AVG Regelgeving, ook voor mij?

# Wat?

Op 27 april 2016 werd “Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG” goedgekeurd. Deze verordening, beter bekend onder de – iets kortere – naam Algemene Verordening Gegevensbescherming (afgekort als AVG) is onmiddellijk van toepassing in het Belgische recht en wil de bescherming van gegevens verhogen.

Wat houdt dit nu concreet in? Deze verordening, die door de Europese Unie werd uitgevaardigd, is rechtstreeks van toepassing. Dit betekent dat alle oudere Belgische wetgeving inzake privacy of gegevensbescherming die minder streng zou zijn of de verordening zou tegenspreken, niet meer geldt. Alle oude regels hierrond mogen dus naar de prullenbak, papierversnipperaar of kolenvuur, terwijl deze nieuwe verordening de **nieuwe Bijbel** inzakegegevens, privacy en persoonlijke levenssfeer wordt.

Deze nieuwe Bijbel verkondigt dus de bescherming van persoonsgegevens. De oude Belgische regels dateren van 1992, lang voor Google, Facebook, Twitter of Tinder zo bekend (of berucht) en wijdverspreid waren. Nu echter zijn de mensen zonder Facebookaccount een uitzondering, is Twitter hét communicatiekanaal bij uitstek van bepaalde politici en kan alles gevonden worden via Google (“als Google het niet vindt, bestaat het niet”). Die bekendheid en dat gebruik heeft echter een prijs. Google heeft YouTube gekocht, dus alle gegevens waarmee u een YouTube-account aanmaakt, zijn door Google verwerkt geweest. Facebook ziet alles wat u doet, wat u liket, waar u op reageert en wat u post. Vandaar dat u zeer gerichte reclame en “tv-spotjes” kan krijgen, omdat Facebook die gegevens verwerkt.

Die gigantische hoeveelheden data, ook wel **“big data”** genoemd, worden ook wel als **“de nieuwe olie”** gezien, omdat ze, net als aardolie en petroleum vroeger, economisch enorm belangrijk worden. Zoals met aardolie echter, werd enkel gekeken naar het economische voordeel, terwijl men nu pas bezorgd geraakt over de nadelen ervan. Vandaar dat de EU alle bedrijven binnen de EU eisen wil opleggen met betrekking tot hun gegevensverwerking.

# Waarom?

Een veel voorkomend argument is “Waarom iemand met privacy zou bezig zijn. Zolang je niets verkeerd doet, mag iedereen alles van je weten, want je hebt niets te vrezen.” Dat klopt helaas niet. Er zijn heel wat praktische problemen en gevaren aan het ongecontroleerd verzamelen en doorgeven van gegevens.

Stel, je koopt iets bij Bol.com, Zalando of aanverwanten. Je moet hiervoor van alles opgeven, zoals je naam, adres etc. Dit is vanzelfsprekend, aangezien Bol.com, Zalando of aanverwanten je bestelling aan je deur moeten komen leveren. Maar wat als zij je adresgegevens nu doorgeven aan willekeurige andere partijen? Je brievenbus kan de week na je bestelling propvol zitten met reclame van allerhande louche en minder louche bedrijven, alleen omdat ze je adresgegevens gekregen hebben.

Wat extra reclamepapier is dan wel onpraktisch, maar nog niet echt gevaarlijk. Dat klopt zeker, maar stel dat je jouw Visakaartgegevens moet doorgeven (om je aankoop te betalen)? Visa werkt gewoon via een kaartnummer en CVC-code, niet via online bankieren. Indien een van die bedrijven jouw Visagegevens zou doorgeven of verkopen aan derden (bedrijven, maar ook particulieren. Het is de droom van elke crimineel om te betalen met andermans budget), kan jouw bankrekening geplunderd zijn nog voor je “AVG” kunt zeggen.



Zo werkt het voor vele gegevens. Sommige data zijn ook niet zo banaal als een adres of telefoonnummer. Jouw medische gegevens, financiële gegevens of gerechtelijke gegevens (heb je een strafblad, was je een anonieme getuige, werk je als halve James Bond bij de undercoveroperaties van de Federale Politie of Staatsveiligheid) zijn heel wat belangrijker, gevoeliger en pijnlijker als die openbaar worden gemaakt. Vandaar dat een regeling rond gegevensbescherming dringend nodig was en is.

# Wanneer?

Hoewel die verordening op 27 april 2016 werd goedgekeurd, treedt ze pas in werking op **25 mei 2018**. Ondernemingen hadden dus meer dan 2 jaar om zich voor te bereiden op de sterkere gegevensbescherming.

Zoals te verwachten viel, is daar bij veel ondernemingen nog weinig mee gebeurd. Nu de deadline van 25 mei 2018 dichterbij komt, beginnen milde paniekaanvallen directies allerhande te teisteren. Vandaar dat nu overal druk gewerkt wordt om bedrijven, vzw’s en andere organisaties “**AVG-proof**” te maken, wat ook inhoudt dat gegevens beter en beter beschermd geraken.

# Voor wie?

Moet iedereen nu op zijn of haar hoede zijn voor gegevensbescherming? Indien niet voldaan zou worden aan de regels van de AVG, kunnen de boetes oplopen tot 20 miljoen (!) euro. Wie moet hier dus aan voldoen?

Om een antwoord te bieden op deze vraag van 20 miljoen, moet men 2 begrippen in het achterhoofd houden.

## Het eerste begrip is “persoonsgegevens”.

Officieel wordt een ‘persoonsgegeven” omschreven als “*alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon („de betrokkene”); als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.*”

Wat houdt dit in? Dat veel meer gegevens vallen onder de gegevensbescherming. De vuistregel is dit: als je via een gegeven of een reeks gegevens een persoon kunt identificeren, dan is dat gegeven of die reeks gegevens een persoonsgegeven. Of het nu namen, adressen, e-mailadressen, IP-adressen, medische gegevens of fysieke kenmerken zijn, indien je via een of meer van deze gegevens iemand kan identificeren, is het een persoonsgegeven.

Bijvoorbeeld: “Donald Trump” op zich is slechts een naam. Er zijn (waarschijnlijk) meerdere Donald Trumps op de wereld. Indien je dus enkel die naam zou doorkrijgen, is dit geen persoonsgegeven. Indien u echter “Donald Trump, Witte Huis, Washington D.C., Verenigde Staten van Amerika” als gegevens zou krijgen, weet je onmiddellijk over wie het gaat. De persoon is in deze zeer makkelijk te identificeren.

De context is met name zeer belangrijk. Gegevens in situatie A zijn geen persoonsgegevens, maar diezelfde gegevens in situatie B kunnen dan weer wel persoonsgegevens zijn volgens de AVG.

Bijvoorbeeld: een IP-adres is een unieke code voor elk toestel dat met het internet verbonden kan worden. Jouw laptop, gsm, tablet of smart-tv hebben elk een unieke code, zodat de gegevens die via internet worden verstuurd, weten naar waar ze moeten gaan. (Als u op 4 schermen tegelijk naar Netflix kijkt en 4 verschillende series tegelijk volgt, weet elke bit en byte naar welk scherm het moet vloeien dankzij het IP-adres).

Indien zelfs een IT’er een willekeurig IP-adres in handen zou krijgen, kan hij of zij hier niemand mee identificeren. Dit IP-adres is in dit geval dus geen persoonsgegeven. Indien Google een willekeurig IP-adres in handen krijgt, en tegelijk ziet dat uit hetzelfde IP-adres dagelijks wordt ingelogd op een specifieke Gmail-account, kan Google redelijkerwijs redeneren aan wie dit adres toebehoort. In dit geval is het IP-adres dus wel een persoonsgegeven.

## Het tweede criterium is dat van “verwerkingsverantwoordelijke”

Officieel is een verwerkingsverantwoordelijke “*een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze verwerking in het Unierecht of het lid statelijk recht worden vastgesteld, kan daarin worden bepaald wie de verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen.*”

Vertaald naar normale-mensentaal betekent dit in feite dat een verwerkingsverantwoordelijke een persoon of bedrijf is die of dat beslist of er gegevens worden verwerkt, welke worden verwerkt en waarom die worden verwerkt.

Bijvoorbeeld: een boekhouder-bediende die een factuur verstuurt en daarvoor opzoekingen verricht naar de naam, het adres en ondernemingsnummer van de gefactureerde, is geen verwerkingsverantwoordelijke. Hij of zij beslist immers niet zelf dat een factuur moet worden opgestuurd naar een bepaalde persoon of onderneming. Het bedrijf dat als werkgever optreedt voor de boekhouder-bediende is dan weer wel de verwerkingsverantwoordelijke. Dat bedrijf beslist namelijk dat de factuur verstuurd moet worden.

**Samengevat is het antwoord op de vraag “wie moet voldoen aan de AVG”: de verwerkingsverantwoordelijke die persoonsgegevens verwerkt, moet voldoen aan de AVG. Telkens je als werkgever persoonsgegevens verwerkt, val je dus onder deze verordening. Dit betekent dat, om aan de AVG te voldoen, je ook enkele zaken in het achterhoofd moet houden wanneer je met persoonsgegevens in aanraking komt.**

# Hoe?

Wat moet je nu doen om “AVG-proof” te zijn? Als je als budgethouder zelf werkgever bent, heb je een ondernemingsnummer en ben je dus gekend als weliswaar atypische, doch kleine onderneming. Heel wat van de zware verplichtingen zijn dus niet op u van toepassing. De enige grote verplichting is het bijhouden van een **dataregister**.

In dit register worden alle verwerkingen opgesomd, zodat dit een overzichtelijk geheel vormt. Hoe zit dit nu in elkaar?

Dit register heeft een aantal verplichte velden. Die moet u dus invullen. Dat kan echter vrij eenvoudig: bijna elke kolom voorziet in een lijstje. Als je het daar niet vindt, schrijf dan in de kolom ernaast wat je precies wil aangeven.

Deze kolommen zijn “naam verwerking” (wat doet u precies), “doel verwerking” (waarom doet u het), “categorie gegevens” (wat vraag je juist op), “categorie betrokkenen” (over wie vraag je het juist op), “bewaartermijn” (hoe lang houd je die gegevens bij, dat mag tussen de 0 en 99 jaar liggen, maar mag niet onbeperkt zijn), “veiligheid” (hoe worden die gegevens beveiligd? Dat mag algemeen omschreven worden, vb. “computer met wachtwoord in gesloten kantoor”) en “categorie ontvangers” (wie krijgt die informatie juist). De laatste categorieën gelden enkel als je gegevens buiten de EU zou versturen, wat waarschijnlijk niet het geval is. Daar mag je dus een streepje zetten.

Wat moet je met het register als dat ingevuld is? Waarschijnlijk niets. Dit register zal het eerste document zijn dat bij een eventuele controle zal opgevraagd worden, maar de kans dat uw onderneming ooit gecontroleerd zal worden, is eerder klein.

Is dit het enige wat je moet doen? Nee, je moet ook enkele kleine, praktische aanpassingen maken aan je werking als werkgever. Met andere woorden: de manier van werken met gegevens moet een beetje veranderd worden.

Wat **elektronische gegevens** betreft, moet je steeds enkele vragen in het achterhoofd houden:

**“Heb ik het nodig?”**

Wanneer je bepaalde gegevens opvraagt, moet je jezelf steeds de vraag stellen of je die gegevens wel nodig hebt voor de taak die je wil volbrengen. Indien u ze niet nodig heeft, laat u die gegevens best met rust.

**“Wat doe ik ermee?”**

Wanneer je dan bepaalde gegevens verwerkt omdat je die verwerking nodig hebt, is de vraag wat je ermee doet. Indien je gegevens moet doorspelen aan een sociaal secretariaat, mag u in de mail geen anderen in CC of BCC zetten.

Volgens de AVG moeten de gegevens gebruikt worden voor het doel waarvoor ze nodig zijn, niet meer, niet minder.

**“Hier ben ik echt niet in geïnteresseerd. Wat nu?”**

Je hebt het zeker ooit al meegemaakt, een mail die voor Jan Verstraete bedoeld was, komt bij Jan Verstraeten terecht. Misschien zat je aan het ontvangende eind, misschien aan het versturende eind van zo’n fout geadresseerde mail.

Indien die mail nu vol zou staan met persoonsgegevens (bijvoorbeeld een uitgebreid Excel-bestand met informatie over tientallen patiënten) en je opent deze per ongeluk, zit men in feite met een zogenaamd **“datalek”**. Wat kan je hier nu mee doen?

Ten eerste, doe je niks met deze gegevens. Je mag ze niet opslaan, niet doorsturen, niet afdrukken etc. Ten tweede breng je natuurlijk diegene die de gegevens verstuurd heeft op de hoogte van zijn of haar foutje, zodat de info bij de juiste persoon terecht kan komen. Deze datalek wordt best gemeld aan de verwerkingsverantwoordelijke.

**“Hoe lang mag ik het bijhouden?”**

In principe mag je niets meer onbeperkt bijhouden. Je kan een termijn kiezen, van 0 tot 99 jaar na het laatste contact met jouw persoonlijke assistent of werknemer, maar je moet wel degelijk een periode kiezen. Die moet ook redelijk blijven, dat wil zeggen dat, voor minder belangrijke gegevens, de termijn korter zal moeten zijn dan voor belangrijke gegevens. Meestal spreekt de gepaste termijn voor zich. Na die termijn dien je gewoon die gegevens in de prullenbak te gooien.



Het kan zeker ook dat u met **papieren gegevens** in aanraking komt. Niet alle dossiers zijn gedigitaliseerd, denk maar aan personeelsdossiers of oude(re) facturen.

Het is moeilijker om papieren gegevens volledig AVG-proof te maken. Om deze bijvoorbeeld enkel toegankelijk te maken voor bepaalde bevoegde personen, zouden deze dossiers in een speciale kamer, kast of kluis moeten zitten waar enkel die bepaalde mensen de code voor kennen. Dit is moeilijk haalbaar, zowel om budgettaire, praktische als tijdsredenen.

**Je kan echter wel enkele voorzorgen nemen:**

* Laat geen dossiers in het rond slingeren of in je auto liggen, om kansen op “datalekken” zo klein mogelijk te houden.
* Probeer dossiers zoveel mogelijk in archiefkasten te bewaren. Indien je gedaan heeft wat je moest, plaats het dan terug en laat het niet op je bureau liggen.

Uiteindelijk dien je gewoon je gezond verstand te gebruiken (wat dus gewoon een voortzetting is van wat je nu al doet). Voor jou zal er dus weinig veranderen, waardoor deze nieuwsbrief niet meer is dan een geheugensteuntje.