Hoofdstuk 1.

# Inleiding

## 1.1. Algemene Verordening Gegevensbescherming van 27 april 2016

Na jarenlange onderhandelingen werd op 27 april 2016 de Algemene Verordening Gegevensbescherming ofwel General Data Protection Regulation (hierna 'GDPR') goedgekeurd.[1] De GDPR is sinds 25 mei 2018 van toepassing op elke verwerking van persoonsgegevens en vervangt hierbij de Europese Richtlijn van 1995.[2] In België vervangt de GDPR de Privacywet van 8 december 1992.[3] Deze wet werd meermaals aangepast, onder andere naar aanleiding van de omzetting naar de Europese Privacyrichtlijn van 1995.

De hervorming van de privacywet was noodzakelijk geworden door de sterke digitalisering en verhoogde verwerking van persoonsgegevens, zowel bij overheden als bij ondernemingen. De Europese wetgever was dan ook van oordeel dat een hogere bescherming van deze persoonsgegevens noodzakelijk was en dat hiertoe een nieuw en strenger kader moest worden aangenomen.

De GDPR is rechtsreeks van toepassing in de hele Europese Economische Ruimte (EER).[4] De GDPR wordt in de publieke opinie veelal als

1 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 de Richtlijn 95/46/EG, *Pb.*L. 119, 4 mei 2016, 1-88, hierna de 'GDPR' genoemd.

2 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb.*L. 281, 23 november 1995, 31-50.

3 Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, *BS* 18 maart 1993.

4 Europese Economische Ruimte (EER) bestaat uit de EU-lidstaten Noorwegen, Liechtenstein en IJsland.

een pestmaatregel gezien die enkel bedoeld is om populaire privacyschenders als Google en Facebook in bedwang te houden. Deze perceptie is echter niet terecht. De GDPR is onder meer van toepassing op iedere verwerking van persoonsgegevens in een professioneel kader.[5]

De hoofddoelstellingen van de GDPR zijn tweevoudig.

- Enerzijds wil de GDPR ondernemingen, verenigingen en overheden op een meer bewuste en veilige manier laten omgaan met persoonsgegevens.

  Door de doorgedreven digitalisering van onze maatschappij in het laatste decennium zijn ondernemingen, waaronder ook de accountantskantoren, veel meer digitaal gaan werken. Terwijl de dossiers vroeger in het accountantskantoor veilig achter slot en grendel zaten, worden gegevens en documenten vandaag hoofdzakelijk digitaal bijgehouden. De communicatie gebeurt grotendeels per e-mail en vertrouwelijke documenten worden steeds meer digitaal bij de cliënt opgevraagd en op een cloud bewaard.

  Bij die digitalisering van een kantoor wordt niet altijd stilgestaan bij de risico's die de verwerking en connectiviteit met zich meebrengen. Toestellen worden steeds mobieler en verhogen de interactie. De mogelijkheden om persoonsgegevens te gebruiken en te delen zijn veelvuldig. Het doel van de GDPR bestaat er dan ook in om die ondernemingen alsnog te laten stilstaan bij de manier waarop persoonsgegevens verwerkt en beveiligd worden.

- Anderzijds wil de GDPR ook de personen van wie de persoonsgegevens verwerkt worden, meer controle geven over hun eigen persoonsgegevens. De aangescherpte informatieplicht moet betrokkenen een beter zicht geven over welke persoonsgegevens van hen verwerkt worden en op welke manier dit gebeurt. Daarenboven krijgen de betrokkenen bijkomende rechten om controle uit te voeren met betrekking tot hun persoonsgegevens. Zij kunnen een recht op inzage, correctie, dataportabiliteit en wissen van gegevens uitoefenen. Indien de betrokkene een klacht indient, gaat de Gegevensbeschermingsautoriteit thans stipt na of een onderneming tijdig en voldoende tegemoetkomt aan deze vragen en wordt er bij een inbreuk een boete uitgeschreven.

5. In artikel 2 GDPR wordt het toepassingsgebied van de GDPR bepaald. De GDPR is van toepassing op zowat iedere verwerking van persoonsgegevens van zowel ondernemingen, overheden als verenigingen.

Voor accountants is de GDPR een noodzakelijke aanvulling op de deontologie en in het bijzonder het beroepsgeheim. Ervaring leert dat veel accountants nog te weinig stilstaan bij de manier waarop ze omgaan met persoonsgegevens. Zo is het versturen van onbeveiligde e-mails en bijlagen met gevoelige gegevens nog steeds een gangbare praktijk.

Daarnaast houdt de digitale bewaring van persoonlijke informatie van cliënten meer risico's in dan het bewaren van papieren dossiers. Gegevens die in handen komen van de verkeerde personen kunnen erg snel verspreid worden naar een groot publiek toe, onder meer via sociale media. Zodra een document op het internet gepubliceerd is, is het heel moeilijk om deze informatie opnieuw te wissen. Dit verhoogt het risico op schade voor de cliënt en voor het kantoor.

Cliënten vertrouwen er echter op dat een accountant vertrouwelijk omgaat met hun persoonsgegevens. De digitalisering heeft deze taak voor de accountant veel zwaarder gemaakt. Het risico en de kans op datalekken is dan ook veel groter geworden.

Het aantal cyberaanvallen in België stijgt jaarlijks met een veelvoud.[6] Hackers gaan naast persoonsgegevens zoals login- of betalingsgegevens ook steeds meer op zoek naar vertrouwelijke data van ondernemingen. Plannen van nieuwe producten, overeenkomsten met een leverancier of de loongegevens van een goede medewerker kunnen erg waardevolle informatie zijn in handen van een concurrent van een onderneming. Daar grote ondernemingen doorgaans een hoger veiligheidsniveau hanteren en hier hoge budgetten tegenaan gooien, gaan hackers zich steeds meer richten op dienstverleners van deze ondernemingen, zoals accountants- en advocatenkantoren, om de gewilde informatie te verkrijgen en te koop aan te bieden.[7]

## 1.2. De Belgische uitvoeringswetten

De Belgische wetgever heeft naar aanleiding van de GDPR enkele uitvoeringswetten aangenomen.

6. De Tijd, 'Recordaantal cybercriminelen vallen Belgen aan', 27 december 2019, https://www.tijd.be/politiek-economie/belgie/federaal/recordaantal-cybercriminelen-vallen-belgen-aan/10194310.

7. K. Van De Wetering, *Digitale bedrijfsspionage: je bedrijf is interessanter dan je denkt*, 2 juni 2018, https://www.mt.nl/business/digitale-bedrijfsspionage-je-bedrijf-is-interessanter-dan-je-denkt/554831.

- De wet van 3 december 2017[8] heeft het kader vastgesteld waarbinnen de nieuwe Gegevensbeschermingsautoriteit (GBA) wordt opgericht als toezichthoudende autoriteit voor de verwerking van persoonsgegevens overeenkomstig de GDPR. De GBA krijgt hierdoor zowel een controle- als een sanctiebevoegdheid en vervangt de Privacycommissie, die hoofdzakelijk een adviesorgaan was.[9]
- De wet van 30 juli 2018 betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens[10] is hoofdzakelijk een aanvulling op de GDPR. Zo bevat zij bijzondere bepalingen omtrent de verwerking van strafrechtelijke, genetische, biometrische en gezondheidsgegevens, evenals de verwerking van persoonsgegevens door overheden. Tevens bevat zij enkele afwijkingen op de GDPR, met name voor België wordt de leeftijd waarop een minderjarige geldige toestemming kan geven in het kader van diensten van de informatiemaatschappij, verlaagd van zestien naar dertien jaar.
- De wet van 5 september 2018[11] brengt enkele wijzigingen aan in diverse andere wetten, waaronder de wet van 13 december 2006 betreffende gezondheid[12] of de wet van 15 januari 1990 betreffende de oprichting en organisatie van de Kruispuntbank van de Sociale Zekerheid[13].

## 1.3. ‘Overige’ privacywetgeving

De GDPR is niet de enige privacywetgeving die van toepassing is op de verwerking van persoonsgegevens. In tal van wetten zijn specifieke bepalingen opgenomen waarmee rekening moet worden gehouden. Zonder

8. Wet tot oprichting van de Gegevensbeschermingsautoriteit van 3 december 2017, *BS* 10 januari 2018.
9. Zie Hoofdstuk 11 voor meer details omtrent de bevoegdheden van de GBA.
10. Wet betreffende de bescherming van natuurlijke personen met betrekking tot de verwerking van persoonsgegevens van 30 juli 2018, *BS* 5 september 2018.
11. Wet tot oprichting van het informatieveiligheidscomité en tot wijziging van diverse wetten betreffende de uitvoering van verordening (EU) 2016/679 van 27 april 2016 van het Europees Parlement en de Raad 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 van 5 september 2018, *BS* 10 september 2018.
12. Wet van 13 december 2006 betreffende de gezondheid, *BS* 22 december 2006.
13. Wet van 15 januari 1990 betreffende de oprichting en organisatie van de Kruispuntbank van de Sociale Zekerheid, *BS* 22 februari 1990.

limitatief te zijn worden hierna enkele relevante wetten en bepalingen voor accountantskantoren opgenomen.[14]

- Het recht op eerbiediging van het privéleven is opgenomen als een grondrecht in artikel 8 van het Europees Verdrag van de Rechten van de Mens[15] (EVRM) en in artikel 7 van het Handvest van de Grondrechten van de Europese Unie (EU-Handvest)[16]. Het recht op bescherming van persoonsgegevens is opgenomen in artikel 8 van het EU-Handvest.
- De Europese e-Privacyrichtlijn[17] bepaalt de regels rond cookies en e-mailmarketing en werd in Belgische wetgeving omgezet in de Wet Elektronische Communicatie[18] en in het Wetboek van economisch recht[19].
- Het was de bedoeling van de Europese Commissie om samen met de GDPR een nieuwe e-Privacyverordening te laten in werking treden op 25 mei 2018. Een akkoord over een definitieve tekst laat echter op zich wachten en de inwerkingtreding van de nieuwe verordening wordt niet verwacht voor eind 2022.
- Op 21 maart 2018 werd een nieuwe Camerawet aangenomen die onder andere een gewijzigde aanmeldingsbepaling invoert en enkele bijkomende verplichtingen oplegt.[20, 21]
- Er werden enkele collectieve arbeidsovereenkomsten gesloten die betrekking hebben op het recht op privacy van de werknemer in de uitvoering van de arbeidsovereenkomst:

14. Voor een meer volledig overzicht, zie W. Debeuckelaere en G. Vermeulen, *Geannoteerde Wetboeken Privacy 2020*, Larcier, 2020.
15. Europees Verdrag van de Rechten van de Mens en de fundamentele vrijheden, d.d. 4 november 1950, www.echr.coe.int/Documents/Convention_NLD.pdf.
16. Handvest van de Grondrechten van de Europese Unie, (2000/C364/01), https://www.europarl.europa.eu/charter/pdf/text_nl.pdf.
17. Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, Pb.L. 201, 31 juli 2002, 37-47. Deze richtlijn werd in 2009 gewijzigd ingevolge de amenderende richtlijn 2009/136/EG.
18. Wet van 13 juni 2005 betreffende de elektronische communicatie, BS 20 juni 2005.
19. Wetboek van economisch recht van 28 februari 2013, BS 28 mei 2003.
20. Wet tot regeling van de plaatsing en het gebruik van bewakingscamera's van 21 maart 2007, BS 31 mei 2007, gewijzigd bij wet van 21 maart 2018, BS 16 april 2018 en bij wet van 30 juli 2018, BS 31 augustus 2018, hierna de 'Camerawet' genoemd.
21. De Camerawet wordt in meer detail besproken in hoofdstuk 5.3.

- ✓ cao nr. 38 van 6 december 1983 heeft betrekking op de werving en selectie van werknemers[22];
- ✓ cao nr. 39 van 13 december 1983 heeft betrekking op de voorlichting en het overleg inzake de sociale gevolgen van de invoering van nieuwe technologieën[23];
- ✓ cao nr. 68 van 16 juni 1998 heeft betrekking op de bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de camerabewaking op de arbeidsplaats[24];
- ✓ cao nr. 81 van 26 april 2002 heeft betrekking op de bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische online communicatiegegevens[25].

♦ De Witwaswet[26] bevat eveneens bepalingen omtrent het verwerken van persoonsgegevens en uitzonderingen op het principe van het uitoefenen van het inzagerecht door de betrokkene.

22. Collectieve arbeidsovereenkomst nr. 38 van 6 december 1983 betreffende de werving en selectie van werknemers, gewijzigd door de collectieve arbeidsovereenkomsten nr. 38bis van 29 oktober 1991, nr. 38ter van 17 juli 1998, nr. 38quater van 14 juli 1999, nr. 38quinquies van 21 december 2004 en nr. 38sexies van 10 oktober 2008, http://www.cnt-nar.be/CAO-COORD/cao-038.pdf.
23. Collectieve arbeidsovereenkomst nr. 39 van 13 december 1983 betreffende de voorlichting en het overleg inzake de sociale gevolgen van de invoering van nieuwe technologieën, http://www.cnt-nar.be/CAO-COORD/cao-039.pdf.
24. Collectieve arbeidsovereenkomst nr. 68 van 16 juni 1998 betreffende de bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de camerabewaking op de arbeidsplaats, https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/01.02.02.09-cao68.pdf.
25. Collectieve arbeidsovereenkomst nr. 81 van 26 april 2002 tot bescherming van de persoonlijke levenssfeer van de werknemers ten opzichte van de controle op de elektronische online communicatiegegevens, http://www.cnt-nar.be/CAO-COORD/cao-081.pdf.
26. Wet van 18 september 2017 tot voorkoming van het witwassen van geld en de financiering van terrorisme en tot beperking van het gebruik van contanten, BS 6 oktober 2017.

## Hoofdstuk 2.

# Is de GDPR van toepassing op accountantskantoren?

De GDPR is van toepassing op:

- elke geheel of gedeeltelijk geautomatiseerde verwerking van persoonsgegevens;
- elke niet-geautomatiseerde verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen.[27]

Om te voorkomen dat een ernstig risico op omzeiling zou ontstaan, dient de bescherming van natuurlijke personen technologieneutraal te zijn en mag zij niet afhankelijk zijn van de gebruikte technologieën.[28] Bijgevolg is iedere digitale verwerking van persoonsgegevens onderworpen aan de GDPR.

Een papieren verwerking is onderworpen aan de GDPR zodra ze op een gestructureerde manier gebeurt, bijvoorbeeld bij het aanleggen van een (papieren) dossier met een bepaald dossiernummer.

Een accountant mag er dus van uitgaan dat iedere verwerking van persoonsgegevens die hij uitvoert in de uitoefening van zijn professionele activiteit, onderworpen is aan de verplichtingen van de GDPR.

De GDPR is niet van toepassing op de verwerking van persoonsgegevens door een natuurlijke persoon bij de uitoefening van een zuiver persoonlijke of huishoudelijke activiteit. De verwerking van gegevens op een persoonlijke smartphone die niet professioneel gebruikt wordt, is dus niet onderhevig aan de GDPR. Ook een persoonlijk profiel op sociale

27. Art. 2 GDPR.
28. Overweging nr. 15 GDPR.

media dat niet professioneel gebruikt wordt, is niet aan de GDPR onderworpen, net zomin als het aanleggen van een fotoalbum van een familiefeest.

Hoofdstuk 3.

# Kernbegrippen van de GDPR

## 3.1. Wat zijn persoonsgegevens?

### 3.1.1. Definitie van persoonsgegevens

Persoonsgegevens zijn alle gegevens aan de hand waarvan een natuurlijk persoon geïdentificeerd kan worden of identificeerbaar is. Het betreft gegevens waarbij de persoon onmiddellijk identificeerbaar is, zoals een naam, een adres, een rijksregisternummer of een foto. Maar ook gegevens waaruit de identiteit van een persoon afgeleid kan worden of die gekoppeld zijn aan een bepaalde persoon: leeftijd, gewoontes en gedragingen, rekeninguittreksels, opleidingsniveau, inloggegevens ...[29]

De definitie van persoonsgegevens is erg ruim en bevat alle gegevens die gekoppeld kunnen worden aan een natuurlijke persoon. Zo maken de contactgegevens van een cliënt persoonsgegevens uit, evenals zijn gezinssituatie, een foto van zijn wagen en de omstandigheden waarin een relatiebreuk tot stand is gekomen.

### 3.1.2. Uitzonderingen

De GDPR voorziet echter in enkele uitzonderingen van gegevens die geen persoonsgegevens uitmaken.

- Gegevens van overleden personen maken geen persoonsgegevens uit. Dit zorgt er echter niet voor dat alle gegevens die betrekking hebben op overleden personen, zonder beperking verwerkt kunnen worden.

29. Art. 4.1 GDPR.

Zo voorziet de wet betreffende de rechten van de patiënt in een beperking op het recht op inzage en kopie van het patiëntendossier van een overleden persoon.[30]

In het kader van een nalatenschap is het vermogen van de overleden persoon rechtstreeks gelinkt aan de erfgenamen, zodat deze gegevens nog steeds onder de GDPR vallen.

Specifiek voor accountants is er geen uitzondering voorzien met betrekking tot het beroepsgeheim aangaande overleden personen. Het beroepsgeheim en dus de vertrouwelijkheid van de gegevens die betrekking hebben op deze overleden persoon blijven dus gelden. Daarenboven zal een nalatenschap toevallen aan de erfgenamen, die uiteraard opnieuw natuurlijke personen zijn.

- Gegevens die betrekking hebben op rechtspersonen maken ook geen persoonsgegevens uit. Ook hier moet rekening gehouden worden met gegevens die gelinkt worden aan natuurlijke personen.

  Bij een eenmanszaak zullen bepaalde gegevens op een jaarrekening snel gekoppeld kunnen worden aan een natuurlijk persoon en persoonsgegevens uitmaken.

  De gegevens van de contactpersonen van een rechtspersoon maken wel persoonsgegevens uit. Zo is het rechtstreekse telefoonnummer van een medewerker een persoonsgegeven. Een 'info@'-adres is geen persoonsgegeven, maar een 'olivier@'-adres maakt wel een persoonsgegeven uit.

- Anonieme gegevens maken geen persoonsgegevens uit. Gegevens zijn pas anoniem indien ze niet (meer) herleidbaar zijn tot een natuurlijke persoon, met andere woorden indien de identificatie van de betrokkenen aan de hand van die gegevens 'redelijkerwijs' onmogelijk gemaakt is. Hierbij dient rekening gehouden te worden met drie risico's die van essentieel belang zijn voor het anonimiseringsproces: de herleidbaarheid, de koppelbaarheid en de deduceerbaarheid van de gegevens.[31]

  Er bestaan verschillende anonimiseringstechnieken. Gegevens kunnen worden geanonimiseerd door persoonsgegevens te schrappen,

30. Art. 9, § 4 van de wet van 22 augustus 2002 betreffende de rechten van de patiënt, BS 26 september 2002.
31. Artikel 29-Werkgroep, Advies 5/2014 over anonimiseringstechnieken, 10 april 2014, WP216, 0829/14/NL, p. 13.

door encryptie te gebruiken, door datasets te verruimen of door randomisatie en generalisatie.[32]

### 3.1.3. Categorieën van persoonsgegevens

Persoonsgegevens kunnen worden onderverdeeld in categorieën, zoals identificatiegegevens, financiële gegevens, leefgewoontes, samenstelling van een gezin, persoonlijke kenmerken, consumptiegewoonten ...

Aan de hand van de categorieën van persoonsgegevens kan de waarde die de persoonsgegevens uitmaakt voor de betrokkene bepaald worden. Niet alle persoonsgegevens hebben voor een persoon namelijk dezelfde gevoeligheid of impact. Zo heeft het verlies van een lijst e-mailadressen een veel kleinere impact voor de betrokkenen dan wanneer een lijst met wachtwoorden, de details van een kredietkaart, bankuittreksels of gegevens die betrekking hebben op minderjarigen verloren gaat.

**Tip**

De volgende categorieën van persoonsgegevens moeten met grotere omzichtigheid verwerkt en beveiligd worden[33]:
- financiële gegevens zoals rekeninguittreksels en kredietkaartgegevens;
- gerechtelijke gegevens zoals vonnissen, boetes;
- wachtwoorden en log-ins;
- gegevens van minderjarigen;
- gegevens van minderheidsgroepen.

### 3.1.4. Bijzondere categorieën van persoonsgegevens

De GDPR definieert enkele limitatieve 'bijzondere' categorieën van persoonsgegevens die, door de gevoelige aard van de gegevens, op een andere manier behandeld moeten worden dan de overige categorieën van persoonsgegevens.[34] De verwerking van deze categorieën van persoonsgegevens is in principe verboden, mits inachtneming van enkele uitzonderingen.

32. Artikel 29-Werkgroep, Advies 5/2014 over anonimiseringstechnieken, 10 april 2014, WP216, 0829/14/NL.
33. Overweging nr. 75 GDPR
34. Art. 9 en 10 GDPR.

De GDPR beschrijft de volgende bijzondere categorieën van persoonsgegevens:

- gezondheidsgegevens, zoals een medisch dossier, een medische behandeling, een diagnose en gegevens met betrekking tot zorg;
- strafrechtelijke gegevens, zoals verdenkingen en inbeschuldigingstellingen van een verdachte, veroordelingen, straffen en veiligheidsmaatregelen[35];
- raciale en etnische gegevens;
- gegevens die betrekking hebben op seksueel gedrag en seksuele geaardheid;
- politieke opvatting en lidmaatschap van een politieke partij;
- lidmaatschap van een vakvereniging of vakbond;
- gegevens die betrekking hebben op een filosofische of geloofsovertuiging;
- genetische gegevens;
- biometrische gegevens, zoals een vingerafdruk of gezichtsherkenning.

Een accountant kan in een dossier in aanraking komen met deze bijzondere persoonsgegevens, zoals veroordelingen van een cliënt, medische gegevens die betrekking hebben op een bepaalde uitkering van cliënten of die verband houden met de loonberekening van werknemers van cliënten.

In principe is de verwerking van bijzondere persoonsgegevens verboden. De GDPR voorziet echter in enkele restrictieve uitzonderingen waarbij de verwerking van bijzondere persoonsgegevens wel toegestaan is.

- Het is toegestaan bijzondere persoonsgegevens te verwerken indien dit noodzakelijk is voor de instelling, de uitoefening of onderbouwing van een rechtsvordering, in een gerechtelijke procedure of in een administratieve en buitengerechtelijke procedure.[36]

- Indien de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt.[37]

- Indien de verwerking noodzakelijk is met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten van de verwerkingsverantwoordelijke of de betrokkene op het gebied van

35. Art. 10 GDPR.
36. Art. 9.2, f GDPR.
37. Art. 9.2, e GDPR.