# Inhoudsopgave

**Woord vooraf** ..... VII

**Hoofdstuk 1. Inleiding** ..... 1

1.1. Algemene Verordening Gegevensbescherming van 27 april 2016 ..... 1

1.2. De Belgische uitvoeringswetten ..... 3

1.3. 'Overige' privacywetgeving ..... 4

**Hoofdstuk 2. Is de GDPR van toepassing op accountantskantoren?** ..... 7

**Hoofdstuk 3. Kernbegrippen van de GDPR** ..... 9

3.1. Wat zijn persoonsgegevens? ..... 9

*3.1.1. Definitie van persoonsgegevens* ..... 9

*3.1.2. Uitzonderingen* ..... 9

*3.1.3. Categorieën van persoonsgegevens* ..... 11

*3.1.4. Bijzondere categorieën van persoonsgegevens* ..... 11

3.2. Wat is verwerken van persoonsgegevens? ..... 13

3.3. Wie zijn de actoren bij de verwerking? ..... 13

*3.3.1. Betrokkene* ..... 13

*3.3.2. Verwerkingsverantwoordelijke* ..... 14

*3.3.3. Verwerker* ..... 15

*3.3.4. Subverwerker* ..... 16

*3.3.5. Meerdere hoedanigheden* ..... 16

3.4. Is een accountant een verwerker of een verwerkingsverantwoordelijke? ..... 17

*3.4.1. Is een individuele accountant een verwerker of een verwerkingsverantwoordelijke?* . . . . . 17
*3.4.2. Is het accountantskantoor de verwerkingsverantwoordelijke of iedere accountant die deel uitmaakt van dit kantoor afzonderlijk?* . . . . . 19

**Hoofdstuk 4. Op welke manier moeten persoonsgegevens verwerkt worden?** . . . . . 23

4.1. Persoonsgegevens moeten steeds op een rechtmatige wijze verwerkt worden . . . . . 23
*4.1.1. Noodzakelijk voor de uitvoering van een overeenkomst* . . . . . 24
*4.1.2. Noodzakelijk voor de uitvoering van een wettelijke verplichting.* . . . . . 25
*4.1.3. Toestemming van de betrokkene.* . . . . . 26
*4.1.4. Noodzakelijk om het vitale belang van een persoon te beschermen.* . . . . . 27
*4.1.5. Noodzakelijk voor het vervullen van een taak van algemeen belang.* . . . . . 28
*4.1.6. Gerechtvaardigd belang.* . . . . . 28
4.2. De verwerking moet doelgebonden zijn . . . . . 29
4.3. De persoonsgegevens moeten toereikend en relevant zijn (dataminimalisatie) . . . . . 30
4.4. De persoonsgegevens moeten juist zijn . . . . . 30
4.5. De persoonsgegevens mogen niet langer bewaard worden dan nodig . . . . . 31
4.6. De persoonsgegevens moeten op een passende manier verwerkt en beveiligd worden. . . . . 34

**Hoofdstuk 5. Het opmaken van een privacybeleid in een accountantskantoor** . . . . . 37

5.1. Verantwoordingsplicht . . . . . 37
5.2. Stappenplan voor het opstellen van een privacybeleid. . . . . 38

**Hoofdstuk 6. Welke persoonsgegevens verwerkt een accountantskantoor?** . . . . . 43

6.1. Persoonsgegevens die worden verwerkt voor de interne werking van het kantoor . . . . . 43

6.2. Persoonsgegevens die worden verwerkt in het kader van de beroepsactiviteiten . . . . . 45

**HOOFDSTUK 7. OPMAKEN VAN EEN REGISTER VAN VERWERKINGSACTIVITEITEN** . . . . . 47

7.1. Wat is een register van verwerkingsactiviteiten? . . . . . 47

7.2. Hoe maak ik een register van verwerkingsactiviteiten op? . . . 48

*7.2.1. De naam en de contactgegevens van de verwerkingsverantwoordelijke en DPO* . . . . . 50

*7.2.2. Een beschrijving van de verwerkingsdoeleinden* . . . . . 51

*7.2.3. Categorie van persoonsgegevens en betrokkenen* . . . . . 51

*7.2.4. Verantwoording van de verwerkingsgronden* . . . . . 55

*7.2.5. Een lijst maken van de categorieën van ontvangers* . . . . . 57

*7.2.6. Doorgifte naar derde landen* . . . . . 58

*7.2.7. De beoogde termijn waarbinnen de verschillende categorieën van persoonsgegevens worden gewist* . . . . . 60

*7.2.8. Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen* . . . . . 60

**HOOFDSTUK 8. DATA PROTECTION OFFICER (DPO)** . . . . . 61

8.1. Wat is een DPO? . . . . . 61

8.2. Is de aanstelling van een DPO voor een accountantskantoor verplicht? . . . . . 61

8.3. Wat is een grootschalige verwerking? . . . . . 62

8.4. Wie kan worden aangesteld als DPO? . . . . . 65

8.5. Wat zijn de taken van een DPO? . . . . . 66

**HOOFDSTUK 9. INFORMATIEPLICHT** . . . . . 69

9.1. Wanneer moet de betrokkene geïnformeerd worden? . . . . . 71

*9.1.1. De informatie wordt verkregen bij de betrokkene zelf* . . . . . 71

*9.1.2. De informatie wordt niet verkregen bij de betrokkene zelf* . . . 73

9.2. Camerabeleid beveiligingscamera's . . . . . 76

*9.2.1. Administratieve verplichtingen* . . . . . 76

*9.2.2. Praktische verplichtingen* . . . . . 78

*9.2.3. Camerabewaking op de werkvloer* . . . . . 79

**9.3. Controle van online communicatiegegevens en opvolging van mailboxen bij afwezigheid** . . . . . 79
*9.3.1. Algemeen principe* . . . . . 80
*9.3.2. Controle* . . . . . 80
*9.3.3. Opvolging van mailboxen* . . . . . 83

**9.4. Cookies** . . . . . 85
*9.4.1. Algemeen* . . . . . 85
*9.4.2. Cookiebeleid* . . . . . 86

**Hoofdstuk 10. Passende technische en organisatorische maatregelen** . . . . . 89

**10.1. In kaart brengen van huidige maatregelen en risico's** . . . . . 90

**10.2. Technische maatregelen** . . . . . 91
*10.2.1. Authenticatie* . . . . . 91
*10.2.2. Wachtwoordbeheer* . . . . . 92
*10.2.3. Meerstapsverificatie* . . . . . 95
*10.2.4. Toegangsbeperking* . . . . . 96
*10.2.5. Loggen van de activiteiten* . . . . . 97
*10.2.6. Automatische slaapstand* . . . . . 97
*10.2.7. Encryptie* . . . . . 98
*10.2.8. Antivirussoftware* . . . . . 99
*10.2.9. Firewall, IDS en IPS* . . . . . 99
*10.2.10. Software-updates* . . . . . 100
*10.2.11. Thuiswerk* . . . . . 100
*10.2.12. Draadloos netwerk* . . . . . 101
*10.2.13. Draagbare toestellen* . . . . . 101
*10.2.14. Internet of Things* . . . . . 102
*10.2.15. Back-up* . . . . . 102
*10.2.16. Penetration test* . . . . . 103

**10.3. Organisatorische maatregelen** . . . . . 103
*10.3.1. Opleiding van het personeel en de medewerkers het rond gebruik van toestellen en GDPR* . . . . . 103
*10.3.2. Opleiding en awarenesstraining rond phishing* . . . . . 104
*10.3.3. Fysieke veiligheidsmaatregelen in het kantoor* . . . . . 107

**Hoofdstuk 11. Datalekken** . . . . . 109

**11.1. Wat is een datalek?** . . . . . 109

**11.2. Welke risico's zijn verbonden aan een datalek?** . . . . . 110

11.3. Wat te doen bij een datalek? . . . . . 111
*11.3.1. Het aanduiden van een SPOC* . . . . . 111
*11.3.2. Het registreren van het datalek in een intern register van datalekken* . . . . . 112
*11.3.3. Het uitvoeren van een risicoanalyse op het datalek* . . . . . 112
*11.3.4. Meldplicht bij de toezichthoudende autoriteit* . . . . . 115
*11.3.5. Meldplicht aan de betrokkenen zelf* . . . . . 116

11.4. Datalekken voorkomen . . . . . 117

**HOOFDSTUK 12. UITWISSELEN VAN PERSOONSGEGEVENS** . . . . . 119

12.1. Met medeverwerkingsverantwoordelijken . . . . . 119

12.2. Met verwerkers . . . . . 120

12.3. Derden-dienstverleners die geen verwerkers zijn . . . . . 122

12.4. Doorgifte van persoonsgegevens buiten de EER . . . . . 123
*12.4.1. Adequaatheidsbesluit* . . . . . 123
*12.4.2. EU-VS Privacy Shield* . . . . . 123
*12.4.3. Modelcontract* . . . . . 125

**HOOFDSTUK 13. HOE OMGAAN MET DE RECHTEN VAN BETROKKENEN?** . . . . . 127

13.1. Beschrijving van de verschillende rechten . . . . . 127
*13.1.1. Zijn er beperkingen op de rechten van betrokkenen?* . . . . . 128
*13.1.2. Is de accountant verplicht om gehoor te geven aan verzoeken van betrokkenen?* . . . . . 130
*13.1.3. Hoe (snel) moeten deze verzoeken beantwoord worden?* . . . 131
*13.1.4. Opmaken van een interne procedure en bewustmaking* . . . . 133
*13.1.5. Identificatie van de betrokkene* . . . . . 133

13.2. Recht op inzage . . . . . 136

13.3. Recht op verbetering (rectificatie) . . . . . 143

13.4. Recht op gegevenswissing (recht om vergeten te worden) . . 144

13.5. Recht op beperking van de verwerking . . . . . 148

13.6. Recht op overdraagbaarheid van gegevens (dataportabiliteit) . . . . . 150

**Hoofdstuk 14. Privacycommissie wordt Gegevensbeschermingsautoriteit (GBA)** . . . 151

14.1. Nieuwe naam en structuur . . . . . 151

14.2. Van adviesbevoegdheid naar volwaardige toezichthouder . . . 152
*14.2.1. Inspectiedienst* . . . . . 152
*14.2.2. Geschillenkamer* . . . . . 153

14.3. Sancties . . . . . 153