'LE GDPR, UNE QUESTION DE BON SENS PAYSAN'

Comme bien d'autres organisations, l'asbl Rotary BeLux Services s'est activement préparée à l'entrée en vigueur, ce 25 mai, du GDPR (Règlement Général sur la Protection des Données). Pour ce faire, nous avons été épaulés par LesJuristes, un cabinet d'avocats spécialisé en droit informatique, propriété intellectuelle et droit des entreprises. On fait le point avec Jan-Willem Lust, responsable Europe et expert dans le domaine de la vie privée. 'J'ai été impressionné de voir à quel point RBS se sentait concerné par la question. Cette prise de conscience a beaucoup facilité les choses.'

Jan-Willem Lust

En quoi consiste le GDPR, et pourquoi le mettre en œuvre ?

Il concerne la gestion et la sécurisation des données privées des citoyens européens. Toute organisation doit pouvoir démontrer quel type de renseignements personnels elle collecte, comment elle utilise ces éléments et comment elle les protège. Notre pays disposait déjà, depuis 1992, d'une loi en la matière mais le GDPR entend mettre en place un règlement européen uniforme. Il est vrai que les sensibilités pouvaient fortement varier d'un pays à l'autre… À partir du 25 mai, ce seront les mêmes règles pour tout le monde. Il s'agit bien d'un règlement et non d'une directive. La loi entre donc en vigueur immédiatement, et elle fixe de manière explicite la responsabilité des organisations qui traitent ce type de données : elles sont tenues de réaliser des screenings et de prendre des mesures en la matière. Elles peuvent bien sûr continuer à traiter des informations privées, mais elles doivent désormais prendre des mesures appropriées pour les protéger efficacement. En outre, les personnes concernées disposent à tout moment d'un droit de regard et même d'un droit à l'oubli (effacement des données).

Quelles mesures concrètes doivent être prises ?

La première étape consiste à créer un registre de données (électronique *et* papier), dont un modèle type est disponible sur le site web de la Commission de la protection de la vie privée. Ce registre reprendra un récapitulatif des actions de l'entreprise dans le domaine du traitement des données : de quels renseignements disposons-nous, de qui et pourquoi ? Il est très important de mentionner cette justification, qui peut être très simple : par exemple, une entreprise classique a besoin des données privées de son personnel dans le cadre de l'exécution du contrat de travail. Si des tiers sont impliqués dans le traitement des données, ils doivent également être répertoriés.

La deuxième partie concerne la protection de ces mêmes données, tant sur le plan de l'organisation que sur le plan technique, afin d'éviter toute utilisation abusive. Ceci suppose une politique interne de gestion des données ainsi que des mesures concrètes telles que l'adoption de mots de passe et de pare-feux efficaces, l'authentification multifactorielle pour les fichiers sensibles, et éventuellement le cryptage. Naturellement, ces mesures doivent rester proportionnées et financièrement acceptables. Par exemple, un boulanger qui stocke des infos liées aux cartes de fidélité de ses clients n'a pas besoin d'une authentification multifactorielle. En substance, il s'agit de faire preuve de 'bon sens paysan' : faites ce qui vous semble nécessaire sur base de la politique de votre organisation en matière de *privacy*.

Quelle est votre offre de services dans ce domaine, et quelles sont les questions qui reviennent le plus souvent ?

Nous proposons un accompagnement de A à Z, en commençant par un audit sur la confidentialité, suivi d'un plan d'action visant à la conformité maximale avec le GDPR : mise en place d'une politique de confidentialité, rédaction de contrats, instauration d'une politique en matière de mot de passe… Mieux encore, en tant que bureau spécialisé en droit des TIC, LesJuristes peut être votre DPO, votre 'Data Protection Officer'. Car il n'est pas forcément intéressant de nommer quelqu'un en interne à ce poste (risque de surcharge de travail ou de recrutement inutile).

Au départ, de nombreuses organisations pensaient que le GDPR ne les concernait pas : 'Nous ne sommes qu'une petite asbl, nous ne faisons pas de marketing…', pouvait-on entendre. Soyons clairs : le GDPR s'applique à tout qui gère des données privées ! Autre question fréquemment posée : 'Pourrons-nous encore contacter des gens après le 25 mai ?' Bien sûr, mais de manière documentée et justifiée. Toute personne qui collecte des données par voie électronique doit désormais demander le consentement préalable, clair et explicite (système 'opt in' : case à cocher), des personnes concernées pour les utiliser.

À mesure que la date limite approche, les questions deviennent plus complexes. Il y a même des personnes qui commencent à paniquer, car une 'machine marketing' s'est mise en branle, faisant planer le risque d'énormes amendes, dès le 25 mai, en cas de non-respect de la législation. Je vous le dis clairement : *personne* ne sera prêt à cette date, pas même la Commission de la protection de la vie privée, qui l'a elle-même admis en long et en large. Donc, ne vous inquiétez pas si vous n'êtes toujours pas en règle. Faites juste en sorte de pouvoir prouver que vous vous activez à le devenir.

Vous avez effectué un *privacy compliance scan* pour RBS. Qu'est-ce que cette analyse a donné ?

Le Rotary s'en est très bien sorti ! Parmi toutes les organisations *screenées*, vous êtes l'une de celles qui obtiennent les meilleurs résultats. Nous avons remarqué une véritable prise de conscience sur le sujet, sans doute parce que vous avez été touchés dans le passé par certaines questions liées à la vie privée. L'expérience, c'est encore le meilleur enseignement…

Plusieurs nouvelles obligations du GDPR étaient déjà respectées dans les faits. Là aussi, c'est une question de bon sens : on a eu un souci, comment éviter qu'il se reproduise à l'avenir ? Il reste quelques points à régler, comme par exemple le droit des personnes concernées par la circulation des données. Avec sa structure organisationnelle à la fois locale, nationale et internationale, le Rotary est un cas à part, et il y a donc encore un peu de peaufinage à effectuer.

Selon moi, la publication de votre annuaire n'est aucunement compromise. En principe, chacun peut s'opposer à ce que son nom y soit mentionné. En pratique, cela me semblerait plutôt illogique puisque, en rejoignant le Rotary, on choisit de faire partie d'un réseau. Tant que l'information reste en interne, aucun problème ne se pose. Une autre question est de savoir si les partenaires doivent continuer à être mentionnés, car à eux on n'a rien demandé…

Dans le cas du Rotary, la nomination d'un DPO interne ne me semble pas nécessaire. En effet, le traitement des données ne constitue pas votre tâche principale, et celles dont vous disposez sont confidentielles mais pas 'sensibles'. Il serait bon, toutefois, que quelqu'un soit chargé des questions de confidentialité, une sorte de 'chef de projet GDPR'. Je déconseille la dénomination 'DPO' ou 'responsable protection des données' car il tomberait alors sous le coup du cadre juridique correspondant.

L'objectif du GDPR est de prévenir les violations de données. Que faire si cela se produit tout de même ?

La 'fuite de données' est un concept plutôt vaste : il s'agit en principe d'un accès non autorisé à des informations personnelles. La forme la plus connue est évidemment le piratage. Ceci dit, la perte d'un téléphone portable ou l'envoi par erreur d'un e-mail comprenant une database peuvent eux aussi mener à une fuite. Il faut alors notifier celle-ci – endéans les 72 heures après le constat – auprès de la Commission de la vie privée, par le biais d'un formulaire en ligne. Dans le cas d'un piratage, plusieurs mois peuvent s'écouler avant que le préjudice ne soit constaté. Même si vous n'avez aucune idée de l'ampleur du dommage, il convient de le signaler à la Commission dans un premier temps, et de fournir ensuite tous les détails dont vous disposez. Ainsi, vous remplissez toutes vos obligations. Vous devez également prévenir et informer les personnes touchées par la fuite. Au-delà de ces impératifs, nous préconisons également de tenir un 'journal de bord' sur les évènements. Pratique en cas de contrôle, cela peut en outre permettre de révéler certains problèmes structurels.

Pour finir : avez-vous été surpris par le récent scandale Facebook ?

Honnêtement, pas du tout, on le voyait venir depuis un bon moment… Il y a eu, en effet, un certain nombre de précédents qui ont toutefois échappé à l'attention générale. L'utilisateur ne se rend pas assez compte que Facebook fonctionne grâce à la collecte d'informations privées, tout comme Google et même Amazon. Si un service est 'libre et gratuit', c'est parce que, en fin de compte, le produit, c'est vous ! Vos données personnelles sont par exemple utilisées pour la publicité ciblée. Le plus embarrassant, c'est que Facebook savait ce qui se passait mais n'a pas réagi…

STEVEN VERMEYLEN / DENIS CREPIN

'GDPR DRAAIT OM GEZOND BOERENVERSTAND'

Net als tal van andere organisaties heeft Rotary BeLux Services zich de voorbije maanden intensief voorbereid op de inwerkingtreding van de GDPR (General Data Protection Regulation of Algemene Verordening Gegevensbescherming – AVG), op 25 mei. We werden daarbij begeleid door deJuristen, een juridisch kantoor gespecialiseerd in ICT-recht, intellectuele eigendom en ondernemingsrecht. We maken een balans op met Jan-Willem Lust, European Head of Legal en expert op het domein van privacy. 'Ik was onder de indruk van de *awareness* die rond dit onderwerp leeft bij RBS. Dat heeft de aanpak flink vooruitgeholpen.'

© Shutterstock

Even kaderen: wat houdt de GDPR precies in en waarom wordt die ingevoerd?

GDPR gaat over het beheer en de beveiliging van persoonlijke gegevens van Europese burgers. Als organisatie moet je kunnen aantonen welke persoonsgegevens je verzamelt, hoe je deze data gebruikt en hoe je ze beveiligt. Voor alle duidelijkheid: in ons land bestond er al een privacywetgeving sinds 1992, die bovendien relatief goed in mekaar stak. Maar nu komen we tot een uniform Europees systeem. Tot nu toe zat er veel verschil op de verschillende nationale privacywetten: in Ierland waren die minimaal, in Nederland dan weer erg goed uitgekiend. Vanaf 25 mei gelden voor iedereen dezelfde spelregels. Het gaat om een verordening, niet om een richtlijn. De wetgeving is dus meteen van kracht. Het komt erop neer dat de verantwoordelijkheid voortaan expliciet bij de gegevensverwerkende organisaties zelf wordt gelegd; zij worden verplicht om hun databeleid te screenen en actie te ondernemen. Je mag dus gerust nog data verwerken maar je moet een aantal adequate technische en organisatorische maatregelen nemen om die te beschermen. Bovendien hebben de betrokkenen op elk moment recht op inzage en eventueel schrapping.

Welke concrete maatregelen zijn er dan nodig?

De eerste stap is het aanleggen van een dataregister. Daarvoor vind je een template op de website van de Privacycommissie. Dat register bewaar je best elektronisch én op papier. Het bevat een opsomming van wat er binnen de organisatie gebeurt op het vlak van gegevensverwerking: welke data hebben we van wie en waarom. Het is van groot belang die rechtvaardigingsgrond te vermelden. Dat kan heel eenvoudig zijn: een klassiek bedrijf heeft bijvoorbeeld de persoonsgege-

vens van zijn personeel nodig in het kader van de uitvoering van de arbeidsovereenkomst. Indien er derde partijen betrokken zijn, moeten ook zij vermeld worden als gegevensverwerker.

Het tweede luik is de bescherming van die gegevens, zowel organisatorisch als technisch, om oneigenlijk gebruik te vermijden. Dat houdt bijvoorbeeld een intern beleid m.b.t. gegevensbeheer in, naast een wachtwoordbeleid en een aantal technische ingrepen als een goede firewall, multifactor-authenticatie voor gevoelige bestanden, eventueel encryptie van bepaalde data. Uiteraard moeten deze maatregelen proportioneel en financieel haalbaar blijven. Een bakker die gegevens bewaart die verbonden zijn aan een klantenkaart, gaat geen multifactor-authenticatie nodig hebben. In essentie gaat het om gezond boerenverstand: ga na hoe jouw organisatie omgaat met persoonsgegevens en doe wat jou noodzakelijk lijkt.'

Welke diensten bieden deJuristen op dit vlak en welke vragen krijgen jullie het meest?

Qua GDPR kunnen wij instaan voor een A tot Z-begeleiding, die start met een privacy-audit, fysiek of met behulp van een speciaal softwarepakket. Dan stellen we een actieplan op om zo goed mogelijk *GDPR-compliant* te zijn. Bij de implementatie daarvan kunnen we helpen bij het uitschrijven van een concrete privacy-policy, het opstellen van contracten, het instellen van een wachtwoordbeleid… Meer nog: als kantoor gespecialiseerd in ICT-recht bieden wij een totaalpakket DPO-services. Met andere woorden: wij fungeren dan als Data Protection Officer voor uw organisatie. Het is niet altijd interessant om zo iemand intern aan te stellen; dat kan aanleiding geven tot een bijkomende belasting van het bestaande personeel of een overbodige aanwerving.

Aanvankelijk dachten veel organisaties dat de GDPR voor hen niet van toepassing zou zijn. 'Wij zijn maar een kleine vzw, wij doen niet aan marketing.', hoorden we dan. Laat het duidelijk zijn: de GDPR geldt voor iédereen die persoonsgegevens beheert! Een andere veel gestelde vraag: 'Mogen wij nog mensen contacteren na 25 mei?' Uiteraard, maar op een gedocumenteerde en gerechtvaardigde manier. Wie elektronisch gegevens verzamelt, bijvoorbeeld via een website, moet voortaan wel de actieve toestemming van de betrokkenen vragen om deze te gebruiken. Zij geven dan vrijelijk, specifiek en ondubbelzinnig hun akkoord, via een opt-in systeem.

Nu de deadline nadert, worden de vragen wat complexer. Hier en daar slaan mensen zelfs aan het panikeren. Er is dan ook een marketingmachine op gang gekomen die ons om de oren slaat met 'waarschuwingen' voor monsterboetes als we niet in orde zijn tegen 25 mei. Ik zeg u: er zal niémand klaar zijn tegen die datum. Zelfs de Privacycommissie niet, dat heeft ze met zoveel woorden al toegegeven. Lig er dus niet van wakker als je nog niet in orde bent. Zorg wel dat je kan aantonen dat je ermee bezig bent. Denk erover na en zet de eerste stappen.

Jullie voerden een *privacy compliance scan* uit voor RBS. Wat heeft die opgeleverd?

Ik moet zeggen dat Rotary hier behoorlijk goed is uitgekomen. Van alle gescreende organisaties kunnen jullie zeker één van de betere resultaten voorleggen. We hebben gemerkt dar er een groot bewustzijn heerst over dit onderwerp, allicht mede omwille van een aantal privacy-gerelateerde kwesties in het verleden. Ervaring is nu eenmaal de beste leerschool.

Een aantal nieuwe verplichtingen binnen GDPR werden eigenlijk al gerespecteerd. Ook daar is sprake van gezond boerenverstand: er is iets verkeerd gelopen, hoe kunnen we dat in de toekomst vermijden? Wat nog verder te bekijken valt, zijn bijvoorbeeld de rechten van de betrokkenen i.v.m. gegevensdoorstroming. Rotary bevindt zich in een aparte situatie door haar organisatiestructuur, met een lokaal, nationaal en internationaal niveau. Dat moeten we verder *finetunen*. Ook de bestaande documentatie hieromtrent moet verder uitgewerkt worden.

De publicatie van jullie jaarboek komt volgens mij niet in het gedrang. In principe mag iedereen die daarin vermeld staat, zich daartegen verzetten. Binnen de Rotarycontext lijkt mij dat evenwel contraproductief: je wordt bewust lid van het Rotarynetwerk… Zolang de info intern blijft, stelt er zich geen probleem. Een andere vraag is of de partners in de toekomst vermeld moeten blijven, want hén is niets gevraagd…

De aanstelling van een interne Data Protection Officer lijkt ons in het geval van Rotary niet noodzakelijk. Gegevensverwerking is niet jullie hoofdopdracht en de data waarover jullie beschikken zijn weliswaar vertrouwelijk, maar niet 'gevoelig'. Het is goed dat binnen de organisatie iemand is aangeduid die zich met privacykwesties bezighoudt, een soort 'projectleider GDPR'. Ons advies is trouwens zo iemand geen 'DPO' of 'verantwoordelijke gegevensbescherming' te noemen, want dan valt hij volledig onder het overeenkomstige wettelijk kader, met alle gevolgen vandien.

De hele GDPR is gericht op het vermijden van datalekken. Wat als er toch zo'n lek optreedt?

Een 'datalek' is een breed begrip: in principe gaat het om elke ongeautoriseerde toegang tot persoonsgegevens. De meest bekende vorm is natuurlijk *hacking*. Maar ook het – al dan niet vrijwillig – verlies van een mobiel toestel of een verkeerd verstuurde e-mail met een databestand, kunnen aanleiding geven tot een datalek.

Indien je zo'n lek vaststelt, doe je binnen de 72 uur na de ontdekking ervan een melding bij de Privacycommissie, via een online formulier. De termijn treedt in werking na de vaststelling; bij een hacking kan het immers maanden duren voor je op de hoogte bent. Ook als je niet weet wat er allemaal gelekt is: toch even melden en laten weten dat je erop terugkomt. Zo heb je voldaan aan je initiële meldingsplicht. Ook de betrokkenen zelf dienen geïnformeerd te worden.

Onze tip is om nog een stap verder te gaan: voldoe niet alleen aan de meldingsplicht, hou zelf ook een soort logboek bij van wat er gebeurd is. Dat is handig bij een eventuele controle, maar kan ook structurele problemen aan de oppervlakte doen komen. Zo komt er idealiter een wisselwerking tot stand tussen je logboek en je databeleid.

Tot slot: was u verrast door het recente privacyschandaal bij Facebook?

Eerlijk? Helemaal niet. Het zat er al lang aan te komen. Er zijn trouwens een aantal precedenten, die echter onder de radar zijn gebleven. De gewone gebruiker beseft te weinig dat het bij Facebook draait om gegevensverzameling, net als bij Google en zelfs bij Amazon. Een 'gratis' service betekent uiteindelijk dat je zelf het product bent! Jouw gegevens worden gebruikt om bijvoorbeeld gericht te adverteren. Het pijnlijke is dat Facebook wist wat er aan de gang was en er niets aan heeft gedaan…

STEVEN VERMEYLEN

E-club Belgium 1

Zoom-conference on GDPR
15 May 2018, 9 PM

Karen Vermaere (Rc Beveren-Waas), partner of the law firm Laurius, will speak about the European General Data Protection Regulation. She will in particular discuss how local Rotary Clubs can comply with this new regulation.

Technical details:
To join from PC, Mac, Linux, iOS or Android: install the software on https://zoom.us/j/734603333
To join using your iPhone (in one-tap):
Belgium: +3225884188,,734603333#
To join using another telephone:
Dial +32 (0)2 588 4188
Meeting ID: 734 603 333
International numbers available: https://zoom.us/u/dVC91428C

Powered by www.laurius.be LAURIUS