Tekst : GDPR Page

## GDPR

Hebt u al gehoord van GDPR?

Weet u niet wat u ermee aan moet? Weet u dat dit bij wet verplicht is?

Wij komen naar u voor advies op maat i.v.m. het register van verwerkingsactiviteiten, de risicoanalyse, IT-beveiliging, opstellen van verplichte documenten, aanpassen van de website, maatregelen rond datalekken. Eggcore helpt u van a to z met de afhandeling van uw dossier

## Wat zijn uw GDPR-verplichtingen?

### Bewustwording in uw bedrijf

De eerste stap in het proces van ‘GDPR-compliance’ is de bewustmaking in uw bedrijf. Het is belangrijk dat uw medewerkers en klanten op de hoogte zijn van de GDPR-regels. Het is raadzaam om sleutelfiguren aan te duiden die weten wat GDPR inhoudt. Zij zullen immers moeten aanduiden op welke vlakken het bedrijf moet ingrijpen om GDPR-compliant te worden.

### Uw dataregister

Vanaf 25 mei 2018 gelden nieuwe privacyregels voor uw organisatie. U zal vanaf dan alle persoonsgegevens, wat u ermee doet en met wie u ze deelt, moeten bijhouden. Dit heet documentatieplicht. Deze documentatieplicht helpt u om de GDPR-wetgeving na te leven en om te bewijzen dat u verantwoord omgaat met de data die u verzamelt.

Bent u nu wat ongerust? Weet u niet hoe u zich een weg moeten banen doorheen uw gegevens? Loopt u misschien wat verloren in alle opgelegde regeltjes?

Geen paniek, de True GDPR-app zorgt ervoor dat u op uw twee oren kan slapen. U geeft op een efficiënte en eenvoudige manier uw datagegevens in en de app doet de rest!

Geen zorgen om uw databeleid! De app evolueert voortdurend en is up-to-date is met de recentste wetgeving en privacy statements.

Weg met uw papieren administratie! Uw dataregister bevindt zich op een digitale bewaarplaats waardoor u op eender welk moment, zeer snel, uw dataregister kan opvragen, bewerken… Uw documenten worden bewaard zo lang als wettelijk nodig is.

Maximale beveiliging en monitoring van uw documentenbeheer.

Wij vertegenwoordigen uw bedrijf! Bent u helemaal niet thuis in wetgeving, processen en andere moeilijke woorden? Geen probleem… Als uw Data Protection Officer (DPO) houden wij een oogje in het zeil en vertegenwoordigen uw bedrijf wanneer er, door de gegevensbeschermingsautoriteit, toch onnauwkeurigheden zouden worden vastgesteld.

### Communicatie

U hebt ongetwijfeld al een privacyverklaring. Maar is deze wel up-to-date en reeds aangepast aan de nieuwe GDPR-wetgeving? Geen idee? Wij helpen u graag met de evaluatie van je bestaande privacyverklaring.

Welke informatie moet er in uw beknopte, begrijpbare en duidelijke privacyverklaring, vanaf 25 mei 2018, zeker extra opgenomen zijn?

Wat zegt de wet voor gegevensverwerking? Hoelang zal je informatie bijhouden? Met wie wissel je gegevens uit buiten de Europese Unie?

De mededeling dat de betrokkene klacht kan indienen bij de Gegevensbeschermingsautoriteit als deze denkt dat zijn persoonsgegevens foutief worden verwerkt.

### Rechten van de betrokkene + wettelijke grondslag voor verwerken van persoonsgegevens

Hebt u al eens nagedacht over de manier waarop u mensen informeert over hun privacy rechten? Staat er in uw privacyverklaring duidelijk vermeld welke rechten de betrokkene heeft, hoe hij zijn persoonsgegevens kan verwijderen of hoe zijn gegevens elektronisch worden gedeeld?

In de nieuwe maatregelen van de GDPR staat duidelijk vermeld dat elke betrokkene:

* zijn persoonsgegevens kan inkijken;
* kan eisen om zijn gegevens aan te passen, om de verwerking ervan te beperken (vb: uitschrijven nieuwsbrief, mails);
* het recht heeft om ‘vergeten’ te worden (gegevens wissen);
* direct marketingpraktijken kan weigeren;
* gegevens kan overdragen naar andere bedrijven;
* elke vorm van geautomatiseerde besluitvorming en profilering kan weigeren.

Samen bekijken we of de procedures in uw bedrijf reeds voldoende aangepast zijn aan deze individuele rechten. Op deze manier verloopt de overgang naar GDPR relatief vlot.

We stellen ons vragen als: “Wie neemt beslissingen?”, “Zijn onze systemen voor GDPR uitgerust?” Wij evalueren al uw procedures en geven advies over eventuele noodzakelijke veranderingen.

### Verzoek tot toegang

Wist u, dat door de GPDR-maatregelen

… de termijn voor de verwerking van ‘toegangsverzoeken’ gelimiteerd wordt tot 30 dagen?

… het noodzakelijk is dat u een update doet van uw bestaande toegangsprocedures?

… u ook eens goed moet nadenken over hoe u toegangsverzoeken voortaan zal behandelen?

Elke betrokkene heeft het recht om zijn persoonsgegevens in te kijken. Dat is nu ook al het geval, maar door de GDPR zal u nu veel sneller moeten reageren. Vanaf 25 mei 2018 moet het verzoek tot toegang gratis en binnen de 30 dagen worden verwerkt.

Het is van belang dat u de betrokkene bepaalde informatie geeft:

* Hoelang zal u informatie bijhouden?
* Binnen welke termijn kan de betrokkene informatie laten verbeteren?

U merkt het al… als uw bedrijf een groot aantal toegangsverzoeken behandelt, zal de GDPR een grote impact hebben op uw bedrijf. Wij kunnen u helpen en ondersteunen bij de logistieke aanpassingen die nodig zijn om alles binnen de voorziene termijn te verwerken en de betrokkene van de noodzakelijke informatie te voorzien.

Wil je toch toegangsverzoeken kunnen weigeren? Dan zal u zeker uw beleid en de procedures moeten aanpassen.

Op termijn zal ons toegangssysteem u helpen om kostenbesparend te zijn omdat het de betrokkene in staat stelt om zijn gegevens online te raadplegen.

### Toestemming

Het is belangrijk dat u controleert op welke manier u toestemming vraagt om gegevens te bekijken en hoe je die toestemming bewaart. U moet namelijk op elk moment kunnen bewijzen dat de betrokkene expliciet en actief toestemming heeft gegeven om gegevens te bewaren.

Wat wil dit concreet zeggen? Je moet met de volgende voorwaarden rekening houden.

1. De toestemming moet vrij, specifiek, geïnformeerd en ondubbelzinnig zijn.
2. De toestemming moet controleerbaar zijn.
3. De toestemming moet begrijpbaar zijn, zodat ook minderjarigen hem begrijpen.
4. De betrokkene

* Moet expliciet toestemming geven.
* Moet actief toestemming geven d.w.z. dat de toestemming van de betrokkene niet afgeleid kan worden uit een stilzwijgen, een vooraf aangevinkt vakje of uit een niet-handelen.
* Heeft meer rechten wanneer je vertrouwt op toestemming als grondslag voor de gegevensverwerking.
* Als je erop rekent dat de betrokkene zeker zijn toestemming geeft om zijn gegevens te verwerken, zorg er dan voor dat je in orde bent met de GDPR-wetgeving. Ben je er niet zeker van dat je al in orde bent, aarzel dan niet om je toegangsprocedure te wijzigen of een alternatief te zoeken voor toestemming als grondslag voor de gegevensverwerking.

Wanneer je gegevens verzamelt van betrokkenen jonger dan 16 jaar, dan moet je de toestemmingen hebben van een ouder of voogd.

### Datalekken

Dankzij de GDPR hebt u een verplichte meldplicht wanneer u een datalek ontdekt waarbij persoonsgegevens (bv. bankgegevens, medische gegevens) gevaar lopen. Het is dus van groot belang dat u procedures ontwikkelt om datalekken zo snel mogelijk op te sporten, te onderzoeken en te melden.

U zal niet elk datalek moeten melden bij de Gegevensbeschermingsautoriteit. Enkel de datalekken waarbij het waarschijnlijk is dat de betrokkene schade zal leiden, zal u moeten melden. Bij niet-naleving van deze meldplicht hangt u een geldboete boven het hoofd, boven op de boete voor het datalek zelf.

### Gegevensbescherming door ontwerp en gegevensbeschermingsbeoordeling

Hier staan 2 begrippen centraal:

Privacy by design of gegevensbescherming door ontwerp  
= Elk proces dat u begint moet van in het begin gericht zijn op privacy!

Privacy Impact Assessment (PIA) of gegevensbeschermingsbeoordeling  
= Een PIA analyseert de impact van een nieuw proces of systeem.  
= Wanneer de PIA aangeeft dat de gegevensverwerking een hoog risico inhoudt, is het wettelijk verplicht om advies in te winnen bij de Gegevensbeschermingsautoriteit in kader van de GDPR.

Weet u hoe u deze concepten kan implementeren in uw bedrijf? Kan u deze begrippen linken aan andere organisatorische processen zoals risicobeheer en projectbeheer? Het is dus belangrijk dat u nu al bekijkt in welke situaties het nodig zal zijn om deze analyses uit te voeren.

Daarnaast start u ook al best met een goede strategie: wie zal de analyse uitvoeren? Wanneer? Hoe kunnen we bestaande systemen en processen verbeteren door ‘privacy by design’?

Het is een voorbeeld van good practices van een bedrijf om gegevensbescherming van bij de start in te bouwen en daarna een effectbeoordeling uit te voeren in hoge risicosituaties (bv. bij de implementatie van nieuwe technologie).

Maar wat als niet de hoofdzetel, maar één van de internationale afdelingen beslist over de gegevensverwerking van het bedrijf? Dan valt het je bedrijf onder de autoriteit in dat specifieke land.

Om te weten te komen welke autoriteit de leiding heeft over jouw bedrijf is het interessant om in kaart te brengen waar je bedrijf haar meest belangrijke beslissingen omtrent gegevensverwerking neemt. Dit zal je helpen bij het bepalen van jouw hoofdvestiging en dus ook de bevoegde toezichthoudende autoriteit.

### Internationaal

Ben je internationaal actief? Verzamel je persoonsgegevens van mensen in het buitenland? Dan moet je weten onder welke toezichthoudende autoriteit je valt, wanneer er zich een klacht met internationaal karakter zou voordoen. Meestal wordt er daarvoor gekeken naar vestigingsplaats van de hoofdzetel.

Voorbeeld: Een bedrijf met een Belgische hoofdzetel en met afdelingen in Frankrijk, valt nog steeds onder de Belgische Gegevensbeschermingsautoriteit.

Maar wat als niet de hoofdzetel, maar één van de internationale afdelingen beslist over de gegevensverwerking van het bedrijf? Dan valt het je bedrijf onder de autoriteit in dat specifieke land.

Om te weten te komen welke autoriteit de leiding heeft over jouw bedrijf is het interessant om in kaart te brengen waar je bedrijf haar meest belangrijke beslissingen omtrent gegevensverwerking neemt. Dit zal je helpen bij het bepalen van jouw hoofdvestiging en dus ook de bevoegde toezichthoudende autoriteit.

### Bestaande Contracten

De GDPR is ook van toepassing op eventuele diensten waar je bedrijf gebruik van maakt. Gebruik je bijvoorbeeld een dataverwerker (een bedrijf dat persoonsgegevens verwerkt zodat jij ze kan gebruiken) of cloudprovider dan is die ook verantwoordelijk voor de privacy van de gegevens. Alle betrokken partijen moeten de GDPR naleven. Als jij hun diensten gebruikt, ben jij verantwoordelijk om te controleren of die diensten GDPR-compliant zijn.

Het is dus noodzakelijk om de bestaande contracten te controleren en indien nodig aan te passen.

### Wettelijke grondslag voor het verwerken van persoonsgegevens

In tegenstelling tot de huidige wet, is het volgens de GDPR noodzakelijk om een wettelijke basis te bepalen voor de gegevensverwerking. Die basis bepaalt immers ook welke rechten de gebruiker heeft omtrent zijn gegevens. Die wettelijke grondslag moet neergeschreven worden in de privacyverklaring.