Ywein Van den Brande

Het Praktijkboek Informaticarecht 3:
Recht rendeert voor uw onderneming

Wat de Projectmanager en Paralegal moet weten over informaticarecht gebundeld in een deskundige gids.

Update 2017

Crealaw

www.crealaw.eu

Het Praktijkboek Informaticarecht

Wat u moet weten over informaticarecht gebundeld in een praktische en deskundige gids.

Ywein Van den Brande
www.crealaw.eu

Crealaw

ISBN 978-1-61979-532-7

Uitgever:
Crealaw Ict Law Partners bvba
Witte Patersstraat 4
1040 Brussel
O.N. 0832.298.008

Inhoudsopgave

Voorwoord

De eerste versie van het Praktijkboek Informaticarecht verscheen in 2012, en de tweede in 2015. Ze bewezen hun nut voor zowel de project manager, de CEO als voor de praktijkjurist die graag hands-on adviseert. Maar net zoals technologie evolueert recht snel. Dus is het tijd voor alweer een nieuwe update.

Ter gelegenheid van deze update is het Praktijkboek grondig bijgewerkt en aangevuld met nieuwe hoofdstukken en tips, zoals privacy en de SLA. Dit maakt dat de gids grondiger en volledi ger is dan voorheen.

Meer nog dan de vorige versies focust het boek op het principe “Recht Rendeert”. Ieder bedrijf heeft een aantal competitieve voordelen. Deze kunnen liggen in IP, klantencontracten, personeel ... maar hoe bescherm je deze assets en hoe kan je ze valoriseren? Een correct begrip van de juridische spelregels en het afsluiten van goede contracten maakt dat deze competitieve voordelen optimaal renderen. De derde versie van het Praktijkboek Informaticarecht is een waardevolle basis voor iedereen die met IT recht te maken krijgt.

Ik dank Jeroen November die ook deze versie weer heeft nagelezen.

Voor vragen, opmerkingen of suggesties kan u mij steeds contacteren: ywein@crealaw.eu.

Ik wens u alvast veel leesplezier.

Ywein, april 2017

H. Territoriale toepassing en bevoegde toezichthoudende autoriteit

a. Wanneer is de AVG van toepassing?

Wanneer de verwerkingsverantwoordelijke binnen de Europese Unie is gevestigd, dan is de AVG van toepassing op alle persoonsgegevens die door hem worden verwerkt.

Bv. een Belgische internetshop zal de AVG moeten respecteren voor al zijn klantgegevens, ook indien deze Amerikaanse consumenten betreffen. Hij moet de AVG zelfs toepassen indien hij beslist om alle servers in de Verenigde Staten te installeren.

Wanneer de verwerkingsverantwoordelijke niet in de Europese Unie is gevestigd, dan is de AVG van toepassing wanneer de verwerking van persoonsgegevens:

- betrekking heeft op het aanbieden van goederen of diensten aan personen binnen de Europese Unie;
- betrekking heeft op het observeren van het gedrag van personen, als dit gedrag plaatsvindt binnen de Europese Unie.

Enkele voorbeelden:

Indien een Japanse producent elektronica verkoopt op de Europese markt, dan is de AVG van toepassing op de persoonsgegevens van zijn Europese klanten. Zijn Japanse klanten genieten deze bescherming niet.

Indien een Amerikaans direct marketingbedrijf profielen opstelt van Europese internetgebruikers dan is de AVG van toepassing. Op de profielen van Amerikaanse consumenten in de Verenigde Staten is de verordening niet van toepassing.

De AVG is dus van toepassing van zodra personen op het Europese grondgebied betrokken zijn. Waar de middelen van de verwerking gevestigd zijn, is voor het bepalen van het toepassingsgebied van de AVG niet van belang.

b. Doorgifte naar buitenland

Vermits de AVG overal binnen Europa geldt, mogen persoonsgegevens binnen Europa worden doorgegeven. Doorgeven buiten Europa is evenwel verboden.

Op dit verbod bestaan een beperkt aantal uitzonderingen, zoals:

- De Europese Commissie kan voor een bepaald land, sector of organisatie specifiek toestemming geven (het zogenaamde adequaatheidsbesluit).
- Machtigingen via voorafgaandelijk door de Europese Commissie of toezichthoudende autoriteiten goedgekeurde bindende documenten zoals bindende bedrijfsvoorschriften, standaardbepalingen voor gegevensbescherming, gedragscodes of certificaten.
- Door een toezichthoudende overheid goedgekeurde overeenkomst met de verwerkingsverantwoordelijke buiten Europa.

Verder is de doorgifte ook mogelijk voor volgende redenen:

- De doorgifte is noodzakelijk voor de uitvoering van een overeenkomst tussen de betrokkene en de verwerkingsverantwoordelijke of voor de uitvoering van precontractuele maatregelen die op verzoek van de betrokkene zijn genomen.
- De doorgifte is noodzakelijk voor de sluiting of de uitvoering van een overeenkomst die, in het belang van de betrokkene, werd afgesloten tussen de verwerkingsverantwoordelijke en een andere, natuurlijke persoon of rechtspersoon.
- Rechtsvordering: de doorgifte is noodzakelijk voor de instelling, uitoefening of onderbouwing van een rechtsvordering.
- Het algemeen belang: de doorgifte is noodzakelijk wegens gewichtige redenen van algemeen belang.
- De toestemming: de betrokkene heeft uitdrukkelijk met de voorgestelde doorgifte ingestemd, na te zijn ingelicht over de risico's die dergelijke doorgiften kunnen inhouden.

- De doorgifte is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke en de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene wegen niet zwaarder. Dit is een uitzonderingsregel die slechts beperkt kan worden toegepast en die aan de betrokkene en de toezichthoudende autoriteit dient te worden gemeld.

c. Bevoegde toezichthoudende autoriteit

De AVG geldt voor alle lidstaten van de Europese Unie. Het is dan ook niet logisch dat een dienstverlener die in een groot aantal lidstaten actief is met iedere toezichthoudende autoriteit zou moeten communiceren.

Daarom heeft de AVG het één-loketmechanisme ingevoerd.
Eén toezichthoudende autoriteit is de enige gesprekspartner van de verwerkingsverantwoordelijke. Dit is de autoriteit van de lidstaat waarin de verwerkingsverantwoordelijke zijn hoofdvestiging heeft. Met hoofdvestiging wordt de centrale administratie van het bedrijf bedoeld. In geval de verwerking van de persoonsgegevens in een bijzondere vestiging zouden plaatsvinden (bv. de hoofdzetel is in Brussel, maar de marketingactiviteiten zijn gecentraliseerd in Parijs) dan is de autoriteit van de lidstaat waar de beslissingen over de persoonsgegevens worden genomen, bevoegd.

Er bestaat wel een samenwerkingsmechanisme waardoor diverse toezichthoudende autoriteiten samen kunnen optreden. Dit is onder meer het geval wanneer een autoriteit in een lidstaat op basis van bovenstaande regel bevoegd is, en:

- de verwerkingsverantwoordelijke gevestigd is op het grondgebied van de lidstaat van een andere toezichthoudende autoriteit;
- betrokkenen in een andere lidstaat wezenlijke gevolgen ondervinden of waarschijnlijk zullen ondervinden;
- bij de toezichthoudende autoriteit in een andere lidstaat een klacht werd ingediend.

Om van dit één-loketmechanisme te kunnen genieten, moet de verwerkingsverantwoordelijke een vestiging hebben in Europa. Wanneer dat niet het geval is, kan hij geen gebruik maken van dit mechanisme en moet hij zich afzonderlijk richten tot alle toezichthoudende autoriteiten.

I. Afdwingen en sancties

a. Afdwingen door de betrokkene

De betrokkende die van oordeel is dat zijn rechten zijn geschonden, heeft een hele reeks mogelijkheden.

Klacht indienen bij de toezichthoudende autoriteit: de meest voor de hand liggende optie is het indienen van een klacht bij de toezichthoudende overheid. Dit is een laagdrempelige procedure. De toezichthoudende autoriteit is verplicht om de klacht te behandelen en de betrokkene in te lichten over de afhandeling ervan.

Dergelijke klacht kan worden ingediend in de lidstaat waar de betrokkene gewoonlijk verblijft, zijn werkplek heeft of waar de beweerde inbreuk is begaan.

Klacht tegen de toezichthoudende autoriteit: de AVG voorziet de mogelijkheid om een klacht in te dienen tegen de toezichthoudende autoriteit wanneer deze een klacht niet of niet volledig behandelt, niet informeert over de opvolging van de klacht of over de uitkomst na de behandeling van de klacht (binnen de 3 maanden). Ook tegen ieder juridisch bindend besluit van de toezichthoudende overheid kan klacht worden ingediend.

Rechtbank: De mogelijkheid van het indienen van een klacht bij de rechtbank is een bijkomende mogelijkheid. Iedereen die zich geschaad voelt in zijn rechten, kan zich steeds tot de gewone rechter richten. Deze kan alle nuttige maatregelen opleggen aan de verantwoordelijke om de naleving van de AVG af te dwingen. Indien nodig kan hij een dwangsom opleggen en schadevergoeding toekennen.

De AVG voorziet in een volledige vergoeding van de geleden schade. Interessant om weten is dat wanneer meerdere verwerkers en verwerkingsverantwoordelijken gezamenlijk bij dezelfde verwerking betrokken zijn en verantwoordelijk worden gesteld voor de schade die door de verwerking

is veroorzaakt, zij allen afzonderlijk voor de gehele schade aansprakelijk worden gehouden. Deze regel wil garanderen dat de betrokkene in elk geval een effectieve schadevergoeding ontvangt. Diegene die de schade heeft betaald, kan zich vervolgens keren tegen zijn collega's.

De gerechtelijke procedure kan worden ingesteld bij de gerechten van de lidstaat waar de verwerkingsverantwoordelijke een vestiging heeft (een vestiging volstaat, het moet niet gaan om de hoofdzetel) of waar de betrokkene gewoonlijk verblijft.

Via een collectieve instelling: De AVG voorziet de mogelijkheid dat bepaalde organisaties en verenigingen kunnen opstreden in het belang van de betrokkenen. Dit kan met of zonder hun mandaat, afhankelijk van het recht van de lidstaat waarin deze optreden.

b. Afdwingen door de toezichthoudende autoriteit

1° Algemene maatregelen

De toezichthoudende autoriteit kan een hele reeks maatregelen nemen, gaande van een eenvoudige waarschuwing tot zeer ingrijpende maatregelen. Meer heeft ze de mogelijkheid om:

- de verwerkingsverantwoordelijke te waarschuwen;
- de verwerkingsverantwoordelijke te berispen;
- de verwerkingsverantwoordelijke te gelasten de verzoeken van de betrokkene in te willigen;
- de verwerkingsverantwoordelijke te gelasten zijn verwerkingen in overeenstemming te brengen met de bepalingen van de AVG;
- de verwerkingsverantwoordelijke te gelasten een inbreuk in verband met persoonsgegevens aan de betrokkene mee te delen;
- een tijdelijke of definitieve verwerkingsbeperking, waaronder een verwerkingsverbod, op te leggen;
- de rectificatie of de wissing van persoonsgegevens te gelasten;
- een certificering of certificeringsorgaan te gelasten een certificering in te trekken;
- de opschorting te gelasten van gegevensstromen naar een derde land.

2° Boetes

De toezichthoudende autoriteit heeft eveneens de bevoegdheid om administratieve geldboeten op te leggen die doeltreffend, evenredig en afschrikkend zijn. Hierbij kan rekening worden gehouden met verzachtende en verzwarende omstandigheden.

Hieronder een aantal elementen waarmee rekening kan worden gehouden:

- De aard, de ernst en de duur van de inbreuk, rekening houdend met de aard, de omvang of het doel van de verwerking in kwestie alsmede het aantal getroffen betrokkenen en de omvang van de door hen geleden schade;
- De opzettelijke of nalatige aard van de inbreuk;
- De maatregelen die de verwerkingsverantwoordelijke of de verwerker hebben genomen om de schade te beperken die de betrokkenen hebben geleden;
- De mate waarin de verwerkingsverantwoordelijke of de verwerker verantwoordelijk is, gezien de technische en organisatorische maatregelen die hij heeft uitgevoerd;
- Eerdere relevante inbreuken die de verwerkingsverantwoordelijke of de verwerker hebben begaan;
- De mate waarin er met de toezichthoudende autoriteit is samengewerkt om de inbreuk te verhelpen en de mogelijke negatieve gevolgen daarvan te beperken;
- De categorieën van persoonsgegevens waarop de inbreuk betrekking heeft;
- De wijze waarop de toezichthoudende autoriteit kennis heeft gekregen van de inbreuk, met name of, en zo ja in hoeverre, de verwerkingsverantwoordelijke of de verwerker de inbreuk heeft gemeld.

Wanneer de verwerkingsverantwoordelijke en de verwerker zich niet houden aan hun verplichtingen, kunnen boetes worden opgelegd tot

10.000.000 Euro of, ingeval van een onderneming, tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar.

Wanneer de algemene beginselen inzake gegevensbescherming alsook de rechten van de betrokkenen niet worden gerespecteerd, kunnen deze oplopen tot 20.000.000 Euro of, ingeval van een onderneming, tot 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar.

De opgelegde boetes kunnen dus bijzonder hoog zijn. Dit is de bedoeling van de AVG, vermits zij een afschrikkend karakter moeten hebben.

5. De nieuwe ePrivacyverordening

A. Inleiding

Net zoals de privacyrichtlijn tegen 25 mei 2018 vervangen wordt door de Algemene Verordening Gegevensbescherming (zie hoger), wil de Europese Commissie met ingang van dezelfde datum ook de huidige ePrivacyrichtlijn 2002/58/EG vervangen door een verordening. De Europese Commissie diende hier een officieel voorstel toe in.

De keuze voor een verordening betekent dat -als het voorstel aanvaard wordt door de Raad en het Europees Parlement- de ePrivacyverordening eenvormig van toepassing zal zijn in alle lidstaten. De lidstaten hebben in het voorstel op bepaalde punten nog vrijheid om aanvullende wetgeving uit te vaardigen, doch deze mogelijkheid is beperkt.

Hieronder volgt een overzicht van de belangrijkste punten.

B. Uitbreiding toepassingsgebied

Uitbreiding naar OTT: Het merendeel van de regels uit de huidige ePrivacyrichtlijn heeft alleen betrekking op telecomaanbieders, zoals bv. de regels betreffende de verwerking van gegevens die aanbieders verkrijgen in het kader van hun dienstverlening en betreffende de geheimhouding van deze gegevens. Online diensten voor elektronische communicatie vallen hier niet onder waardoor “over the top” (OTT) diensten zoals Skype, Facebook Messenger, Whatsapp, Gmail en dergelijke momenteel buiten het

toepassingsgebied blijven. De voorgestelde verordening heeft een ruimere werkingssfeer en is ook van toepassing op aanbieders van deze diensten.

Buiten de Europese Unie: Net zoals de AVG, krijgt de nieuwe verordening toepassing buiten het grondgebied van de Europese Unie. Iedere (ook niet-Europese) dienstverlener die elektronische dienstverlening aanbiedt aan eindgebruikers die zich in de Europese Unie bevinden zal deze regels moeten respecteren.

De term "eindgebruiker" wordt zeer ruim gedefinieerd en houdt geen rekening met het onderscheid particulier of professioneel.

Uitbreiding naar IOT: Bovendien heeft de verordening ook betrekking op communicatie tussen apparaten. Dat betekent dat ook het zogenaamde internet of things (IOT) binnen het toepassingsgebied van de verordening valt.

C. Spam en direct marketing

Het verbod om spam te sturen (ongewenste elektronische communicatie via e-mail, SMS of geautomatiseerde telefoonoproep) wordt uitgebreid onder de verordening. De toestemming van de betrokkene is vereist voor het versturen van commerciële communicatie, tenzij er al sprake is van een bestaande relatie met een klant. In dat geval moet een opt-out wel steeds mogelijk zijn.

De regels voor direct marketing wijzigen niet bijzonder. Direct marketing met behulp van elektronische communicatiemiddelen is enkel toegestaan indien de eindgebruikers hun toestemming hebben verleend. Dit betekent een voorafgaande opt-in.

Het is wel mogelijk om met bestaande klanten betreffende gelijkaardige producten of diensten te communiceren, vooropgesteld dat ze afdoende geïnformeerd geweest zijn.

Zich verzetten tegen het ontvangen van de communicatie moet steeds mogelijk zijn. Dit recht op verzet moet kosteloos en moeiteloos kunnen worden uitgeoefend. De klassieke uitschrijflink onderaan de email blijft behouden.