

Inhoudsopgave

WOORD VOORAF	vii
HOOFDSTUK 1 INLEIDING	1
1.1. Algemene Verordening Gegevensbescherming van 27 april 2016	1
1.2. De Belgische uitvoeringswetten	4
1.3. ‘Overige’ privacywetgeving	5
HOOFDSTUK 2 IS DE GDPR VAN TOEPASSING OP ADVOCATENKANTOREN?	7
HOOFDSTUK 3 KERNBEGRIPPEN VAN DE GDPR	9
3.1. Wat zijn persoonsgegevens?	9
3.1.1. <i>Definitie van persoonsgegevens</i>	9
3.1.2. <i>Uitzonderingen</i>	9
3.1.3. <i>Categorieën van persoonsgegevens</i>	11
3.1.4. <i>Bijzondere categorieën van persoonsgegevens</i>	11
3.2. Wat is verwerken van persoonsgegevens?	13
3.3. Wie zijn de actoren bij de verwerking?	14
3.3.1. <i>Betrokkene</i>	14
3.3.2. <i>Verwerkingsverantwoordelijke</i>	14
3.3.3. <i>Verwerker</i>	15
3.3.4. <i>Sub-verwerker</i>	16
3.3.5. <i>Meerdere hoedanigheden</i>	16
3.4. Is een advocaat een verwerker of een verwerkingsverantwoordelijke?	17
3.4.1. <i>Is een individuele advocaat een verwerker of verwerkingsverantwoordelijke?</i>	17

HOOFDSTUK 6	WELKE PERSOONSgegevens VERWERKT EEN ADVOCATENKANTOOR?.....	45
6.1.	Persoonsgegevens die worden verwerkt voor de interne werking van het kantoor	45
6.2.	Persoonsgegevens die worden verwerkt in het kader van de beroepsactiviteiten	47
HOOFDSTUK 7	OPMAKEN VAN EEN REGISTER VAN VERWERKINGSACTIVITEITEN	51
7.1.	Wat is een register van verwerkingsactiviteiten?.....	51
7.2.	Hoe maak ik een register van verwerkingsactiviteiten op?	52
7.2.1.	<i>De naam en contactgegevens van de verwerkingsverantwoordelijke en DPO.....</i>	<i>54</i>
7.2.2.	<i>Een beschrijving van de verwerkingsdoeleinden</i>	<i>55</i>
7.2.3.	<i>Categorie van persoonsgegevens en betrokkenen</i>	<i>55</i>
7.2.4.	<i>Verantwoording van de verwerkingsgronden</i>	<i>60</i>
7.2.5.	<i>Oplijsten van de categorieën van ontvangers.....</i>	<i>63</i>
7.2.6.	<i>Doorgifte naar derde landen</i>	<i>64</i>
7.2.7.	<i>De beoogde termijn waarbinnen de verschillende categorieën van persoonsgegevens worden gewist</i>	<i>66</i>
7.2.8.	<i>Een algemene beschrijving van de technische en organisatorische beveiligingsmaatregelen.....</i>	<i>66</i>
7.2.9.	<i>Voorbeelduittreksel uit het register van verwerkingsactiviteiten</i>	<i>66</i>
HOOFDSTUK 8	DATA PROTECTION OFFICER (DPO)	69
8.1.	Wat is een DPO?.....	69
8.2.	Is de aanstelling van een DPO verplicht voor een advocatenkantoor?	69
8.3.	Wat is een grootschalige verwerking?.....	70
8.4.	Wie kan aangesteld worden als DPO?.....	72
8.5.	Mag een advocaat de functie van externe DPO uitvoeren?	73
8.6.	Wat zijn de taken van een DPO?.....	74

HOOFDSTUK 9	INFORMATIEPLICHT	75
9.1.	Wanneer moet de betrokkene geïnformeerd worden? . . .	76
9.1.1.	<i>De informatie wordt verkregen bij de betrokkene zelf</i> . . .	77
9.1.2.	<i>De informatie wordt niet verkregen bij de betrokkene zelf</i>	79
9.2.	Camera-beleid beveiligingscamera's	81
9.2.1.	<i>Administratieve verplichtingen</i>	82
9.2.2.	<i>Praktische verplichtingen</i>	84
9.2.3.	<i>Camerabewaking op de werkvloer</i>	85
9.3.	Controle van online communicatiegegevens en opvolging van mailboxen bij afwezigheid	85
9.3.1.	<i>Algemeen principe</i>	86
9.3.2.	<i>Controle</i>	86
9.3.3.	<i>Opvolging van mailboxen</i>	89
9.4.	Cookies	91
9.4.1.	<i>Algemeen</i>	91
9.4.2.	<i>Cookiebeleid</i>	92
HOOFDSTUK 10	PASSENDE TECHNISCHE EN ORGANISATORISCHE MAATREGELEN	95
10.1.	In kaart brengen van huidige maatregelen en risico's . . .	96
10.2.	Technische maatregelen	97
10.2.1.	<i>Authenticatie</i>	97
10.2.2.	<i>Wachtwoordbeheer</i>	98
10.2.3.	<i>Meerstapsverificatie</i>	101
10.2.4.	<i>Toegangsbeperking</i>	102
10.2.5.	<i>Loggen van de activiteiten</i>	103
10.2.6.	<i>Automatische slaapstand</i>	104
10.2.7.	<i>Encryptie</i>	104
10.2.8.	<i>Antivirussoftware</i>	105
10.2.9.	<i>Firewall, IDS en IPS</i>	106
10.2.10.	<i>Software updates</i>	106
10.2.11.	<i>Thuiswerk</i>	106
10.2.12.	<i>Draadloos netwerk</i>	107
10.2.13.	<i>Draagbare toestellen</i>	108
10.2.14.	<i>Internet of Things</i>	108
10.2.15.	<i>Back-up</i>	108
10.2.16.	<i>Penetration test</i>	109

10.3. Organisatorische maatregelen	109
10.3.1. Opleiding van het personeel en medewerkers rond gebruik van toestellen en GDPR	109
10.3.2. Opleiding en awareness-training rond phishing	110
10.3.3. Fysieke veiligheidsmaatregelen in het kantoor.....	113
HOOFDSTUK 11 DATALEKKEN	115
11.1. Wat is een datalek?	115
11.2. Welke risico's zijn verbonden aan een datalek?	116
11.3. Wat te doen bij een datalek?	117
11.3.1. Aanduiden van een SPOC.....	117
11.3.2. Registreren van het datalek in een intern register van datalekken	118
11.3.3. Het uitvoeren van een risicoanalyse op het datalek	118
11.3.4. Meldplicht bij de toezichthoudende autoriteit	120
11.3.5. Meldplicht aan de betrokkenen zelf	122
11.4. Datalekken voorkomen	123
HOOFDSTUK 12 UITWISSELEN VAN PERSOONSGEGEVENS	125
12.1. Met mede-verwerkingsverantwoordelijken	125
12.2. Met verwerkers	128
12.3. Derden-dienstverleners die geen verwerkers zijn	131
12.4. Doorgifte van persoonsgegevens buiten de EER	131
12.4.1. Adequaateheidsbesluit.....	132
12.4.2. EU-VS Privacy Shield	132
12.4.3. Modelcontract	133
HOOFDSTUK 13 HOE OMGAAN MET DE RECHTEN VAN BETROKKENEN?	135
13.1. Beschrijving van de verschillende rechten	135
13.1.1. Zijn er beperkingen op de rechten van betrokkenen?....	136
13.1.2. Is de advocaat verplicht om gehoor te geven aan verzoeken van betrokkenen?	138
13.1.3. Hoe (snel) moeten deze verzoeken beantwoord worden?	139
13.1.4. Opmaken van een interne procedure en bewustmaking	141
13.1.5. Identificatie van de betrokkene	141

13.2. Recht op inzage	144
13.3. Recht op verbetering (rectificatie).....	152
13.4. Recht op gegevenswissing (recht om vergeten te worden)	153
13.5. Recht op beperking van de verwerking.....	156
13.6. Recht op overdraagbaarheid van gegevens (dataportabiliteit)	158
HOOFDSTUK 14 PRIVACYCOMMISSIE WORDT GEGEVENS BESCHERMINGS-AUTORITEIT (GBA)	161
14.1. Nieuwe naam en structuur	161
14.2. Van adviesbevoegdheid naar volwaardige toezichthouder	162
14.2.1. <i>Inspectiedienst</i>	162
14.2.2. <i>Geschillenkamer</i>	163
14.3. Sancties	163