

Inhoud

Woord vooraf	11
Hoofdstuk 1	
Inleiding	13
1.1 Algemene Verordening Gegevensbescherming van 27 april 2016	13
1.2 De Belgische uitvoeringswetten	15
1.3 ‘Overige’ privacywetgeving	15
Hoofdstuk 2	
Is de GDPR van toepassing op accountantskantoren?	19
Hoofdstuk 3	
Kernbegrippen van de GDPR	21
3.1 Wat zijn persoonsgegevens?	21
3.1.1 Definitie van persoonsgegevens	21
3.1.2 Uitzonderingen	21
3.1.3 Categorieën van persoonsgegevens	22
3.1.4 Bijzondere categorieën van persoonsgegevens	23
3.2 Wat is verwerken van persoonsgegevens?	24
3.3 Wie zijn de actoren bij de verwerking?	24
3.3.1 Betrokkene	24
3.3.2 Verwerkingsverantwoordelijke	24
3.3.3 Verwerker	26
3.3.4 Subverwerker	26
3.3.5 Meerdere hoedanigheden	26
3.4 Is een accountant een verwerker of een verwerkingsverantwoordelijke?	27
3.4.1 Is een individuele accountant een verwerker of een verwerkingsverantwoordelijke?	27
3.4.2 Is het accountantskantoor de verwerkingsverantwoordelijke of iedere accountant die deel uitmaakt van dit kantoor afzonderlijk?	29

Hoofdstuk 4

Op welke manier moeten persoonsgegevens verwerkt worden? 33

4.1	Persoonsgegevens moeten steeds op een rechtmatige wijze verwerkt worden	33
4.1.1	Noodzakelijk voor de uitvoering van een overeenkomst	34
4.1.2	Noodzakelijk voor de uitvoering van een wettelijke verplichting	35
4.1.3	Toestemming van de betrokkene	35
4.1.4	Noodzakelijk om het vitale belang van een persoon te beschermen	37
4.1.5	Noodzakelijk voor het vervullen van een taak van algemeen belang	37
4.1.6	Gerechtvaardigd belang	37
4.2	De verwerking moet doelgebonden zijn	38
4.3	De persoonsgegevens moeten toereikend en relevant zijn (dataminimalisatie)	39
4.4	De persoonsgegevens moeten juist zijn	39
4.5	De persoonsgegevens mogen niet langer bewaard worden dan nodig	40
4.6	De persoonsgegevens moeten op een passende manier verwerkt en beveiligd worden	42

Hoofdstuk 5

Het opmaken van een privacybeleid in een accountantskantoor 45

5.1	Verantwoordingsplicht	45
5.2	Stappenplan voor het opstellen van een privacybeleid	46

Hoofdstuk 6

Welke persoonsgegevens verwerkt een accountantskantoor? 49

6.1	Persoonsgegevens die worden verwerkt voor de interne werking van het kantoor	49
6.2	Persoonsgegevens die worden verwerkt in het kader van de beroepsactiviteiten	50

Hoofdstuk 7

Opmaken van een register van verwerkingsactiviteiten 53

7.1	Wat is een register van verwerkingsactiviteiten?	53
7.2	Hoe maak ik een register van verwerkingsactiviteiten op?	54
7.2.1	De naam en de contactgegevens van de verwerkingsverantwoordelijke en DPO	55
7.2.2	Een beschrijving van de verwerkingsdoeleinden	56
7.2.3	Categorie van persoonsgegevens en betrokkenen	56
7.2.4	Verantwoording van de verwerkingsgronden	59
7.2.5	Een lijst maken van de categorieën van ontvangers	61
7.2.6	Doorgifte naar derde landen	62

7.2.7	De beoogde termijn waarbinnen de verschillende categorieën van persoonsgegevens worden gewist	63
7.2.8	Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen	63
Hoofdstuk 8		
Data Protection Officer (DPO)		65
8.1	Wat is een DPO?	65
8.2	Is de aanstelling van een DPO voor een accountantskantoor verplicht?	65
8.3	Wat is een grootschalige verwerking?	66
8.4	Wie kan worden aangesteld als DPO?	68
8.5	Wat zijn de taken van een DPO?	69
Hoofdstuk 9		
Informatieplicht		71
9.1	Wanneer moet de betrokkene geïnformeerd worden?	72
9.1.1	De informatie wordt verkregen bij de betrokkene zelf	72
9.1.2	De informatie wordt niet verkregen bij de betrokkene zelf	74
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	84
9.4.1	Algemeen	84
9.4.2	Cookiebeleid	85
Hoofdstuk 10		
Dataveiligheid binnen het kantoor		87
10.1	In kaart brengen van huidige maatregelen en risico's	88
10.2	Technische maatregelen	89
10.2.1	Authenticatie	89
10.2.2	Wachtwoordbeheer	89
10.2.3	Meerstapsverificatie	92
10.2.4	Toegangsbeperking en access management	93
10.2.5	Loggen van de activiteiten	94

10.2.6	Automatische slaapstand	95
10.2.7	Encryptie	95
10.2.8	Antivirussoftware	97
10.2.9	Firewall, IDS en IPS	97
10.2.10	Updates van besturingssystemen en software	98
10.2.11	Thuiswerk	99
10.2.12	Draadloos netwerk	100
10.2.13	Draagbare toestellen	100
10.2.14	Internet of Things	101
10.2.15	Back-up	101
10.2.16	Penetration test	101
10.2.17	ISO27001 Certificering	102
10.3	Organisatorische maatregelen	102
10.3.1	Opleiding van het personeel en de medewerkers rond het gebruik van toestellen en GDPR	102
10.3.2	Opleiding en awarenessstraining rond phishing	103
10.3.3	Fysieke veiligheidsmaatregelen in het kantoor	116
Hoofdstuk 11		
	Datalekken	119
11.1	Wat is een datalek?	119
11.2	Welke risico's zijn verbonden aan een datalek?	120
11.3	Wat te doen bij een datalek?	120
11.3.1	Het aanduiden van een SPOC	121
11.3.2	Het registreren van het datalek in een intern register van datalekken	121
11.3.3	Het uitvoeren van een risicoanalyse op het datalek	122
11.3.4	Meldplicht bij de toezichthoudende autoriteit	124
11.3.5	Meldplicht aan de betrokkenen zelf	125
11.4	Datalekken voorkomen	126
Hoofdstuk 12		
	Uitwisselen van persoonsgegevens	129
12.1	Met medeverwerkingsverantwoordelijken	129
12.2	Met verwerkers	130
12.3	Derden-dienstverleners die geen verwerkers zijn	131
12.4	Doorgifte van persoonsgegevens buiten de EER	132
12.4.1	Adequaatheidsbesluit	132
12.4.2	EU-VS Data Privacy Framework	132
12.4.3	Modelcontract	134

Hoofdstuk 13	
Hoe omgaan met de rechten van betrokkenen?	137
13.1 Beschrijving van de verschillende rechten	137
13.1.1 Zijn er beperkingen op de rechten van betrokkenen?	138
13.1.2 Is de accountant verplicht om gehoor te geven aan verzoeken van betrokkenen?	139
13.1.3 Hoe (snel) moeten deze verzoeken beantwoord worden?	140
13.1.4 Opmaken van een interne procedure en bewustmaking	141
13.1.5 Identificatie van de betrokkene	142
13.2 Recht op inzage	144
13.3 Recht op verbetering (rectificatie)	150
13.4 Recht op gegevenswissing (recht om vergeten te worden)	151
13.5 Recht op beperking van de verwerking	155
13.6 Recht op overdraagbaarheid van gegevens (dataportabiliteit)	156
Hoofdstuk 14	
Privacycommissie wordt Gegevensbeschermingsautoriteit (GBA)	159
14.1 Nieuwe naam en structuur	159
14.2 Van adviesbevoegdheid naar volwaardige toezichthouder	160
14.2.1 Inspectiedienst	160
14.2.2 Geschillenkamer	160
14.3 Sancties	161
Bijlagen	163
1. Register van gegevenslekken	163
2. Register van verwerkingsactiviteiten	164