White Paper

GDPR

Hoe bereid je je voor op de vernieuwde GDPR?

Maak uw organisatie klaar voor de GDPR:

10 stappen toegelicht

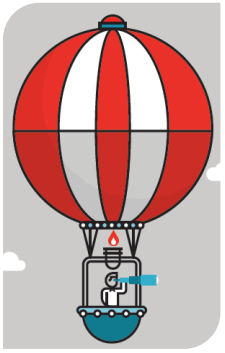
creditsafe

Inhoudstafel: GDPR

Hoe bereid ik me voor op de vernieuwde GDPR?

Wie is Creditsafe?

Van "changing the way business information is used", streven we naar wereldwijde erkenning om zo naar "the global business intelligence experts" te evolueren. Met de nodige passie en de juiste drijfveer willen we superieure informatie leveren, om zo aan de noden van onze klanten te kunnen voldoen. Elke klant, groot of klein, willen we voorzien van de vertrouwde inzichten met behulp van onze sterke data en intuïtieve platforms.

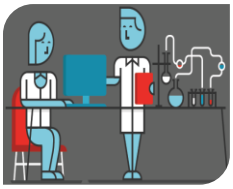


GLOBAL

Met 16 kantoren in 12 landen en 1.500 collega's wereldwijd, kunnen we met de nodige trots meegeven dat we een (h)echte, wereldwijde leverancier zijn van handelsinformatie. Een netwerk van 26 partners laat ons toe het productaanbod, de data en de inhoud te versterken, te verbeteren en te verbinden, zodat klanten steeds nieuwe inzichten kunnen verkrijgen over meer dan 230 miljoen bedrijven in 170 landen.

BUSINESS

Wij hebben de manier waarop bedrijven gebruik maken van handels-informatie veranderd, en uiteraard blijven we onze service koesteren en aanbieden om bedrijven te ondersteunen in het realiseren van hun doelstellingen. Ons productgamma biedt een scala aan zakelijke oplossingen voor credit risk management, conformiteitsprocedures en marketing data. Wij begrijpen de markt en wij begrijpen bedrijven.



INTELLIGENCE

Kennis is macht, en onze kennis is wat ons groot heeft gebracht. Met behulp van een combinatie aan unieke datasets, streven wij ernaar om een schat aan productoplossingen te creëren en te leveren die gericht zijn op bedrijven van alle groottes. Dit alles gecombineerd met de nodige inzichten die belangrijk zijn om sterke en geïnformeerde zakelijke beslissingen te kunnen nemen.

EXPERTS

Met bijna 15 jaar ervaring in het bedrijfsleven en een gemiddelde van 10 jaar ervaring bij onze account management teams, is het ons doel om te blijven innoveren, om onze kennis uit te breiden en zo echte experts te worden in alle gebieden, op alle markten.

Hoe bereid je je voor op de vernieuwde GDPR?

Introductie

De vernieuwde regelgeving van de gegevensbescherming is reeds in werking getreden op 24 mei 2016. Maar, weliswaar, krijgen bedrijven de kans om zich tijdig voor te bereiden en de nodige aanpassingen te doen. Vanaf 25 mei 2018 moeten alle bedrijven klaar zijn met hun huiswerk.

De wet op de privacy is uiteraard niets nieuws. De verschillende regels die deze omvat bestaan al sinds geruime tijd. De '(ver)nieuw(d)e' regels zullen de huidige structuur (licht) wijzigen, wat betekent dat er enkele nieuwigheden zijn en dat huidige regels aangepast en verbeterd worden. Dit alles om de simpele reden dat we steeds meer en meer in een veranderlijke samenleving leven, waar digitalisatie, automatisatie en sociale media een grotere impact op ons leven uitoefenen. Uit een recent onderzoek van "The Economist" is uitgewezen dat de meest waardevolle bron van de wereld niet langer olie is, maar de verzamelde data.

De lokale autoriteiten, verantwoordelijk voor de privacy bescherming, en de Europese Groep gegevensbescherming artikel 29 zullen de nodige bijstand verlenen in samenwerking met de verschillende sectoren. Bijkomende richtlijnen en instrumenten zullen worden uitgewerkt om de bedrijven te helpen de nodige voorbereidingen te treffen.

De AVG of GDPR zal vooral de nadruk leggen op de documentatieplicht van de verwerkingsverantwoordelijken. Het is ook belangrijk om te weten dat de bepalingen van de GDPR niet voor elk bedrijf even zwaar doorwegen. Zo zijn de nieuwe bepalingen van zeer groot belang voor bedrijven actief in een B2C secor. Nog specifieker voor bedrijven die aan profilering doen of organisaties dat werken met persoonsgegevens, zoals de gegevens van kinderen.

Wat is GDPR?

Vooraleer we verder gaan in dit document, leggen we eerst vereenvoudigd uit wat GDPR betekent.

De General Data Protection Regulation (GDPR) is de Europese wetgeving over hoe overheden, instanties, bedrijven en organisaties moeten omgaan met het gebruiken en verwerken van persoonsgegevens en de bijhorende privacy. Deze vernieuwde regels, die opgenomen zijn in de GDPR, dienen uiteraard nageleefd en gerespecteerd te worden.

Persoonsgegevens slaan letterlijk op alle informatie die gelinkt kan worden aan de identiteit van een persoon. Dit is heel variërend, zoals gegevens van patiënten van bvb. een ziekenhuis, tot kindergegevens, tot IP-adressen.

De GDPR wil juist voorkomen dat het gebruik en de verwerking van gegevens schade zou kunnen berokken aan de personen in kwestie.

Waarom is dit nodig?

De nieuwe GDPR heeft als doelstelling om de huidige wet- en regelgevingen extra kracht bij te zetten en om de tekortkomingen of hiaten te 'herstellen'. Men moet hierbij denken aan de verschillende datadocumentatieregels, IT procedures, het op de hoogte stellen van bepaalde 'inbreuken' aan eindgebruikers en overheden, het versterken van dataminimalisatie regels en dergelijke.

Het toezicht zal gebeuren op alle persoonlijke gegevens zoals namen, persoonlijke adressen, persoonlijke telefoonnummers, rekeningnummers, emailadressen en IP adressen. Eigenlijk is dit toezicht vrij logisch als men voorgenoemde gegevens bekijkt. Het is belangrijk dat er een duidelijke en gestructeerde regelgeving is met zowel de nieuwe regels als de versterkte bestaande regels.

M.a.w. het hele idee achter de 'nieuwe GDPR' bestaat uit het legaliseren van logische data beveiligingsideeën, met voornamelijk de bescherming van het verzamelen van persoonlijke data, het minimaliseren van deze data en het verwijderen van bepaalde data die niet noodzakelijk is of niet (meer) gebruikt wordt.

Op welke bedrijven en organisaties is de GDPR van toepassing?

De GDPR is eigenlijk van toepassing op praktisch alle bedrijven en organisaties. Dit vanwege het feit dat vrijwel alle organisaties voor hun bedrijfsuitvoering en dienstverlening diverse soorten persoonsgegevens (kunnen) verwerken. De GDPR legt specifiek de nadruk op twee verschillende rollen, namelijk de 'controllers' en de 'processors' (*wordt verderop toegelicht*).

Wat zijn persoonsgegevens overeenstemmend met de GDPR (en dewelke niet?)

In alle eerlijkheid is het steeds opnieuw vatbaar voor interpretatie. M.a.w. er kan altijd discussie ontstaan over welke gegevens als persoonsgegevens onder de GDPR vallen en dewelke niet. Wat we met zekerheid kunnen zeggen, is dat organisaties heel wat minder gegevens (gaan) moeten verzamelen. M.a.w. enkel de data gebruiken die noodzakelijk zijn voor de doeleinden van de organisatie.

Wat zijn persoonsgegevens?

Persoonsgegevens omvat informatie die gelinkt kan worden aan een identiteit. Het zijn de gegevens waarmee men een persoon kan herkennen zoals foto's, namen, adressen en rijksregisternummers. Om deze data te gebruiken, zouden we voortaan de toestemming nodig hebben van de betrokkene persoon. Dit slaagt zowel op persoonsgegevens te verzamelen vanaf 2018, als de reeds bestaande verzamelde data.

Wat met IP-adressen, gebruikersnamen en dergelijke?

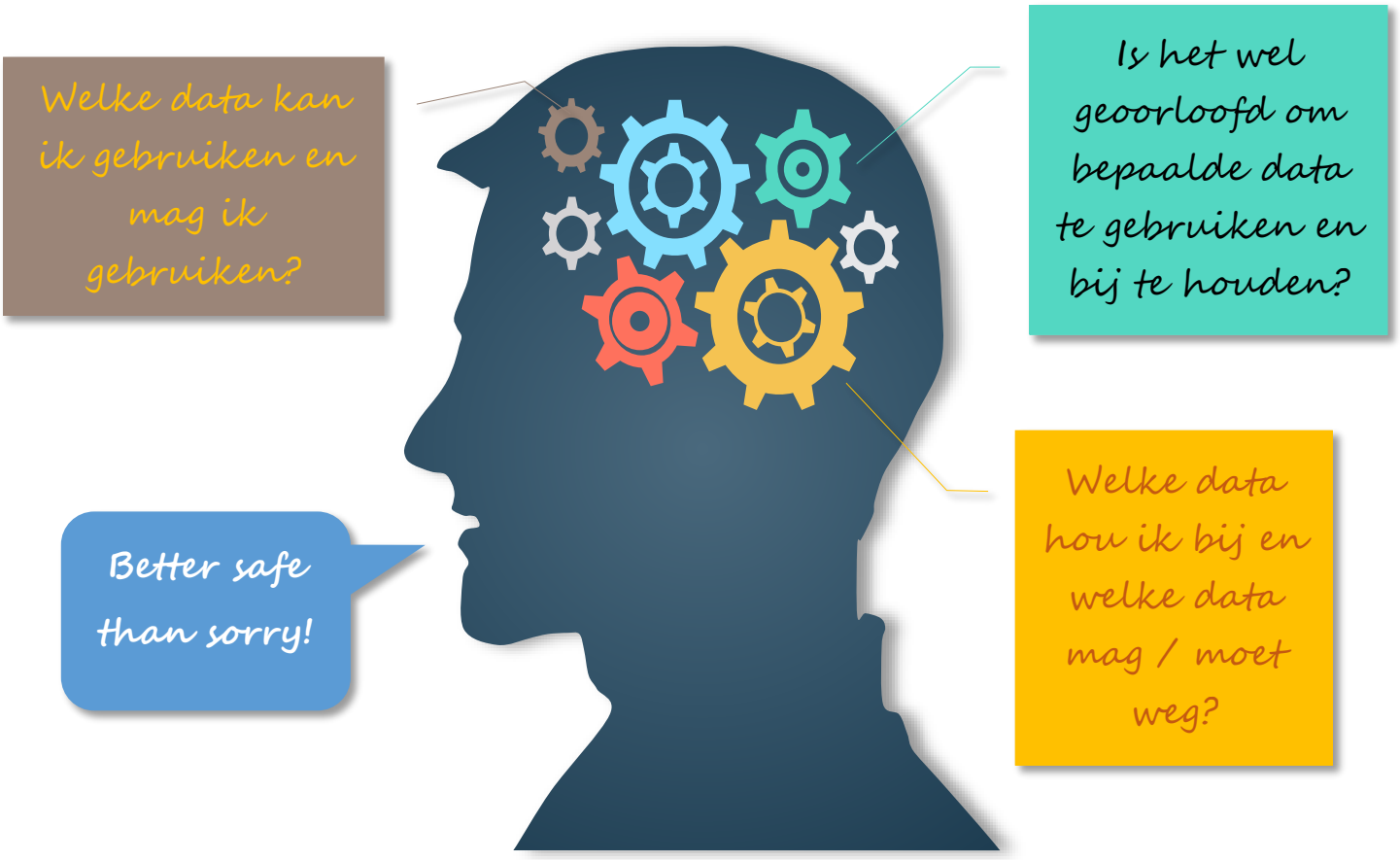
Ook dergelijke gegevens blijven niet gespaard. Alles wat aan een (persoons)naam kan gelinkt worden, valt onder de vernieuwde wetgeving van de GDPR. Neem nu IP-adressen, deze kunnen via een omweg herleid worden naar een persoon.

Anonieme gegevens

De uitzondering op de regel zijn de geanonimiseerde persoonsgegevens. Onder deze gegevens vallen versleutelde bestanden, anonieme data, onherkenbare foto's, etc.

Conformiteit

Zoals men kan merken, vele organisaties zullen veel werk voor de boeg hebben. De grote hoeveelheid aan data die zij ter beschikking hebben en gebruiken, zullen dus moeten herzien worden.



Basisprincipe: het verschil tussen 'controller' en 'processor'

Controller:

De controller is de verantwoordelijke voor de verwerking van de gegevens. Het is elke natuurlijke- of rechtspersoon die de doeleinden en de middelen voor de verwerking van de persoonsgegevens bepaald. We kunnen hier bijvoorbeeld denken aan een adverteerder die gegevens nodig heeft voor de promotie van zijn of haar product en/of dienst.

Processor:

De processor is de eigenlijke verwerker voor de behandeling van persoonsgegevens. Het is elke natuurlijke- of rechtspersoon die de gegevens verwerkt in naam van de controller. We kunnen hier bijvoorbeeld denken aan callcenters, IT-leveranciers en dergelijke.

Wat zijn de rechten van de betrokkenen?

Verwerking:

De verwerking van de persoonsgegvens moeten duidelijk opgenomen worden in de privacy voorwaarden. Tevens moet er een zeer duidelijke reden zijn waarom gegevens moeten verwerkt worden. Voor de verwerking moet er vooraf toestemming gevraagd worden aan de betrokken personen, met een gegronde reden. Hieronder vindt u een tabel van de rechten van de betrokkenen:

Nu	Nieuwe rechten
- Recht om **geïnformeerd** te worden - Recht om **toegang** te hebben tot zijn of haar gegevens - Recht om **foutieve gegevens** recht te zetten (=rectificatie) - Recht om **bezwaar** te maken als men ernstige en gerechtvaardigde redenen kan aanleveren. Voor het gebruik van uw gegevens in direct marketing, waaronder reclame acties, kan u verzet tonen zonder enige verantwoording. De enige **uitzondering** op de regel: wanneer gegevens nodig zijn om een overeenkomst af te sluiten.	- Recht om niet te worden onderworpen aan een geautomatiseerde beslissing in geval van **profilering** wanneer bepaalde aspecten van uw persoonlijkheid geëvalueerd worden die voor de betrokkene ingrijpende gevolgen kan hebben. - Recht om **vergeten** te worden - Recht op een **beperking van het verwerken** van gegevens - Recht op **gegevensoverdraagbaarheid** waarbij de betrokkene onmiddelijk zijn gegevens van de ene naar de andere verwerkingsverantwoordelijke kan worden doorgezonden Dit recht kan slechts uitgeoefend worden als de verwerking gebeurt op basis van een toestemming of overeenkomst en het een geautomatiseerde verwerking betreft.

De nieuwe en voornaamste vereisten van de GDPR:

Zoals u zich wel kan inbeelden omvat de GDPR heel veel teksten, regelgevingen en wetsregels. Alle nieuwigheden kan u ook terugvinden in de verniewde GDPR van de Europese Unie zelf. Hieronder vindt u de voornaamste en belangrijkste punten van de 'nieuwe' GDPR.

Data Protection by Design - Data Protection by Default.

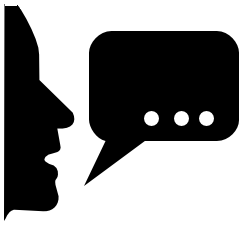
Wanneer een bepaald informatiesysteem bedacht en ontwikkeld wordt, moet er rekening gehouden worden met de bijhorende privacy van een gebruiker. Dit geldt ook voor organisaties die persoonlijke gegevens verwerken. Elke instantie / organisatie dient interne beleidsmaatregelen te hebben betreft de privacy. Die maatregelen dienen ook te voldoen aan de gegevensbescherming door ontwerp en gegevensbescherming door standaardinstellingen (**Data Protection by Design en Data Protection by Default**).

Gegevensbescherming door ontwerp is een benadering die als doel heeft de privacy te bevorderen om ervoor te zorgen dat de waarborgen voor de gegevensbescherming worden ingebouwd in producten en diensten vanaf de eerste ontwikkelingsfase van de software, goederen en diensten. Nog anders gesteld wil dit zeggen dat ondernemingen, die gegevens verwerken, de privacy van personen en de bescherming ervan zeer ernstig moeten nemen vanaf de eerste stap, namelijk de conceptfase.

Welke technische en organisatorische maatregelen zijn er?

Pseudonimiseren maakt deel uit van een 'privacy enhancing technique'. Een techniek die als doel heeft de bescherming van de privacy van gegevens te bevorderen. Met pseudonimiseren worden alle persoonlijke gegevens omgezet in een bepaalde dataset die men niet direct kan herleiden naar een persoon. M.a.w. de gegevens worden geëncrypteerd of versleuteld. Met deze techniek worden dus alle direct identificeerbare gegevens van een persoon weggehaald, bvb. namen, geboortedatums, adressen,... en gevonverteerd in een bepaalde code. Achteraf kunnen deze codes terug omgezet worden door gebruik te maken van de encryptiecode of sleutel, opdat het terug 'leesbaar' wordt. De dataset en de sleutel moeten appart bewaard worden. Pseudonimiseren vermindert het privacyrisico van betrokkenen, maar ook het risico voor organisaties die met deze gegevens werken.

Transparant te werk gaan met betrekking tot de verwerking van persoonsgegevens. Als verwerkingsverantwoordelijke moet men gebruik maken van een duidelijke en eenvoudige taal als het gaat over de identiteit, de doeleinden van de verwerking en eventuele bijkomende informatie dat verstrekt kan worden. De betrokken personen dienen op de hoogte gesteld te worden in geval van risico's, regels, garanties en rechten die samenlopen met deze verwerking.



Controleerbaar:

De betrokkenen moeten in staat zijn om een bepaalde controle te kunnen uitvoeren op de verwerking van zijn of haar gegevens. De verwerkingsverantwoordelijken moeten in staat zijn om bepaalde veiligheidskenmerken te kunnen aanpassen, verbeteren en zelfs wijzigen.

Minimalisering: Alle organisaties die gegevens verwerken dienen de nodige maatregelen te nemen opdat enkel gegevens verwerkt worden die echt noodzakelijk zijn voor de doeleinden van die organisatie. We noemen dit ook minimalisering van dataverzameling.

Het principe van 'Less is more'

De tijdspanne van het bijhouden van de nodige data, de minimalisering van data-verzameling en de onderverdeling ervan zullen er uiteindelijk voor zorgen dat het veiliger is voor de privacy. Deze 3 elementen zorgen ervoor dat hackers bijvoorbeeld minder kunnen stelen. Indien een hacker toegang heeft tot ontelbare gegevens en deze zal gebruiken voor 'phishing', dan hebben organisaties een veiligheidsrisico ontwikkeld voor hun klanten. Door de nieuwe regelgeving, met name meer transparanter te werk gaan, kan de EU gemakkelijker achterhalen van waar dit 'lek' afkomstig is.

Big Data en privacy kunnen hand in hand gaan dankzij privacy by design:

Data Protection Impact Assessments (DPIA)

In een letterlijke context wilt dit zeggen: de gevolgen of effecten beoordelen over de bescherming van data of privacy. Om een duidelijk inzicht te verkrijgen in waar de risico`s liggen, stelt de GDPR dat deze ricico`s via een DPIA in kaart moeten worden gebracht. Ondernemingen moeten privacy-problemen identificeren, begrijpen en aanpakken, die kunnen ontstaan nog voor er producten of diensten worden ontwikkeld. Dit dient dus te gebeuren alvorens nieuwe activiteiten tot stand komen.

Documentatieplicht

De documentatieplicht is de meest typerende wijziging. De documentatieplicht houdt in dat de verschillende organisaties moeten kunnen bewijzen welke informatie wordt opgeslagen en welke gegevens verwerkt worden. Anderzijds moeten zij kunnen voorleggen van waar de data afkomstig is, waar en hoe dit opgeslagen wordt en hoe dit alles wordt beschermd.

Doelgericht

Zoals reeds een paar maal vermeld in dit document, persoonsgegevens mogen alleen verwerkt worden voor een specifieke doelstelling. Overdadige verwerking van persoonsgegevens is dus niet toegestaan en bovendien mogen dezelfde gegevens niet zonder toestemming gebruikt worden voor de aanlevering van andere producten of diensten.

Het recht om gewist of vergeten te worden

De betrokken EU-burger heeft het recht om zijn persoonsgegvens te laten wissen of om vergeten te worden. De verwerker is verplicht dit te doen indien die gegevens niet langer nodig zijn voor de doeleinden van de onderneming waarvoor deze juist verzameld werden of wanneer de betrokkene de toestemming tot gebruik ingetrokken heeft. Indien andere partijen ook gebruik gemaakt hebben van de gegevens die de verwerker heeft verzameld, dient de verwerker ook deze partijen op de hoogte te stellen met de boodschap dat de betrokkene een verzoek tot wissen of vergeten heeft aangevraagd.

Uiteraard zijn er een aantal uitzonderingen, zoals: er is geen verplichting indien de gegevens gebruikt worden voor de uitoefening van het recht op vrije meningsuiting en -informatie en het nakomen van wettelijke verplichtingen. Andere redenen kan u steeds terugvinden in de nieuwe regelgeving zelf. Ook belangrijk om te weten, gebasseerd op de grond van het recht om vergeten te worden, heeft men het recht om onjuiste of verouderde privacygevoelige informatie te laten verwijderen uit archieven.

Extraterritorialiteit

Wanneer een onderneming geen 'fysische aanwezigheid' heeft in de EU, maar wel data verzamelt van binnen de EU, valt deze organisatie dusdanig ook onder de GDPR.

Een bekend voorbeeld hiervan is Facebook. Facebook is gevestigd in de Verenigde Staten, maar verzamelt wel persoonlijke gegevens van over de hele wereld, waaronder Europa. Daarom moet Facebook ook conform zijn met deze nieuwe regelgeving. Dit zal dus een grote invloed hebben op bedrijven met e-commerce of cloud doelstellingen op een globaal niveau.

Kennisgeving van breuken of overtredingen

Een niewe regel die bedrijven verplicht om de nodige autoriteiten aan te spreken in geval van een breuk op de dataregelgeving én dit binnen de 72 uur. Belangrijke kantekening betreft deze regel: enkel geldig in het geval dat deze breuk een rechtstreeks gevaar vormt voor de rechten en vrijheden van de betrokkenen.

Data Protection Officer

Een DPO is een persoon, al dan niet gebonden aan het bedrijf, die de desbetreffende organisatie adviseert en informeert betreft de verwerking van persoonsgegevens. De DPO gaat ook na of er geen lekken of breuken zijn in de privacy en moet kunnen aantonen of de desbetreffende organisatie conform is met de regelgeving van de GDPR. Opvallend uiteraard is dat een DPO geen verwerker zelf mag zijn, noch iemand dat een leidinggevende rol heeft binnen de organisatie en moet 1 landstaal machtig zijn.

Boetes

Verschillende boetes kunnen worden uitgedeeld en worden opgelegd, naar gelang de ernst van de overtreding. De EU wil het belang van de nieuwe regelgeving zeker en vast benadrukken. Deze boetes zijn hiervan het voorbeeld, doordat ze grote happen uit een organisatie kunnen nemen, bvb. tot 4% van de globale omzet van de gehele organisatie.

Concluderend...

Concreet kunnen we uit deze verschillende '(ver)nieuw(d)e' zaken aannemen dat het de bedoeling is van de Europese Unie om de bescherming van de privacy van personen te versterken, te verbeteren en te optimaliseren.

Echt afvragen 'waarom' is eigenlijk niet moeilijk.

Steeds meer geautomatiseerde processen, een digitale wereld, het verhaal van 'big data', Global Social Media en zo verder. Het zijn allemaal mooie technologische innovaties. Helaas gaat dit gepaard met concrete gevaren zoals cyberaanvallen, stelen en fraude van persoonlijke gegevens, etc. Denk maar aan de recente cyberaanval van 12 mei 2017, die zware gevolgen heeft gehad voor de gehele wereld. Ziekenhuizen werden 'lam' gelegd, automatische parkeergarages waren als het ware een opendeurdag voor iedereen, bedrijven konden niet normaal functioneren...

Daarom is het meer dan logisch en overduidelijk dat onze persoonlijke data dient beter beschermd te worden. Zoals reeds gesteld in dit document: de meest waardevolle bron van de wereld is niet langer olie, maar de verzamelde (persoonlijke) data (= een schat aan gegevens).

Europa duwt daarom door naar meer sensibilisering naar bedrijven toe. Bedrijven moeten een automatisme hebben, transparant zijn en alles kunnen documenteren omtrend de bescherming van de data die ze gebruiken.

Organisaties moeten het belang kunnen inzien van de gevoeligheid van persoonlijke gegevens.

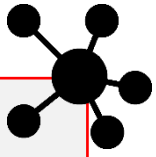
Vervolgens vindt u een stappenplan over hoe u uw organisatie klaar te maken voor de GDPR.
Wenst u meer informatie over Big Data, databescherming of Creditsafe?
Neem dan gerust vrijblijvend contact met ons op:
T: 02/481.88.60
E: info@creditsafe.be

Maak uw organisatie klaar voor de GDPR: 10 stappen toegelicht

1. Bewustmaking

Alle beleidsvormers en bedrijfsverantwoordelijken dienen geïnformeerd te worden over de aangekondigde veranderingen. Deze personen moeten een inschatting (assesment) kunnen maken over welke gevolgen de GDPR of AVG zal teweegbrengen voor de onderneming. Deze inschattingen bepalen dan de verschillende risico's die eventueel aanwezig kunnen zijn. De implementatie van de assesment kan behoorlijk wat uitlokken op de huidige processen, procedures, middelen en uitvoeringen. Dit verklaart ook de lange overgangsperiode van de nieuwe regels, opdat bedrijven zich tijdig kunnen voorbereiden.

2. Data-mapping



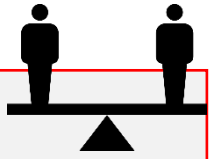
"Map" welke persoonsgegevens je in kaart brengt. Dit zijn de gegevens die je gebruikt en bijhoudt. Je moet kunnen toelichten van waar deze gegevens komen, hoe en met wie je deze gegevens deelt. Deze verwerkingen dienen tot slot geregistreerd en gedocumenteerd te worden. Hou hierbij rekening met de wettelijke kaders die hier van toepassing zijn. M.a.w. identificieer de wettelijke grondslag voor elke verwerking die je uitvoert.
Om dit praktisch te kunnen realiseren kan het aangewezen zijn hiervoor en info-audit te organiseren voor het gehele bedrijf of voor enkele afdelingen.

<u>Een praktisch voorbeeld waarom mapping belangrijk kan zijn:</u>
Wanneer "bedrijf A" onnauwkeurige gegevens doorgeeft aan "bedrijf B", dan moet "bedrijf B" hiervan op de hoogte gesteld worden dat er onnauwkeurige gegevens aanwezig zijn. Zo kan "bedrijf B" dit correct opnemen in hun registratie en documentatie.

3. Communiceren

Wanneer de eigen organisatie reeds persoonsgegevens verwerkt, dient men de betrokken partijen hiervan op de hoogte te stellen, zoals de identiteit van de verwerker en de wijze waarop deze de gegevens zal gebruiken. Gewoonlijk wordt dit in een privacyverklaring gegoten.
De evaluatie van uw bestaande privacyverklaring dient dus in eerste instantie te gebeuren. Op basis van deze analyse kan je dan de belangrijke aanpassingen doen indien nodig. Uiteraard zijn deze aanpassingen conform met de nieuwe regelgeving. Communiceer vervolgens deze 'nieuwe' privacy regelgeving met derden (bvb. via de website).

4. De rechten van de betrokkenen



Onderzoek of er bepaalde procedures zijn binnen de onderneming, waarop de betrokkenen zich kunnen beroepen. Denk na over en implementeer hoe bepaalde persoonsgegevens kunnen worden verwijderd en over hoe electronische gegevens kunnen worden medegedeeld. Dit is uiteraard ook van belang in de communicatie naar derden toe.
Anderzijds is de toestemming die men nodig heeft om gegevens te gebruiken belangrijk. Evalueer dus zeker de manier waarop men toestemming vraagt, verkrijgt en communiceer waarvoor men de gegevens kan gebruiken. Doe zeker de nodige aanpassingen waar nodig.

RECHTEN:

- **Recht op informatie en toegang tot zijn of haar persoonsgegevens**
- **Recht op correctie en uitwissing van eventuele foutieve gegevens**
- **Recht op bezwaar tegen direct marketingpraktijken**
- **Recht op bezwaar tegen geautomatiseerde besluitvorming en profilering**
- **Recht om vergeten te worden**
- **Recht op overdraagbaarheid van de gegevens**

5. Ik wens toegang tot...

Bij bepaalde diensten verzoeken mensen graag toegang te hebben tot bepaalde zaken. Deze verzoeken dienen misschien geüpdate te worden, conform met de nieuwe regelgeving. Denk zeker na hoe je de verzoeken zult verder behandelen in de toekomst. De bescherming van persoonlijke gebruikersnamen en wachtwoorden zijn hier een goed voorbeeld van.

6. Datalekken

Onderzoek of er geen defaults in de verwerkingssystemen zitten. Implementeer bepaalde procedures om dit te kunnen onderzoeken en te rapporteren.

7. Protect by Design & DPIA

Het is belangrijk om u vertrouwd te maken met deze 2 begrippen. Eens u het verschil duidelijk kan onderscheiden, ga dan zeker na hoe je deze concepten in de opperationele werking van het bedrijf kan implementeren.

- **Gegevensbescherming door ontwerp of data protection by design**
  Zoals reeds vermeld in het document, dient u ervoor te zorgen dat er gegevensbescherming-maatregelen worden ingebouwd in de producten en/of diensten vanaf de eerste ontwikkelingsfase of conceptfase.

- **Data Protection Impact Assessments of gegevensbeschermingseffectbeoordeling**
  Ook zoals reeds vermeld in dit document, een voorafgaande inschatting van de privacygevolgen is nodig. M.a.w. men moet dus kunnen aantonen dat er bij elke nieuwe actie die de onderneming uitvoert op gebied van het verzamelen, bewerken, en beheren van persoonsgegevens, men rekening heeft gehouden met de privacy van de betrokkene personen. De risico's op eventuele schendingen moeten in kaart gebracht worden en er moeten maatregelen getroffen zijn om de inbreuk op de privacy te beperken tot een minimum.

8. Internationale activiteit

Het is belangrijk om te bepalen onder welke toezichthoudende autoriteit de organisatie valt, indien de eigen onderneming ook internationaal actief is.

9. Bestaande contracten

Indien men met verwerkers en onderaannemers samenwerkt is het belangrijk om deze contracten te beoordelen, om zo noodzakelijke veranderingen aan te brengen indien nodig.

10 Functionaris voor gegevensbescherming

Stel een functionaris indien nodig aan. Men noemt deze persoon ook wel de DPO (Data Protection Officer). Deze persoon draagt de verantwoordelijkheid voor de naleving van de databeschermingsregels. Criteria waar men dient rekening mee te houden:

- **Deze persoon is 1 van de landstalen machtig**
- **Voor elke entiteit (=land) dient men dan iemand aan te duiden**
- **De functie en titel moeten duidelijk vermeld worden**

Bronvermelding

Deze white paper kwam tot stand dankzij volgende waardevolle bronnen, waarvoor dank:

- *Creditsafe - Data Business Teams & Marketing Teams*
- *De privacy-commissie - Commissie voor de bescherming van de persoonlijke levenssfeer – Algemene Verordening Gegevensbescherming - Drukpersstrat 35 | 1000 Brussels*
- *De privacy-commissie - Algemene Verordening Gegevensbescherming en publicaties (https://www.privacycommission.be/nl/algemene-verordening-gegevensbescherming-0)*
- *De privacy-commissie - Publicaties van de Werkgroep 29*
- *European Commission – Justice Rules of Law – Data Protection – Protection of personal data – GDPR (http://ec.europa.eu/justice/data-protection/)*
- *Varonis – GDPR: A practical guide – EU GDPR LESSONS – www.varonis.com*
- *STIMA | BDMA – Werkgroep GDPR | Legal Task Force - NEW DATA PROTECTION REGULATION – several workshops attended –*
- *STIMA | BDMA – Werkgroep GDPR | Legal Task Force - NEW DATA PROTECTION REGULATION – Position paper – (https://www.stima.be/nieuws/gdrp-positioning)*
- *GDPR PORTAL EU - The main elements of the General Data Protection Regulation (GDPR) - (http://www.eugdpr.org/)*
- *Smartbiz – artikel/post: De GDPR-wetgeving uitgelegd in vijf vragen – Karen Gijsbrechts (09/08/2016) - (http://www.smartbiz.be/achtergrond/167961/de-gdpr-wetgeving-uitgelegd-vijf-vragen/)*
- *Smartbiz – artikel/post: Checklist voor de GDPR: maak je bedrijf compliant in 13 stappen – Karen Gijsbrechts (26/09/2016) - (http://www.smartbiz.be/achtergrond/168496/checklist-voor-de-gdpr-maak-je-bedrijf-compliant-13-stappen/)*
- *The Economist – Article: Fuel of the future: Data is giving rise to a new economy*
- *LinkedIn – www.LinkedIn.com – Usefull insights and posts*

creditsafe

Creditsafe Belgium

Steenweg op Zellik 12

1082 Brussels

T: 02.481.88.60

E: info@creditsafe.be