op of werk je bestaan de privacyverklaring bij rekening houdend met de GDPR.

6. DATALEKKEN

Werk adequate procedures uit om datalekken op te sporen, te rapporteren en te onderzoeken. Zorg tevens voor (model)documenten om beslissingen, o.a. omtrent het al dan niet rapporteren, te staven.

7. GEGEVENSBESCHERMING DOOR ONTWERP EN GEGEVENSBE-SCHERMINGSEFFECTBEOORDE-LING

De nieuwe "Good practices" houden in dat "Privacy by design" wordt geïmplementeerd in uw bedrijf en op de gepaste momenten, bij hoge risicosituaties, een "Privacy impact assessment (PIA)" wordt uitgevoerd.

8. DPO (DATA PROTECTION OFFICER)

Ga na of u verplicht bent om een DPO aan te stellen en duid deze desgevallend aan (intern of extern) conform de GDPR. Alleszins is het aangewezen een verantwoordelijke aan te duiden die de naleving van de databeschermingsregels opvolgt. Indien een DPO niet verplicht is, is het aangewezen deze functie anders te benoemen.

9. INTERNATIONAAL

Bepaal onder welke toezichthoudende autoriteit je valt indien jouw bedrijf of organisatie internationaal actief is.

10. BESTAANDE CONTRACTEN

Pas uw bestaande contracten, o.a. met verwerkers (leveranciers) en onderaannemers, aan rekening houdend met de GDPR. Ook bij outsourcing dienen de nodige veiligheidsmaatregelen contractueel geregeld te worden.

**GDPR COMPLIANT IN
10 STAPPEN**





MERITIUS
ADVOCATEN - AVOCATS

Onze diensten:

Bryan ROUTH

Teneinde u te begeleiden bij de aanpassingen die nodig zijn binnen de GDPR, kunnen wij u onder andere van dienst zijn met het volgende:

- Opleidingen binnen uw bedrijf (personeel, kaderleden, ...)
- Modeldocumenten (vaste prijs) en het personaliseren ervan
- Opstellen van een privacyverklaring
- Bijstand bij het samenstellen van uw gegevensregister en het bepalen van de rechtmatigheidsgronden
- Sectorspecifieke adviezen en opleidingen
- Aanpassen/ opstellen van contracten met verwerkers / leveranciers / bij outsourcing
- Advies omtrent de bevoegde gegevensautoriteit
- Bijstand bij het uitvoeren van een informatie-audit
- Advies omtrent bewaringstermijnen van gegevens

Onze kantoren

MERITIUS® GENT

Keiskantstraat 74 - 9031 Gent (Drogen)
Tel. +32 (0)476 21 83 77
info.gent@meritius.be

MERITIUS® BRUXELLES

Avenue Georges Henrilaan 431 - 1200 Bruxelles
Tel. +32 (0)2 735 91 56 - Fax +32 (0)2 734 35 00
info.brussels@meritius.be

MERITIUS® MONS

Rue Ste Gertrude 1 - 7070 Le Roeulx
Tel. +32 (0)64 66 50 12 - Fax +32 (0)64 67 60 93
info.mons@meritius.be

MERITIUS® NAMUR

Rue des Aubépines 44 - 5101 Namur (Erpent)
Tel. +32 (0)81 32 22 70 - Fax +32 (0)81 32 22 79
info.namur@meritius.be

MERITIUS® ANTWERPEN

Jules Moretuslei 374-376 - 2610 Antwerpen
Tel. +32 (0)3 825 55 00 - Fax +32 (0)3 825 56 00
info.antwerpen@meritius.be

Bezoek ook onze website: <http://www.meritius.be>



MERITIUS is a member of **CYRUS ROSS INTERNATIONAL EEIG**

With member offices in Austria, Belgium, Bulgaria, Denmark, Finland, France, Germany, Great Britain, Ireland, Italy, Luxembourg, Netherlands, Norway, Portugal, Spain, Sweden, Switzerland

www.cyrusross.com