bron 21 maart 2018
https://www.smartbiz.be/achtergrond/174280/stand-van-zaken-zijn-belgische-bedrijven-klaar-voor-de-gdpr-deadline/

Stand van zaken: zijn Belgische bedrijven klaar voor de GDPR-deadline?

Volgende maand gaat de General Data Protection Regulation officieel van kracht in België, maar veel bedrijven zijn nog niet compliant. We maken een stand van zaken op.

Op vrijdag 25 mei is het D-day bij Belgische bedrijven: vanaf dan treedt de General Data Protection Regulation (GDPR) officieel in werking. Een broodnodige regelgeving voor burgers, maar een heus huzarenstukje voor bedrijven om compliant te raken. Helaas zijn vele organisaties nog niet op de hoogte dat er een monsterboete boven hun hoofd hangt als ze geen actie ondernemen (tot vier procent van de totale bedrijfsomzet). Is het voor hen te laat om tijdig conform te zijn aan de nieuwe privacywetgeving? Om een stand van zaken op te stellen spraken we met Anja Lemmens, data protection officer bij Intigio, en Philippe De Backer (Open Vld), Staatssecretaris voor Privacy. Ze schijnen onder meer licht over de

misverstanden die de ronde doen over de Europese verordening.

Philippe De Backer (Open Vld) is de Staatssecretaris voor Bestrijding van de Sociale Fraude, Privacy en de Noordzee.

Wat is de GDPR?

Ongetwijfeld heb je ondertussen al over de GDPR gehoord. Mocht je in de afgelopen twee jaar onder een steen hebben geleefd, dan leggen we nog (voor één keer) uit waarvoor de nieuwe privacywet staat. De GDPR of de Algemene Verordening Gegevensbescherming (AVG) is een geheel aan regels om de gegevens van Europese burgers beter te beschermen. De wetgeving werd op het einde van 2015 goedgekeurd en bestaat uit twee delen: de Regulation, die van toepassing is op de bedrijfswereld, en de Directive, voor overheidsdiensten zoals politie en justitie.

De GDPR is geen geheel nieuwe wetgeving, maar een herziening van de Data Protection Directive (DPD). Deze richtlijn werd opgesteld in 1995, in een tijdperk waarin Facebook en Google nog niet de scepter zwaaiden op het internet. De DPD was gedateerd en werd bovendien door elke Europese lidstaat op een andere manier geïnterpreteerd, wat leidde tot fragmentatie en onduidelijkheid. Om die reden is de GDPR geen richtlijn, maar een verordening, wat betekent dat de tekst overal op dezelfde wijze wordt toegepast.

Persoonsgegevens

Er was dringend nood aan modernisering om ontwikkelingen zoals cloud en sociale media – en de enorme hoeveelheden data die daarmee gepaard gaan – het hoofd te bieden. De nieuwe GDPR is van toepassing op alle automatische en digitale verwerkingen van persoonsgegevens, iets wat vandaag de dag in nagenoeg alle bedrijven gebeurt. Concreet zullen bedrijven die persoonsgegevens verzamelen, volledig moeten voldoen aan de nieuwe set regels van de GDPR.

Wat bedoelt Europa nu met 'persoonsgegevens'? Het gaat hier om alle informatie waarmee iemand geïdentificeerd kan worden, zoals een naam, foto of telefoonnummer. Over deze data moeten bedrijven voortaan transparant zijn. Ze moeten burgers informeren hoe de gegevens worden verzameld en verwerkt, en binnen de 72 uur melden als er een datalek plaatsvindt. Ook krijgen burgers meer autonomie over hun persoonsgegevens. Als ze willen dat hun data gewist of overgezet wordt naar een ander bedrijf (bijvoorbeeld bij het wisselen van telecomprovider), dan moeten de desbetreffende organisaties hiermee instemmen.

Negatieve connotatie

Voor vele bedrijven is de impact van de GDPR groot. Daarom kan de nieuwe verordening rekenen op heel wat kritiek. Toch zijn er ook heel wat voordelen voorhanden. De eenmaking van een versnipperd legaal raamwerk bijvoorbeeld. Wegens de uiteenlopende interpretatie van de vorige wetgeving, moesten bedrijven voordien rekening houden met 28 verschillende raamwerken rond databescherming. Binnenkort zorgt de GDPR voor één legaal kader dat in heel Europa geldt. Zo wordt het gemakkelijker voor kmo's om de activiteiten in het buitenland uit te breiden, aangezien ze geen rekening moeten houden met een andere wetgeving. Bovendien kan de GDPR bedrijven op die manier collectief zo'n 2,3 miljard euro per jaar kunnen besparen; geld dat normaal naar advocaten en consultants zou gaan om wijs te geraken uit de verschillende wetgevingen.

Taxibedrijf Uber stak in 2017 een hack van 57 miljoen klantgegevens in doofpot. Met de komst van de GDPR moeten dergelijke datalekken sneller gemeld worden.

“Vele bedrijven zien de nieuwe regels als bijkomende bureaucratische overlast”, aldus Staatssecretaris De Backer. “Nochtans kunnen de ondernemingen zich ermee profileren. De klanten zullen kritischer worden over hoe met hun gegevens moet omgegaan worden. Zij verlangen meer duidelijkheid en verantwoordelijk van het bedrijfsleven en de overheid. Voor bedrijven die zorgvuldig omgaan met persoonsgegevens, is de GDPR eerder een opportuniteit. Aan de hand van audits kunnen privacylabels worden toegekend, die de marktpositie van onze kmo’s en bedrijven in het algemeen versterken.”

DPO

De impact van de GDPR op een bedrijf hangt in grote mate af van de activiteiten die het uitvoert. Toch zijn er bepaalde voorbereidingen die elk bedrijf, ongeacht de grootte of aard van zijn activiteiten, best kan treffen. De belangrijkste verandering die de GDPR voor een doorsnee bedrijf – dat niet specifiek datagevoelige gegevens verwerkt – met zich meebrengt, is dat het moet kunnen aantonen dat het zijn best heeft gedaan om de wetgeving na te leven. Voor grotere firma’s is het bijhouden van big data een heuse boterham.

Daarom is het aangeraden voor vele organisaties om een data protection officer (DPO) aan te nemen. De DPO, of de 'functionaris voor gegevensbescherming', is degene die controleert of alla data naar behoren wordt bewaard, gebruikt en gedeeld. Sommige bedrijven hebben al geïnvesteerd in gelijkaardige functies (zoals bijvoorbeeld een privacy officer), maar voortaan wordt de DPO een gevestigde waarde. Hij adviseert enerzijds hoe een bedrijf compliant wordt en welke rechten en plechten het heeft in verband met de bescherming van data. Daarnaast heeft hij een controlerende functie: hij moet toezien dat de wetgeving wordt nageleefd. Hij moet onder meer nakijken of de data adequaat wordt bewaard, of het personeel voldoende wordt getraind en of de nodige audits worden gehouden. Ten slotte fungeert hij als contactpunt voor de externe autoriteiten. Als het bedrijf bijvoorbeeld te maken krijgt met een datalek, kan hij de Privacycommissie te woord staan voor meer informatie.

Nieuwe werknemer nodig?

Anja Lemmens profileert zich als GDPR consultant en richtte daarvoor haar eigen bedrijf Intigio op.

Moet je nu een dedicated DPO aannemen? We vroegen het aan Anja Lemmens, data protection officer bij Intigio. "Dat hangt af van een paar factoren. In drie gevallen is het verplicht om een DPO te hebben. Eén: organisaties in de publieke sector, zoals overheidsorganisaties. Twee: bedrijven die verwerkingen doen die regelmatige en stelselmatige observatie vereisen, zoals een telecomnetwerk die aan tracking doet. Drie: bedrijven die 'bijzondere persoonsgegevens' verwerken, zoals over ras, religie of biometrische gegevens. Denk daarbij aan bijvoorbeeld zorginstellingen of ziekenhuizen." In andere gevallen is het in principe niet verplicht, zolang de organisatie maar GDPR-compliant wordt.

Daarnaast hoeft de data protection officer niet per se een vaste werknemer te worden: je kan ook opteren voor een consultant, zoals Anja Lemmens.

Bovendien kan ook een bestaande werknemer de rol van DPO op zich nemen, zolang zijn andere functie niet in conflict komt met het nieuwe takenpakket. Beide opties kunnen de kosten drukken, en maken het vinden van een geschikte DPO heel wat eenvoudiger. Volgens Lemmens vormt het financiële plaatje immers een grote hindernis voor bedrijven om GDPR compliant te zijn. “Bedrijven willen graag met de beste beveiligde systemen werken, maar dit kost ook een heleboel geld. De processen in bedrijven zijn reeds jaren ingeburgerd, waardoor het zeer uitdagend is om op korte tijd compliant te worden en competitief te blijven.”

Veel vraag naar GDPR-specialisten

Uit een onderzoek van rekruteringsbedrijf Robert Half (oktober 2017) blijkt dat toch heel wat bedrijven een nieuwe werknemer in dienst nemen. Maar liefst zestig procent heeft een (al dan niet tijdelijke) werknemer aangeworven die instaat voor de implementatie van de GDPR. “Bedrijven willen werkkrachten met overdraagbare vaardigheden om hun compliance te garanderen, maar gekwalificeerde GDPR-specialisten zijn dun gezaaid”, aldus Jeroen Diels, de Director van Robert Half.

Over welk profiel moet een DPO beschikken? Lemmens: “Een matuur persoon als DPO is zeker aangewezen. Bovendien moet hij idealiter over een aantal kwaliteiten beschikken, aangezien een DPO een adviserende, informerende en controlerende rol heeft. Zo is een communicatieve geest een must en moet hij over voldoende knowhow beschikken van juridische, administratieve en technische aard. Een gezonde dosis vertrouwen vormt de kers op de taart.”

België is nog niet klaar

Niet alle organisaties beseffen welke potentiële impact de GDPR kan hebben op hun bedrijfsvoering. Onderzoek van Kaspersky Lab van eind vorig jaar toont aan dat heel wat Belgische bedrijven nog onvoldoende voorbereid zijn op de komst van de GDPR of zelfs niet weten wat de verordening precies inhoudt. Amper een derde van de Belgische IT-professionals wist wat de GDPR juist is. Daarmee was ons land de rode

lantaarn in de studie, die ruim 2.000 beleidsmakers ondervroeg bij bedrijven met meer dan vijftig werknemers in elf Europese landen.

32 procent van de Belgische respondenten wist wat de GDPR is, maar had geen zicht op de inhoud ervan. Het percentage van professionals dat met zekerheid durfde te stellen dat ze wisten wat de wetgeving omvat, was minder dan twintig procent. Zestien procent van de Belgen zegt zelfs dat ze er nog nooit van hebben gehoord. Opvallend: primus van de klas is het Verenigd Koninkrijk, ook al zegt het land binnenkort vaarwel aan de Europese landen. Al is de eerste plaats relatief: hier weet 49 procent van de respondenten wat de nieuwe privacywetgeving precies inhoudt. Volgens de Europese Commissie zijn enkel Duitsland en Oostenrijk al klaar voor de GDPR.

Ondanks dat het Verenigd Koninkrijk binnenkort de Europese Unie verlaat, scoren ze het best op een enquête over de GDPR.

Geen reden tot paniek

“Bedrijven hoeven zich geen zorgen te maken zolang ze aandacht hebben voor de vier pijlers van de nieuwe privacywetgeving”, stelt De Backer gerust. “Ik soms ze nog eens alle vier op. Eén: hou je gegevensverwerkingsproces kritisch tegen het licht. Twee: leg een register aan van de gegevens die je verwerkt. Drie: meld datalekken aan de Gegevensbeschermingsautoriteit. Vier: stel een data protection officer aan

als je een grote gegevensverwerker bent. De nieuwe gegevensbeschermingsautoriteit zal klaar staan om bedrijven hierin van A tot Z te begeleiden."

"Ik heb er alle vertrouwen in", gaat hij verder. "Van in het begin heb ik ingezet op bewustwording en begeleiding waarbij de verschillende sectorfederaties en het maatschappelijk middenveld nauw betrokken worden. Mijn kabinet, administratie en ikzelf hebben al ettelijke malen deelgenomen aan studiedagen, infosessies en sectorspecifieke trainingen. Ook de partners binnen de Privacycommissie nemen hierin hun rol op, bijvoorbeeld Unizo. Alle Belgische bedrijven moeten op een gegeven moment hier kennis van genomen hebben. Awareness raising is van cruciaal belang: niet om bedrijven angst aan te jagen, maar om hen bewust te maken van de noodzaak om hun processen van gegevensverwerkingen te analyseren in het licht van de nieuwe verordening. Ik kan moeilijk geloven dat er een bedrijf in België is dat nog niet op de hoogte is van de nieuwe wetgeving die eraan zit te komen na alle inspanningen die we geleverd hebben. Moest dit toch het geval zijn en ze lezen dit artikel: neem zo snel mogelijk contact op met de nieuwe Gegevensbeschermingsautoriteit. Daar zullen ze je graag verder helpen."

Prille wetgeving

Dat bedrijven zenuwachtig zijn, is grotendeels omdat bepaalde GDPR-concepten nog voor interpretatie vatbaar zijn. Daar leveren De Backer en zijn team de nodige inspanningen. "Op Europees niveau zijn al verschillende richtlijnen uitgewerkt, maar ook op nationaal niveau heeft de Privacycommissie al verschillende aanbevelingen neergepend, bijvoorbeeld over de functie van de data protection officer. Ook bij de sectorfederaties kan het nodige gedaan door gedragscodes uit te werken, in samenwerking met de Privacycommissie."

Op wetgevend vlak zijn eveneens initiatieven genomen om rond te raken met de omzetting van de Europese privacy-verordening. "Eind vorig jaar werd de wet goedgekeurd die de nieuwe structuur en bevoegdheden vastlegt van de nieuwe Gegevensbeschermingsautoriteit. Deze vervangt de

Privacycommissie en moet een echte compagnon worden die bedrijven begeleidt en informeert. We kunnen immers van onze bedrijven niet verlangen dat ze zich conformeren aan een nieuwe wetgeving zonder hen daarin bij te staan. Ook is op 16 maart de kaderwet-De Backer goedgekeurd, die de huidige privacywet vervangt. Dit is het sluitstuk van de omzetting van de Europese verordening."

Monsterboetes

Bedrijven die aan de GDPR verzuimen, kunnen zware repercussies verwachten. Zo wordt er in de GDPR gewag gemaakt van verschillende boetes. Wanneer de verzamelde data niet correct wordt beheerd, een serieus datalek niet wordt gemeld of het bedrijf geen risico-assessment houdt, kan de boete oplopen tot twee procent van de jaarlijkse omzet. Voor ernstige misstappen kan dat bedrag stijgen tot maar liefst vier procent van de omzet, met een maximum van 20 miljoen euro. Worden vanaf 25 mei de grote middelen bovengehaald? Lemmens: "Bedrijven denken dat ze tegen die datum volledig GDPR compliant moeten zijn, maar dit is niet zo. Je moet wel kunnen aantonen dat je ermee bezig bent om je bedrijf compliant te maken."

Er worden niet meteen grove middelen bovengehaald om GDPR-compliancy te forceren.

“Geen zorgen, we gaan niet meteen met de bezem erdoor”, beaamt De Backer. “Laat mij alle bedrijven meteen geruststellen: de nieuwe Gegevensbeschermingsautoriteit moet in eerste instantie de bedrijven bijstaan in de overgang naar de nieuwe wetgeving. We zijn niet van plan om meteen de bazooka’s boven te halen. Pas als het niet anders kan zal zij overgaan tot proportionele sancties. Deze bestaan uit een brede waaier, variërend van sepot over waarschuwingen, bevelen tot schorsing, bevriezing of in overeenstemming brengen van verwerking tot effectieve boetes.”

Dat betekent niet dat de Gegevensbeschermingsautoriteit een katje wordt om zonder handschoenen aan te pakken. De Backer: “We hebben er bewust voor gekozen om een autoriteit op te richten die ook tanden heeft. Dat was nu niet het geval. In het belang van de privacy van de burger is dat onaanvaardbaar.” Het wordt duidelijk: het GDPR-project staat gelijk aan een heuse revolutie in businessland en wordt voor vele bedrijven ingrijpend. We sluiten af met een geruststellende boodschap van onze Staatssecretaris voor Privacy: België is *on track*.