MEET & GREET
met de wellicht voor U nog onbekende
(dit artikel zal daar alles aan veranderen)
DATA PROTECTION OFFICER
VAN DE BALIE GENT

graag stellen wij U voor :

Mr. Jents DEBRUYNE

| door Vincent Rits en Lenny Van Tricht

Kunt U zich kort even voorstellen ?
Mijn naam is Jents Debruyne en ik ben sinds 2013 actief aan de balie van Kortrijk.

In de lente van 2017 heb ik mijn eigen kantoor opgericht, **www.advocaatdebruyne.be**, dat zich vooral toelegt op IT – recht, privacy en innovatie.

Naast adviesverlening, word ik geregeld aangesteld als Data Protection Officer (afgekort DPO), voornamelijk voor ondernemingen en sinds enige tijd ook voor de Balie Gent.

Wat doet een Data Protection Officer ?

De functie van Data Protection Officer is een voortvloeisel van de Algemene Verordening Gegevensbescherming (GDPR) die in België werd omgezet in de Wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen in verband met verwerking van persoonsgegevens.

Internetgebruikers leveren immers vaak 'gratis' hun persoonsgegevens in ruil voor een aantal diensten. Op basis van deze gegevens wordt een persoonlijk profiel aangemaakt waarop allerlei 'volgtechnieken' worden losgelaten. Op basis van deze profielen kunnen 'social media', 'zoekmachines', 'internetwinkels' of andere platformen advertenties aan u persoonlijk richten. Bedrijven en organisaties kopen deze advertentieruimtes.

Maar er is een keerzijde aan de medaille. Wie advertenties aankoopt kan een doelpubliek misleiden, enorm beïnvloeden of groepen mensen tegen elkaar opzetten. De volgtechnieken van deze platformen worden steeds radicaler. Daarnaast weten gebruikers vaak niet hoeveel informatie zij zelf hebben gedeeld, of hun informatie in goede handen is en waarvoor deze gegevens zullen worden gebruikt. De negatieve aspecten van een globale digitale omgeving zullen in de komende maanden en jaren steeds acuter op de voorgrond treden. De verordening is een eerste stap om onze regelgeving aan te passen aan de digitale omgeving.

De belangrijkste wijziging bestaat hierin dat elke organisatie die persoonsgegevens gaat verzamelen, inclusief de overheid, dient aan te tonen ten aanzien van de betrokkenen en de bevoegde gegevensbeschermingsautoriteit hoe de persoonsgegevens binnen de organisatie worden verwerkt en op welke legitieme en proportionele manier dit gebeurt, zowel in een digitale als fysieke omgeving. Van zodra een onderneming, eender waar ter wereld gevestigd, persoonsgegevens van betrokkenen binnen de Unie gaat verwerken, is deze verplicht te voldoen aan de principes van de GDPR.

Een Data Protection Officer of functionaris gegevensbescherming vormt het aanspreekpunt voor de Gegevensbeschermingsautoriteit, implementeert en houdt toezicht op de vele procedures die moeten gevolgd worden (zoals het stappenplan hieronder) en houdt de evoluties verder in het oog.

Er zijn 3 categorieën waarin het verplicht is om een Data Protection Officer aan te wijzen:

(1) wanneer de verwerking wordt verricht door een overheidsinstantie of overheidsorgaan, behalve bij gerechten in de uitoefening van hun rechterlijke taken;
(2) wanneer een verwerkingsverantwoordelijke hoofdzakelijk belast is met verwerkingen die regelmatige en stelselmatige observatie op grote schaal van betrokkenen vereisen;
(3) wanneer de verwerkingsverantwoordelijke hoofdzakelijk belast is met grootschalige verwerking van bijzondere categorieën van gegevens en strafrechtelijke veroordelingen en strafbare feiten.

Wat houdt de functie van Data Protection Officer specifiek in voor de balie en meer concreet voor de individuele advocaat ?

De Orde van Vlaamse Balies heeft behoorlijk wat richtlijnen en templates online geplaatst om elke advocaat zoveel als mogelijk GDPR-compliant te maken. Deze documenten zijn terug te vinden op het privaat luik op www.advocaat.be.

De GDPR geldt voor iedereen die persoonsgegevens bijhoudt en/of verwerkt, ongeachte de grootte van de onderneming.

Hoewel de GDPR bijkomende verplichtingen voor grote(re) ondernemingen voorziet, bent u als individueel advocaat gehouden tot diverse verplichtingen inzake het verzamelen, bijhouden en verwerken van (persoonlijke) informatie.

Als individuele advocaat komt u uit de aard van uw beroep in aanraking met (vaak gevoelige) informatie van uw cliënten. Het verzamelen en archiveren van dergelijke informatie betekent dat u als advocaat ook gebonden bent door de GDPR. Gezien Balie Gent op grote schaal gevoelige dossiers verwerkt, heeft Balie Gent een Data Protection Officer nodig.

Moet een Data Protection Officer aan bepaalde kwalificaties/kwaliteiten voldoen? Bestaat hiervoor een opleiding?

Voorlopig is de enige opleidingsvereiste voor een Data Protection Officer dat je voldoende kennis moet hebben van de GDPR- en privacywetgeving. Er zijn commerciële opleidingen, maar een opleidingscertificaat dat erkend is door de Gegevensbeschermingsautoriteit bestaat voorlopig niet.
Een andere belangrijke voorwaarde is dat de Data Protection Officer onafhankelijk dient te zijn bij het uitvoeren van de taken. Een vennoot kan dus geen Data Protection Officer zijn binnen het eigen advocatenkantoor, maar ook de IT-manager mag de rol van Data Protection Officer niet opnemen.

Hoeveel tijd besteedt U aan Uw functie als Data Protection Officer ?
Ik ben hier dagelijks mee bezig.

Ik werk voornamelijk voor HR – en IT bedrijven, de bank - en verzekeringssector en sinds enige tijd ook voor de balie Gent die mij heeft aangeworven als Data Protection Officer.

Mijn hoofdbezigheid bestaat uit het verstrekken van advies in het kader van de GDPR en het zorgen voor een juridische omkadering van nieuwe software-projecten (Privacy by design) .

Ik verwacht dat in de nabije toekomst dergelijke adviesverlening heel sterk zal toenemen omdat er meer conflicten zullen zijn m.b.t. digitale dossiers en rond eigendom van data. We staan op een punt waarop alles snel zal veranderen want de digitalisering is volop aan de gang.

Op welke manier kan men als advocaat best de GDPR implementeren ?
Ik raad het volgende pragmatische stappenplan aan:

1. Het opstellen van een extern privacybeleid dat op de website wordt geplaatst (privacypolicy) en het aanpassen van de algemene voorwaarden;
2. Een verwerkingsregister opstellen als kapstok voor de verwerking van persoonsgegevens binnen uw kantoor. Dit is een uitstekende oefening om na te gaan welke gegevens u verwerkt, wat ermee gebeurt en hoe u deze gaat beschermen;
3. Nagaan (samen met je websitebeheerder) welke cookies je website gebruikt en je cookiepolicy hier conform de wetgeving aan aanpassen. Je aanwezigheid op sociale media GDPR-conform maken;
4. Het opstellen van een intern beleid; van zodra een cliënt binnenstapt in het kantoor bepalen wat zal er gebeuren met het dossier, digitaal en/of fysiek;
5. Nagaan of uw externe partners (vb. boekhouder, sociaal secretariaat, IT-leverancier) een gelijkaardig beschermingsniveau hebben op het vlak van gegevensbescherming. Sommige leveranciers nemen clausules op in hun algemene voorwaarden, maar het kan nodig zijn een verwerkersovereenkomst met hen te tekenen;
6. Ten aanzien van het personeel en medewerkers ervoor zorgen dat zij GDPR-conform werken, ook bij het beëindigen van de samenwerking. Anderzijds ook maatregelen nemen voor het verwerken van de persoonsgegevens en informatie van de (kandidaat) personeelsleden zelf;
7. Procedures opstellen ten aanzien van betrokkenen die hun rechten willen uitoefenen en die bijvoorbeeld inzage willen in het dossier. Deze vragen dienen in beginsel binnen één maand te worden beantwoord maar de rechten zijn niet absoluut;
8. In een aantal gevallen het opstellen van een privacy impact assessment (bij hoge risico's).
9. Een register inzake data-incidenten bijhouden binnen de organisatie. De procedure inzake data-incidenten nauwgezet opvolgen en meldingen doen aan de autoriteit en de betrokkenen wanneer dit nodig is conform de wetgeving;
10. Een Data Protection Officer aanduiden (indien dit verplicht is) die regelmatige evaluaties maakt van de te doorlopen procedures en kijkt of alle organisatorische en technische maatregelen voldoende worden geïmplementeerd.

Uiteraard is ieder kantoor verschillend en kan een specifieke aanpak nodig zijn.

Zijn er straffen als men niet voldoet aan de GDPR en zijn er reeds voorbeelden gekend in de praktijk ?
Er zijn twee categorieën van administratieve sancties:

- De eerste categorie zijn in beginsel de sancties voor inbreuken op de verplichtingen van de verwerkingsverantwoordelijke en de verwerker: Deze administratieve boetes lopen op tot 10 000 000 Euro of, ingeval van een onderneming, tot 2% van de totale wereldwijde jaaromzet in het voorgaande boekjaar.
- De tweede categorie betreffen in beginsel de sancties voor inbreuken op de algemene beginselen inzake gegevensbescherming alsook voor inbreuken op de rechten en vrijheden van de betrokkenen: deze administratieve boetes lopen op tot 20 000 000 Euro of, ingeval van een onderneming, tot 4% van de totale wereldwijde jaaromzet in het voorgaande boekjaar.

Daarnaast kan de Gegevensbeschermingsautoriteit verschillende handelingen stellen om inspecties en onderzoeken uit te voeren. De Belgische Privacywet heeft daarnaast ook strafrechtelijke sancties bijkomend opgenomen.

De juridische website JUBEL werd recent door de Gegevensbeschermingsautoriteit veroordeeld tot een boete van 15.000 euro. In de beslissing werd uiteengezet dat het cookiebeleid niet voldeed aan de vereisten van de e-privacyrichtlijn en GDPR.

Een cookie is een tekstbestandje dat door de server van een website in de browser van uw computer of op uw mobiel apparaat wordt geplaatst wanneer u de website raadpleegt. Die bestanden kunnen in het beheer zijn van de website-eigenaar zelf ('Eerste Partij cookies' genoemd) of ze kunnen beheerd worden door een derde partij zoals bijvoorbeeld Facebook, Google,… ('Derde Partij cookies' genoemd).

Derde Partij cookies moeten in beginsel altijd onderworpen worden aan de toestemming van de persoon die een website bezoekt.

Voor Eerste Partij cookies is een toestemming niet altijd vereist. Dit hangt af van het type cookies.

Er zijn verschillende soorten cookies o.a. :

- noodzakelijke cookies zijn cookies die ervoor zorgen dat alle onderdelen van een website goed werken;
- analytische cookies gaan na hoeveel bezoekers je hebt en wat ze bekijken;
- tracking cookies verzamelen in beginsel zoveel mogelijk informatie over internetgebruikers;

De mogelijkheid moet altijd voorzien worden om een website te kunnen bezoeken/gebruiken zonder daarbij te botsen op analytische – en trackingcookies. Enkel de noodzakelijke of 'minimale' cookies mogen zonder een vrijblijvende toestemming worden gebruikt.

In onze buurlanden zijn voor inbreuken op de GDPR enorme boetes uitgesproken die oplopen tot vele miljoenen euro's. De Belgische Gegevensbeschermingsautoriteit heeft zich de voorbije twee jaar vooral gericht op preventie en informeren van alle organisaties. Zelf ben ik ook voorstander van deze aanpak. Zeker het preventieve luik aangaande beveiliging van ondernemingen zal in de komende jaren Belgische ondernemingen meer moeten beschermen tegen cybercriminaliteit. Ik verwacht wel dat er dit jaar enkele hogere boetes zullen worden opgelegd. Daarnaast mogen sommige dubieuze praktijken van grote IT-wereldspelers goed worden bestudeerd. Er zijn immers geavanceerde technieken die ervoor zorgen dat zij alle data stevig in handen kunnen houden. Het is een uiterst boeiende materie in een innoverende wereld.

Strop & Toga dankt u van ganser harte voor dit verhelderende interview en wenst U alle succes toe in het digitale tijdperk !!