



## **Bent u klaar voor de GDPR?**

Vraag en antwoord webinar  
22 november 2017

### **Hoe kwalificeer je gespreksverslagen van een vertrouwenspersoon?**

Gespreksverslagen zullen informatie bevatten waaruit een natuurlijk persoon kan worden geïdentificeerd. Dit zal als persoonlijke data worden gekwalificeerd. Afhankelijk van de inhoud en gedetailleerdheid van het verslag kunnen het ook bijzondere persoonsgegevens zijn (bv. politieke overtuiging, seksuele geaardheid, etc.).

Zowel in het licht van de privacywetgeving als uit confidentialiteitsoverwegingen van de vertrouwenspersoon dienen gespreksverslagen met de nodige voorzichtigheid en conform de GDPR-regels te worden behandeld.

#### **Rechtsgrond:**

Art. 4 GDPR: definitie persoonsgegevens.

Art. 9 GDPR: definitie gevoelige persoonsgegevens.

### **In kader van offertes en de wet op de overheidsopdrachten sturen wij referentielijsten mee op vraag van de prospect. Moet dit goedgekeurd worden door de referentie in kwestie?**

Dit is afhankelijk van de inhoud van de referentielijst. Staan er op deze lijst louter bedrijfsgegevens dan zal dit niet worden gezien als een persoonsgegeven. Eenmaal er natuurlijke personen (bv. een contactpersoon) bij naam worden vernoemd, zullen deze als persoonlijke data worden beschouwd en zal er goedkeuring dienen te zijn bij doorgifte.

#### **Rechtsgrond:**

Art. 4 GDPR: definitie persoonsgegevens, data subject.

### **Is er ergens een lijst beschikbaar van de persoonsgegevens en vertrouwelijke gegevens? Wat wel, wat niet?**

Neen, zowel voor de persoonsgegevens als de vertrouwelijke gegevens (= 'bijzondere persoonsgegevens' in de GDPR) is er enkel een definitie opgenomen. Een onderneming dient de verzamelde gegevens zelf te toetsen aan deze definities.

#### **Rechtsgrond:**

Art. 4 GDPR: definitie persoonsgegevens.

Art. 9 GDPR: definitie bijzondere persoonsgegevens.

### **Wij zijn een productiebedrijf van 150 mensen (puur B2B). Moeten wij een DPO aanstellen? Wat zijn de voorwaarden voor een kmo om een DPO aan te stellen?**

Een DPO dient enkel door een onderneming te worden aangesteld indien er bijvoorbeeld op grootschalige wijze gevoelige persoonsgegevens worden verwerkt (= persoonlijke data met betrekking tot ras, politieke voorkeur, etc.). De andere gevallen zijn minder voorkomend en minder relevant voor een kmo.

De definitie van de GDPR verduidelijkt niet welke bedrijven op een 'grootschalige' manier gegevens verwerken. Het aanstellen van de DPO is dus niet steeds noodzakelijk, maar in het kader van de rechtszekerheid toch een aanbeveling voor iedere kmo.

#### **Rechtsgrond:**

Art. 37, lid 1 GDPR: bespreking van alle gevallen waarin een DPO dient te worden aangesteld.

Art. 9 GDPR: een bespreking van bijzondere persoonsgegevens.

### **Wie moet een DPO aanstellen? Een controller of een processor? Of beide?**

De hoedanigheid van controller of processor is irrelevant met betrekking tot de aanstelling van een DPO. Een DPO dient te worden aangesteld als er bijvoorbeeld in het bedrijf op grootschalige wijze gevoelige persoonsgegevens worden verwerkt (zie vorige vraag). Iedere onderneming dient een afweging te maken zowel in hoofd van controller als in hoofd van processor.

Bv. Indien een ziekenhuis (controller) opdracht geeft aan een serverbeheerder (processor) om uitsluitend patiëntengegevens op te slaan en te verwerken, zullen beide ondernemingen een DPO dienen aan te stellen.

#### **Rechtsgrond:**

Art. 37 GDPR: bespreking DPO.

### **Dient er voor een leverancier van cloudoplossingen zoals OneDrive van Microsoft een verwerkersovereenkomst opgesteld te worden?**

Niet noodzakelijk. Internationale bedrijven kennen de nieuwe privacy verordening reeds en hebben hun privacyregeling daar al op afgestemd. Controleer wel steeds wat er in hun privacyregeling staat. Iedere onderneming kan bepaalde voorwaarden stellen om deze privacy compliance te garanderen.

Bv. Voorwaarden Microsoft Office 365: data dient in de cloud te zitten en geclassificeerd te zijn a.d.h.v. labels.

### **Wij zijn als bedrijf niet verplicht om een DPO te hebben. Moeten we dan iemand aanduiden als contactpunt voor vb. de Privacycommissie?**

Uiteraard is het aan te raden een duidelijke contactpersoon te hebben. Dit is volgens de GDPR echter niet verplicht.

### **Wat is de toekomst van een telefoongids met persoonsgegevens?**

Ze zullen blijven bestaan maar niet meer in hun huidige vorm. Alle vormen van persoonlijke data dienen een gelimiteerde bewaartermijn te hebben. Daardoor moet een telefoongids worden geëvalueerd in het kader van noodzakelijkheid, proportionaliteit, etc. In tegenstelling tot vandaag, is het de bedoeling dat een klantenlijst/telefoongids beantwoordt aan de realiteit en dat de klant toestemming heeft gegeven om in de lijst te staan. Op regelmatige basis data opnieuw evalueren en verwijderen is een must.

### **Alle persoonlijke data kunnen of mogen voor marketing doeleinden verkocht worden. Kan dit nog binnenkort?**

Ja en nee, de nieuwe regeling laat nog steeds de mogelijkheid om persoonlijke data door te geven of te verkopen voor marketing doeleinden. Deze nieuwe regeling is echter heel wat strikter. Ondernemingen mogen lijsten aankopen of verkopen, maar enkel indien de natuurlijke persoon op de lijst is geïnformeerd, heeft toegestemd (schriftelijk) en de koper/verkoper de persoonlijke data privacy conform zal behandelen of heeft verkregen.

### **Welke clause i.v.m. privacy kan er worden opgenomen in de algemene voorwaarden op de achterzijde van de bestelbon? Quid raadpleegbaarheid van de privacy policy in de winkel bij ondertekening van de bestelbon?**

Een verwijzing naar de privacy declaration (normaal gezien naar de website of plaats van publicatie) en een vermelding dat de bestelbon ondertekenen een impliciete aanvaarding uitmaakt van deze declaration.

### **Moeten alle bestaande klanten opnieuw aangeschreven worden om hun uitdrukkelijke toestemming te bekomen om nog nieuwsbrieven, info, ... te ontvangen?**

Dit is afhankelijk van de inhoud van de nieuwsbrief. Indien het gaat om informatie zonder marketingdoeleinden, dan dient de klant enkel de mogelijkheid te hebben om zich naar de toekomst toe uit te schrijven (opt-out). Indien de klanten worden aangeschreven vanuit een commercieel oogpunt (met het doel iets te verkopen), dan dient er voorafgaande toestemming te zijn, behalve als het gaat om reclame voor producten gelijkaardig aan diegene die de klant in het verleden reeds heeft aangekocht.

### **Definieer een bestaande klant: stel dat ik drie jaar terug iets verkocht heb aan die klant, om daarna drie jaar geen contact meer te hebben gehad, mag ik die klant dan nog steeds als "klant" beschouwen?**

#### **Hoe lang mag een rekruteringskantoor de gegevens van haar kandidaten bijhouden?**

Bij deze vragen is de sector en de motivatie ontzettend belangrijk. Indien een bakker drie jaar geen brood meer heeft verkocht aan een persoon, dan kan deze niet langer worden gezien als een klant. Daarentegen, als het gaat om een autodealer, dan kan deze mogelijks wel nog als klant gelden. Bij kandidaten kan eenzelfde afweging worden gemaakt.

Twee gemakkelijke vuistregels:

- Motiveer waarom je bepaalde termijnen hebt gekozen (ook bv. voor het bijhouden van hun gegevens, het versturen van direct marketing, etc.)
- Wees consistent in het gebruik van de termijnen.

### **Quid als bedrijf in zijn geheel verkocht wordt?**

Normaal gezien gaan alle privacy gerelateerde vereisten over op de koper, die in de plaats komt van de verkoper, en wordt deze aanzien als initiële controller of processor. Dit kan anders worden bedongen in de overnameovereenkomst indien nodig.

### **Valt het sturen van een kerstkaartje per email naar alle contacten van het bedrijf onder GDPR?**

In principe wel. De ontvanger zou de mogelijkheid moeten hebben om zich te verzetten tegen het verkrijgen van kerstkaarten in de toekomst (opt-out).

### **Vraagje over tweede pol (omtrent het verkopen van persoonlijke data): Indien ze op de hoogte zijn, en geen tegenwoord bieden, zijn ze in se dan niet impliciet akkoord?**

In principe niet. De verwerker moet de specifieke toestemming met betrekking tot het verkopen van data kunnen bewijzen.

#### **Rechtsgrond:**

Art. 7 GDPR: omtrent de voorwaarden voor de toestemming.

### **Wat met direct marketing naar prospecten d.m.v. emailadressen die via LinkedIn of internet gevonden werden? Dus zonder toestemming van betrokkene.**

Direct marketing is niet toegelaten naar een betrokkene die zijn toestemming niet heeft gegeven. Het openbaar maken van een e-mailadres op LinkedIn is geen toestemming om de betrokkene direct marketing te sturen.

#### **Rechtsgrond:**

Art. 7 GDPR: omtrent de voorwaarden voor de toestemming.

### **Kan een klant zelf bepalen hoe lang zijn gegevens mogen bijgehouden worden?**

Indirect wel. De klant heeft namelijk steeds de mogelijkheid om het 'right to be forgotten' aan te vragen. Daardoor is de onderneming verplicht al de persoonlijke data van de betrokkene te verwijderen. Indien de klant dit recht niet aanvraagt, blijft hij wel onderhevig aan het beleid omtrent de bewaartermijnen dat door de onderneming is opgesteld.

#### **Rechtsgrond:**

Art 17 GDPR: omtrent het recht op gegevenswissing.

**In het CRM-systeem staan 'tags' op klantnamen die bepalend kunnen zijn in marketingcampagnes dit is geen persoonlijke data maar moet de klant/prospect weten dat ik deze data heb?**

Over alle persoonlijke data die een onderneming heeft, moet ze transparant zijn. De onderneming moet deze data proportioneel hebben verzameld en de toestemming hebben verkregen van de betrokkene. Welke data er is, hoe die werd verzameld, etc. dient dan ook te worden opgenomen in de privacy statement (of in een contract). Het concrete antwoord hangt af van de inhoud van de tags. Klanten onderverdelen op basis van financiële situatie, persoonlijke interesses, beroepsprestaties, locatie, etc. kunnen wel degelijk persoonlijke data uitmaken.

**Een camera aan de parking van het gebouw om eerder als inbraakwerend te werken - valt die daar dan ook onder?**

Ja, dergelijke camera valt ook onder deze regelgeving. De camera in kwestie zal vermoedelijk zowel klanten als personeel kunnen filmen op de parking van de arbeidsplaats/het gebouw. Zowel de Camerawet als de CAO nr. 68 moeten dan gelijktijdig worden toegepast.

**Moeten we het hangen van een camera op de werkvloer melden aan de Privacycommissie?**

Ja, een camera op de werkvloer moet steeds gemeld worden aan de Privacycommissie.

**Mag een werknemer een foto die staat op intranet van een bedrijfsfeest op zijn Facebookpagina posten?**

Ja, mits toestemming van de betrokken personen en de werkgever. Dit legt u best vast in een social media policy/arbeidsreglement. Uiteraard kunnen wij u hierin steeds bijstaan.

**Op intranet staat te lezen wie er in het gebouw is (via de badge geregistreerd). Valt dit onder rechtmatig doel?**

Dit zal afhankelijk zijn om welke redenen deze gegevens weergegeven en geregistreerd worden en welke info hierdoor toegankelijk is. Het is steeds van belang dat de finaliteit en het rechtmatige doel gerespecteerd worden, alsook de proportionaliteit. Als dit kan bereikt worden door minder data te delen, moet hiervoor geopteerd worden. Belangrijke bijkomende vraag hierbij is: wie kan dit allemaal zien? Aarzel zeker niet ons te contacteren om dit nader te onderzoeken.

**Mag een (volledige) mailbox van een ontslagen/zieke collega overgedragen worden aan een andere collega?**

Automatisch forwarden van e-mails wordt nooit toegestaan door de Privacycommissie. Toegang verschaffen tot de mailbox van een ontslagen/zieke werknemer kan slechts onder heel beperkte voorwaarden die dienen uitgestippeld te worden in een beleid hieromtrent. Dit kan worden opgenomen in een aparte policy dan wel in het arbeidsreglement, uiteraard steeds rekening houdend met de beginselen inzake transparantie, finaliteit en proportionaliteit. Uiteraard kunnen wij u hierin steeds bijstaan.

**Moet van de werknemers een uitdrukkelijk (schriftelijk) akkoord worden bekomen met (elke wijziging van) het arbeidsreglement?**

Als een arbeidsreglement in de onderneming wordt ingevoerd of het bestaande arbeidsreglement wordt gewijzigd, dient in principe een door de wet bepaalde procedure te worden gevolgd. Slechts in een aantal uitzonderlijke gevallen, die worden beschreven in artikel 14 van de Arbeidsreglementenwet is de procedure niet van toepassing. Dit betreffen de algemene regels zoals vastgelegd in de Wet tot instelling van de arbeidsreglementen. De privacywetgeving verandert of verstrengt dit niet. Indien u bepaalde wijzigingen wenst door te voeren in het kader van de GDPR, aarzel dan zeker niet ons hiervoor te contacteren.

**Wat als iemand ziek is en men foto's ziet op Facebook dat hij aan het voetballen is of op reis is? Kan hij hiervoor gesanctioneerd worden?**

In de rechtspraak wordt ook aangenomen dat Facebook-berichten kunnen worden gebruikt om een ontslag om dringende reden te staven. Er kan natuurlijk ook geopteerd worden voor minder ingrijpende sancties en de context is alles bepalend. We verwijzen hiervoor naar de slides 41 t.e.m. 46 van de presentatie.

In de mate u een concreet geval heeft, helpen wij u graag bij de inschatting van de sancties en de opbouw van uw dossier.

### Mag men brandstofverbruik van de bedrijfswagen controleren?

Indien u het brandstofgebruik wenst te controleren, neemt u dit best op in een schriftelijk document zoals een bijlage bij de arbeidsovereenkomst, het arbeidsreglement of een bedrijfs(car)policy. Het opstellen van schriftelijke procedures en richtlijnen binnen de onderneming is belangrijk. Niet alleen omdat transparantie in het algemeen belangrijk is, maar vooral omdat bij latere betwistingen er zal kunnen aangetoond worden dat de werknemer wist wat het beleid van de werkgever was. Daarnaast hebben schriftelijke documenten ook hun belang omdat beperkingen op de privacy erin vervat moeten zijn. Uiteraard kunnen wij u hierin bijstaan.

## Disclaimer

De antwoorden zijn enkel gebaseerd op de beperkte omschrijving en zijn in geen geval zonder verdere uitwerking in de praktijk toepasbaar. Consulteer onderstaande contactpersonen met vragen omtrent de implementatie van de nieuwe privacywetgeving in de praktijk.

Contacteer ons:



#### Anaïs De Boulle

##### GDPR specialist

Business en commercieel recht  
adeboulle@deloitte.com  
0476 66 12 53



#### Flore Lesage

##### GDPR specialist

Arbeidsrecht en sociale zekerheidsrecht  
flesage@deloitte.com  
0498 40 80 45

# Deloitte.

## Private

Accountancy & Advisory

ACCOUNTING & REPORTING TAX & LEGAL M&A & FINANCE  
BUSINESS CONTROL & TECHNOLOGY STRATEGY & GROWTH

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see [www.deloitte.com/about](http://www.deloitte.com/about) for a more detailed description of DTTL and its member firms.

© 2017 Deloitte Accountancy.  
Designed and produced by the Creative Studio at Deloitte, Belgium