15 tips voor een beter beheer van uw gegevens

Gilles Quoistiaux, Trends-Tendances

De GDPR (General Data Protection Rule) is ingevoerd en dat gaat gepaard met de nodige vragen en angsten bij kleine en heel kleine ondernemingen. Hieronder 15 concrete tips en oplossingen om de zaken met de nodige gemoedsrust aan te pakken.

1. Wat met foto's die tijdens een event genomen zijn?

Uw bedrijf bestaat 10 jaar en daarvoor organiseert u een kleine drink met uw klanten. Kunt u de foto's die bij de gelegenheid genomen zijn, op de website of de Facebook-pagina van uw bedrijf plaatsen? "Vanaf het moment waarop foto's openbaar gemaakt worden, moet u de toestemming van de gefotografeerde personen hebben, " stelt Pascal Lambert, jurist bij de UCM (Union des Classes Moyennes). Een mogelijke oplossing om te vermijden dat elke deelnemer aan de drink een document moet ondertekenen, bestaat erin de fotograaf vooraf te briefen zodat die de gefotografeerde mensen duidelijk uitlegt welk gebruik er van de foto's gemaakt zal worden. Daardoor zijn deelnemers die niet in het online album willen verschijnen (gewoonlijk is hun aantal beperkt), gemakkelijk te identificeren.

2. Moet u uw gegevensbanken uitzuiveren?

Wanneer u klanten, potentiële klanten of alle andere mensen die in uw gegevensbanken voorkomen, aanspreekt, is er één essentiële vraag die u moet stellen: hebben ze zich akkoord verklaard om op die manier aangesproken te worden? Sommige bedrijven zijn van mening dat die toestemming, die vaak verscheidene jaren geleden geregistreerd werd, niet op de juiste manier verkregen werd of, nog eenvoudiger, dat ze moeilijk te bewijzen is (een geschreven toestemming ontbreekt). Dat is de reden waarom we allemaal tal van mails krijgen met de vraag of we in een bepaalde lijst opgenomen willen blijven of dat we daaruit geschrapt willen worden. Het probleem daarbij is dat de gegevensbanken van bedrijven een werkinstrument zijn die soms van onschatbare waarde zijn. Dat is het geval van een rekruteringsbedrijf (dat anoniem wil blijven) waar 15 mensen werken en dat in de loop der jaren 30.000 cv's in zijn gegevensbank verzameld heeft. "Als we een mass mailing doen, kunnen we hoe dan ook een laag responscijfer verwachten, ongeveer 7 %, " stelt de data protection officer van het bedrijf. Maar we kunnen geen 93 % van de kandidaten in onze gegevensbank schrappen. Dat zou economische zelfmoord zijn!" De oplossing van de KMO in kwestie bestaat erin om nieuwe kandidaten een toestemming te laten ondertekenen, en de bestaande gegevensbank te behouden.

Bij Lexgo, een online platform dat werkaanbiedingen in de juridische sector bundelt, is men van mening dat de goedkeuring van de 7.000 lezers van de nieuwsbrief voor '95%' in orde is. Het bedrijf is niet van plan om opnieuw het akkoord van de lezers te vragen. Maar het gaat wel zijn gegevensbank uitzuiveren door foutieve adressen te wissen en door de procedure om een abonnement stop te zetten, te automatiseren. "Omdat we in de juridische sector actief zijn, publiceren we ook een tekst om onze

politiek op het vlak van gegevens uit te leggen, " reageert Hugo De Maertelaere, partner bij Lexgo. "Maar we moeten wel aan de slag kunnen blijven en daarvoor hebben we een minimum aan gegevens nodig: naam, voornamen en mailadressen. We zullen ons aan de GDPR aanpassen, maar we gaan ook geen weken aan dat onderwerp besteden. Er is geen reden om te panikeren."
Een laatste advies: als u een e-mailingcampagne opzet om toestemming te vragen, is het wellicht interessant om een iets subtielere aanpak te volgen dan gewoon een ja/nee-vraag. U kunt de consumenten een aantal keuzes voorstellen zodat ze de communicatie die u hun opstuurt, kunnen verfijnen. U kunt hun voorstellen om de frequentie ervan in te stellen (een keer per maand, een keer week, enz.), of het type van e-mail aan te geven dat ze bereid zijn te ontvangen (nieuwsbrieven, promoties, aanbiedingen van partners, enz.). "Dat is een positievere benadering die vaak in een groter aantal reacties uitmondt, " aldus Damien Jacob (Retis).

3. Wenskaarten: een bedreigde traditie?
Wenskaarten blijven een sympathieke manier om klanten en/of potentiële klanten weer even aan u te doen denken. Maar hebben we vanaf nu hun toestemming nodig om hun bij de jaarwisseling een stukje karton op te sturen? In de meeste gevallen zal dat niet nodig zijn. "Als u een klein persoonlijk woordje schrijft, wordt dat als een gewone briefwisseling beschouwd. Dat spreekt vanzelf, " stelt consultant Damien Jacob (Retis). "Als u daarentegen zulke wenskaarten als een drager voor een promotiecampagne gebruikt, is de toestemming vereist. Maar dan zijn we ver verwijderd van wat Kerstmis betekent …"

4. Het adresboek van uw bedrijvenclub: een goudmijn die geëxploiteerd mag worden?
Leden van een club, een kring of een handelskamer hebben vaak toegang tot het adresboek van de vereniging in kwestie. Een interessante bron om contact te leggen met potentiële klanten. Maar mag men die wel gebruiken? Als occasioneel contact opgenomen wordt met een lid, is er geen probleem: daarvoor dient dat adresboek. Maar de ledenlijst en hun adressen in de gegevensbank van uw bedrijf integreren, kan niet zonder de toestemming van de betrokkenen. Anderzijds mag uw zakenkring evenmin uw gegevens aan een derde doorgeven zonder uw toestemming. "Zelke gegevens mag men niet op een ondoordachte manier doorgeven, " merkt Stéphanie De Ridder op, advocate bij Reliance. "Het gebeurt soms dat bedrijven hun klantengegevens verkopen of die voor sponsoring ruilen. Zonder toestemming is dat niet toegelaten."

5. Klantenkaarten: moet die manier van werken aangepast worden?
Dertiende boeket gratis. 20 % korting op de zesde knipbeurt. Dessert aangeboden na 10 aankopen. Heel wat handelaars bieden hun klanten een getrouwheidskaart aan. Maar kunnen ze daarbij ook vrij persoonlijke gegevens verzamelen? Ja, natuurlijk. Maar de klant moet wel correct geïnformeerd worden over het gebruik dat van die gegevens gemaakt wordt. Bijvoorbeeld dat een e-mailadres gebruikt wordt om een nieuwsbrief naar toe te sturen. Of dat de geboortedag dient om een verjaardagspromotie voor te stellen. Heel vaak volstaan enkele inlichtingen. "Sommige handelaars verzamelen onnodig te veel gegevens en kunnen dat niet rechtvaardigen. Waarom zou een bloemenverkoper mijn gsm-nummer nodig hebben, " geeft Jacques Folon (Edge Consulting) als voorbeeld. Wanneer u de gegevens die u verzamelt, tot een strikt minimum beperkt en wanneer u daarover open bent naar uw klanten toe, bent u perfect in orde.

6. Zijn uw onderaannemers betrouwbaar?
De persoonlijke gegevens die uw bedrijf verwerkt, worden soms door onderaannemers gemanipuleerd. Uw elektronische berichtendienst, uw online voorraadbeheerder of uw communicatiebureau hebben toegang tot bepaalde gegevens. Het nieuwe voorschrift bepaalt dat u verantwoordelijk bent voor het gebruik dat die onderaannemers van die gegevens maken. U moet u in feite garant stellen voor die commerciële partners. Moet u daarom contact opnemen met al uw onderaannemers om te controleren of ze zich op hun beurt aan de GDPR houden? "Neen, je moet keuzes maken. Je moet de grote risico's dekken en de overheden kunnen aantonen dat je de meest essentiële initiatieven genomen hebt, " stelt Adrien van den Branden, advocaat bij CMS. De grote spelers zijn perfect op de hoogte van de invoering van de GDPR en zetten gewoonlijk zelf stappen naar hun klanten toe om te tonen dat ze in orde zijn. Dat spaart u een groot deel van de verificatie uit.

7. Mag je je dossiers in kartonnen dozen bewaren?
De GDPR slaat niet alleen op elektronische bestanden. De bedrijven moeten ook maatregelen nemen om de gegevens op papier waarover ze beschikken, te beschermen. Sommige zogenaamde 'gevoelige' gegevens vereisen een bijzondere aandacht. Dat is bijvoorbeeld het geval met bepaalde personeelsdossiers waarin gewag gemaakt kan worden van de medische geschiedenis van de medewerkers. Dat soort van documenten mag niet ergens in een gang rondslingeren of zomaar in kartonnen dozen bewaard worden. "De GDPR bepaalt dat 'technische en operationele' maatregelen genomen moeten

worden om die gegevens te beveiligen. Dat kan gewoon betekenen dat ze in een afgesloten kast opgeborgen moeten worden, " verduidelijkt Jacques Folon, specialist GDPR bij Edge Consulting. En ook hier slaat die vorm van voorzorg, die uiteindelijk voor de hand ligt, alleen op de meest kritieke gegevens.

8. Wat doe je met de naamkaartjes die je tijdens een conferentie in handen krijgt?

Het uitwisselen van naamkaartjes tijdens professionele evenementen is een geliefkoosd tijdverdrijf. Maar is dat niet te vergelijken met het verzamelen van persoonlijke gegevens? Neen, helemaal niet. U bent uiteraard vrij om weer contact op te nemen met de personen die u ontmoet hebt: daar zijn die evenementen trouwens voor in het leven geroepen. Als u de gegevens van het naamkaartje in uw bestand met klanten en/of potentiële klanten invoert met het oog op marketingdoeleinden, zult u echter via het vakje 'toestemming' moeten passeren.

9. USB-sticks: een praktijk die risico's inhoudt?

Om te vermijden dat je een pc moet vervoeren, kan een USB-stick of een kleine externe schijf van pas komen. Maar denk toch even na over de bestanden die u daarop zet. Als u thuis nog een PowerPoint-presentatie wilt bijschaven, is er geen probleem. Maar staan er persoonlijke of gevoelige gegevens op de drager, dan loopt u bij verlies daarvan een risico, zeker als de stick niet beveiligd is. "Een directeur van een webagentschap vertelde me ooit eens dat hij op zijn USB-stick de logins en wachtwoorden van zijn klanten bewaarde. Dat is uiteraard erg risicovol, " waarschuwt Damien Jacob. Sommige bedrijven die gevoelige gegevens verwerken, hebben beslist om het gebruik van USB-sticks te verbieden. Het is niet altijd nodig om zover te gaan: eenvoudige richtlijnen voor de personeelsleden over de gegevens die ze buiten het bedrijf mogen meenemen, kunnen volstaan.

10. Moeten de professionele Facebook-pagina's afgesloten worden?

Sommige professionele Facebook-pagina's worden gebruikt om over het leven van het bedrijf te communiceren: nieuwe aanwervingen, nieuwe projecten, professionele evenementen, conferenties, personeelsdagen, enz. Al die publicaties kunnen ertoe leiden dat persoonlijke gegevens gedeeld worden (naam, Facebook-profiel, foto, leeftijd, enz. van een werknemer). Het probleem is dat Facebook door de Europese overheid in het oog gehouden wordt wegens de slordigheid waarmee het bedrijf gegevens beheert. "Facebook biedt geen voldoende garanties voor de vertrouwelijkheid van de gegevens. Alle gegevens met betrekking tot het personeel, zouden dus alleen intern gepubliceerd moeten worden, bijvoorbeeld op het intranet van het bedrijf, " meent Olivier Rijckaert, advocaat arbeidsrecht en oprichter van Sotra. Niets belet echter om de Facebook-pagina als een bedrijfsetalage te behouden waar klanten en potentiële klanten alle nodige informatie over de producten en diensten van het bedrijf kunnen vinden.

11. Pseudoniemen voor iedereen?

Personen een 'pseudoniem' geven, is een techniek die in de GDPR vermeld wordt om de anonimiteit van bepaalde personen en dus de bescherming van hun persoonlijke gegevens te garanderen. Dat is wat Gail Bajraktari, consultant bij Dynafin, sommige van zijn klanten die in de financiële sector actief zijn, aanraadt. Makelaars of Belgische filialen van buitenlandse banken zijn immers in het bezit van zogenaamde 'gevoelige' gegevens die met de grootste omzichtigheid verwerkt moeten worden. Concreet bestaat de techniek van het pseudoniem erin om de gegevens te scheiden van de respectieve eigenaars opdat elke link naar de identiteit onmogelijk zou worden zonder een identificatiesleutel, " aldus Gail Bajraktari.

12. Alles archiveren... of alles door de papierversnipperaar jagen?

Archieven opstapelen, dat betekent dat je de kans loopt om zonder noodzaak persoonlijke gegevens te bewaren. Je hoeft echter niet paranoïde te zijn en systematisch elk document na gebruik te vernietigen. Alles hangt af van de gegevens in kwestie. Zo heeft een KMO die in de sector van de rekrutering actief is, onlangs een nieuwe papierversnipperaar besteld om geen documenten met persoonlijke gegevens te laten slingeren. Maar het bedrijf heeft nog vragen over wat het met de cv's waar gedurende jaren niets mee gebeurd is, moet doen. "We denken er nog over na, " vertelt de data protection officer van de KMO in kwestie. "Sommige profielen worden weinig gevraagd, maar jaren later kan er plots een vraag komen. Het zou dan jammer zijn dat we daar niet meer over zouden beschikken omdat we beslist hebben om ze bijvoorbeeld na vier jaar te vernietigen." Het kan dus gerechtvaardigd zijn om op een veilige manier bepaalde documenten gedurende jaren te bewaren. Andere documenten daarentegen zouden snel vernietigd moeten worden. Medische certificaten bijvoorbeeld die gevoelige informatie bevatten en die voor de werkgever helemaal niet van belang zijn om ze te bewaren.

13. Moeten de bruggen met callcenters buiten Europa opgeblazen worden?

De GPDR geldt voor alle persoonlijke gegevens van particulieren in Europa. Als u een beroep doet op buitenlandse contractanten, moet u er zich van verzekeren dat die in orde zijn met de richtlijn, ook al zijn ze niet in Europa gevestigd. En bepaalde dienstverleners hebben zich nog niet in orde gesteld. Moeten daarom de bruggen met bijvoorbeeld een callcenter in Afrika opgeblazen worden? "Grote bedrijven ontdoen zich op het ogenblik van hun banden met callcenters buiten Europa omdat ze van mening zijn dat die niet in orde zijn. Wij raden KMO's een overgangsregeling aan met structuren op het Europese continent, " adviseert Anne Mikusinski, opdrachthoudster bij de UCM op het vlak van de GDPR. Dezelfde vraag kun je stellen bij de opslag van gegevens. Hoe langer hoe meer bedrijven repatriëren hun gegevens op servers of in datacenters in

Europa. Een verplichting is dat echter niet.

14. Moet je de 'remarketing' opgeven?
Instrumenten zoals Facebook Pixel of de remarketingdienst van Google maken het mogelijk om internetgebruikers opnieuw aan te spreken over producten die ze voordien op een website voor e-commerce opgezocht hebben. Op dat moment verzamelen zowel Google als Facebook gegevens over de consumenten die de site van de handelaar bezoeken. Ideaal gesproken zou je de internetgebruiker dan moeten verwittigen dat zijn gegevens opnieuw voor marketingdoeleinden gebruikt kunnen worden. "Vaak weet de KMO niet precies wat Google als gegevens verzamelt. We raden het bedrijf aan om zich zo goed mogelijk te informeren wanneer het op zulke instrumenten een beroep doet, " stelt Anne Mikusinski (UCM). We durven er echter heel wat om verwedden dat Europa en de overheden die voor de gegevensbescherming bevoegd zijn, in de eerste plaats hun pijlen op de grote internetplatforms zullen richten, vooraleer de kleine handelaars aan te pakken die afhankelijk zijn van instrumenten die ze niet onder controle hebben.

15. Is het een goed idee om zijn eigen privacycharter te schrijven?
Zulk een charter omvat de regels die het bedrijf bij het beheer van de persoonlijke gegevens van zijn klanten hanteert. Vaak vind je het op de website van het bedrijf en even vaak is het door een advocaat opgesteld. Maar waarom zou u het niet zelf schrijven? Dat is alvast de raad van Damien Jacob, consultant bij Retis: "Het idee van de GDPR is precies dat zulk een document begrijpbaar moet zijn voor de particulieren die het lezen. Als u het in uw eigen woorden schrijft, vermijdt u jargon. Bovendien onderscheidt u zich op een positieve manier met uw communicatie." En niets belet u om uw tekst door een specialist te laten nalezen om zeker te zijn dat u niets vergeten bent. ■

E-business

Is uw website klaar voor de mobiele navigatie?

Aurelia Ricciardi

Het massale gebruik van smartphones en de efficiëntie van het 3G/4G-internet werken de online verkoop in de hand. Dat impliceert dat almaar hogere eisen aan de gebruikerservaring op het internet gesteld zullen worden. Na de 'responsive web design' worden de 'progressieve web apps' de norm voor een goed werkende e-commerce of zelfs m-commerce.

Enkele jaren geleden had men de mond vol van de 'responsive web design', een concept dat we als een aanpasbare website kunnen omschrijven. Het tijdschrift Mashable nomineerde het begrip zelfs als het 'woord van het jaar 2013': wat ook het schermtype was (pc, tablet, smartphone, enz.), de website moest zich automatisch aan de grootte van het scherm aanpassen om een optimale leesbaarheid te garanderen. Een 'responsieve' gebruikerservaring vergt dus dat de karaktertekens en lay-out zo min mogelijk aangepast worden, terwijl je de pagina's ook in alle richtingen moet kunnen doorlopen.
Vandaag echter staan de Progressive Web Apps (PWA's in het jargon) klaar om de norm op het vlak van de responsieve design te worden. De PWA's die in 2015 oorspronkelijk door Google ingevoerd werden, kunnen de kloof tussen browsers en de oorspronkelijke mobiele apps overbruggen waardoor ze zich als de nieuwe norm aandienen. Die hybride toepassingen – tussen webpagina's en eigen toepassingen in – combineren de nieuwste functies van de browsers met het beste van de gebruikerservaring op mobiele toestellen. De PWA's bieden eenzelfde gebruikservaring als de browser. Bovendien lijken ze op een app en werken ze als een app, maar hoef je niets te downloaden. Het volstaat om de site vanuit de mobiele browser op je scherm te registreren. En dat is een eerste voordeel: de App Store wordt overbodig en het geheugen van het toestel raakt niet overladen.