

# Table des matières/Inhoudstafel

## LA PROTECTION DES DONNÉES ET LES ENTREPRISES

<b>Préface</b>	11
DIDIER REYNDERS	
<b>Introduction</b>	13
AXEL BEELEN ET NATHALIE RAGHENO	
<b>L'employeur face au RGPD : rappel des principes et cas pratiques</b>	15
ANNE LAURE BROCORENS	
<b>Introduction</b>	15
<b>1. Les principes et notions du RGPD appliqués à la relation de travail</b>	16
1.1. Les notions essentielles	16
1.2. L'employeur et ses obligations ; le travailleur et ses droits	20
1.2.1. Les obligations de l'employeur	20
1.2.2. Les droits du travailleur	36
<b>2. Le droit de contrôle de l'employeur</b>	39
2.1. Introduction	39
2.2. Le contrôle de l'utilisation des technologies de l'information et de la communication (TIC) : e-mail et internet	40
2.2.1. La problématique	40
2.2.2. Le RGPD	40
2.2.3. La CCT n° 39 et la CCT n° 81	42
2.3. Le contrôle du télétravailleur	44
2.3.1. La CCT n° 81	45
2.3.2. Le cadre général : le RGPD et l'article 8 de la Convention européenne des droits de l'homme	45
2.3.3. En pratique	46
2.4. La géolocalisation	48
2.4.1. Général	48
2.4.2. L'analyse d'impact	50
2.4.3. Finalité, licéité et information (transparence)	50

2.4.4.	Le principe de proportionnalité	53
2.4.5.	Conclusion quant à la géolocalisation	54
	<b>Conclusion</b>	<b>55</b>
	<b>Comment s'assurer de la conformité au RGPD de tout nouveau produit ou service ?</b>	<b>57</b>
	FANNY COTON	
<b>1.</b>	<b>Introduction</b>	<b>57</b>
1.1.	<i>Privacy by design</i>	57
1.2.	<i>Privacy by default</i>	59
1.3.	Associer le délégué à la protection des données en temps utile	59
1.4.	Réaliser une analyse d'impact sur la protection des données	59
1.4.1.	Quand ?	60
1.4.2.	À chaque fois ?	62
1.4.3.	Qui ?	62
1.4.4.	Comment ?	63
1.4.5.	Doit-elle être publiée ?	63
<b>2.</b>	<b>R&amp;D</b>	<b>64</b>
2.1.	Recherche scientifique	64
2.2.	Traitement initial	64
2.3.	Traitement ultérieur	65
2.4.	Exigences spécifiques du droit belge pour la recherche scientifique	66
2.5.	Données de test	68
2.6.	Environnement de tests	68
2.7.	Anonymisation des données personnelles	68
2.8.	Pseudonymisation des données personnelles	69
2.9.	Réaliser des tests visant spécifiquement la protection des données	70
2.10.	Checklist chronologique	70
2.10.1.	Phase 0 : demande	70
2.10.2.	Phase 1 : définition/planification	71
2.10.3.	Phase 2 : conception détaillée	72
2.10.4.	Phase 3 : vérification	74
2.10.5.	Phase 4 : validation	74
2.10.6.	Phase 5 : commercialisation	74
2.11.	Développement en partenariat	75

<b>3. Règles spécifiques à la commercialisation de certains produits ou services en fonction des données traitées</b>	77
3.1. Services de la société de l'information visant les enfants	77
3.1.1. Quand le consentement du titulaire de l'autorité parentale est-il nécessaire ?	77
3.1.2. Comment faire ?	78
3.1.3. Et après ?	80
3.2. Produits relatifs à des données de santé	80
<b>4. Règles spécifiques à la commercialisation de certains produits ou services en fonction de la technologie utilisée</b>	81
4.1. Applications	81
4.1.1. Transparence	81
4.1.2. <i>Privacy by default</i>	81
4.1.3. Consentement	82
4.1.4. Sécurité	82
4.2. Objets connectés	82
4.3. Assistants vocaux	83
<b>5. Espaces d'échange avec la clientèle</b>	85
5.1. Environnement « <i>Brick and mortar</i> »	85
5.1.1. Caméras de surveillance	85
5.1.2. Accueil	86
5.1.3. Commerce dématérialisé	88
<b>6. Requêtes des personnes concernées</b>	91
6.1. Bonne gestion des plaintes	91
6.2. Quelles exceptions possibles ?	92
6.3. Garantir le droit à la portabilité des données – Mise en œuvre concrète ?	93
<b>La protection des données personnelles et le département Marketing</b>	97
BART VAN DEN BRANDE (TRADUCTION ET ADAPTATION D'AXEL BEELEN ET NATHALIE RAGHENO)	
<b>1. Introduction : le marketing numérique et la protection des données sont-ils condamnés à être inconciliables ?</b>	97

<b>2. L'essentiel du RGPD pour les spécialistes du marketing</b>	99
2.1. Les principes de base du RGPD et leur signification pour les spécialistes du marketing	99
2.1.1. Qu'entend-on par une « donnée personnelle » et un « traitement » ?	99
2.1.2. La base : l' <i>accountability</i> des sociétés	101
2.1.3. La transparence	103
2.1.4. Minimisation des données	106
2.1.5. Périodes limitées de conservation ou « limitation du stockage »	107
2.1.6. Principe de limitation des finalités	110
2.1.7. <i>Data security</i>	111
2.1.8. « <i>To opt-in or not to opt-in</i> » : à propos des bases légales du traitement des données personnelles	114
2.1.9. Créer et tenir à jour un registre des activités de traitement (ou registre des traitements)	126
2.2. Le RGPD n'est pas une réglementation isolée : sur l'interaction avec d'autres réglementations	130
2.2.1. ePrivacy (marketing direct et antispam) pour le marketing digital	130
2.2.2. <i>Don't call me</i> pour le télémarketing	133
2.2.3. La liste Robinson pour les mailings directs sur papier	133
<b>3. Mise en pratique du RGPD pour les spécialistes du marketing</b>	134
3.1. Nécessité d'une politique et d'un plan de marketing intégrés à long terme : obtenez vos consentements aujourd'hui pour des actions que vous réaliserez demain	134
3.2. Quelle la situation juridique de votre agence marketing ?	135
3.2.1. Sous-traitant ou responsable du traitement ?	136
3.2.2. Points d'attention pour les accords de sous-traitance	138
3.2.3. Utilisation de sous-traitants non européens pour le traitement des données	141
3.3. Achat, location et échange de données	145
3.4. Profilage et segmentation	149
3.5. <i>Cookies</i>	150
<b>4. Les défis futurs des spécialistes du marketing</b>	153

<b>Développement informatique et sécurisation technique des données personnelles</b>	157
CYNTHIA CHARLIER ET JOFFREY VIGNERON	
<b>Introduction</b>	157
<b>1. Sécurisation du matériel informatique permettant un accès direct ou indirect aux données personnelles</b>	158
1.1. Généralités	158
1.1.1. Détermination des équipements autorisés à accéder aux informations de l'entreprise	158
1.1.2. Distinction entre matériel privé et matériel professionnel	158
1.1.3. Sécurisation minimale	159
1.2. Poste de travail et informatique mobile	160
1.2.1. Sécurisation minimale	160
1.2.2. Poste de travail	161
1.2.3. Informatique mobile	162
1.3. Réseaux informatiques internes	164
1.4. Serveurs	165
1.5. Locaux	167
<b>2. Sécurisation de l'accès aux données personnelles</b>	169
2.1. Authentification	169
2.1.1. Précautions à prendre	170
2.1.2. Caractéristiques des mots de passe	170
2.2. Gestion des habilitations	171
2.3. Traçage des accès	173
2.3.1. Précautions à prendre	173
2.3.2. Caractéristiques du système de journalisation	174
2.4. Wi-Fi	174
2.4.1. Utilisation du Wi-Fi pour le compte de l'entreprise	174
2.4.2. Utilisation du Wi-Fi de l'entreprise par des tiers	175
2.5. Sites internet	175
2.5.1. Sécurisation des sites de l'entreprise	175
2.5.2. Sécurisation de l'utilisation de sites appartenant à des tiers	176
2.6. Sécurisation des échanges avec les tiers	178
2.6.1. Sécurisation de la transmission de données aux tiers	178
2.6.2. Sécurisation de la réception de données par l'entreprise	179

<b>3. Sécurisation des données personnelles</b>	180
3.1. Sauvegarde et continuité de l'entreprise	180
3.1.1. Sécurisation de la sauvegarde des données	180
3.1.2. Gestion adéquate des incidents	180
3.1.3. Protection du matériel servant aux traitements essentiels	181
3.2. Archivage et destruction des données archivées	181
3.3. Maintenance et destruction des données	181
<b>4. Sécurisation du traitement des données par des tiers</b>	182
4.1. Garanties des sous-traitants	183
4.2. Contrat avec les sous-traitants	183
<b>Conclusion</b>	185
<b>Le RGPD et le département Finances et achats</b>	187
LAURE-ANNE NYSSSEN ET ARIANE WARNIMONT	
<b>Introduction</b>	187
<b>1. Identification des principaux traitements du département Finances et registre des traitements</b>	188
1.1. Questions pratiques au sujet du registre des traitements	188
1.1.1. Comment identifier les traitements devant être renseignés dans le registre ?	188
1.1.2. Quel est le niveau de précision devant être atteint ?	189
1.1.3. Comment répondre aux questions auxquelles on n'a pas (encore) la réponse ?	190
1.2. Analyse des principaux traitements du département Finances	197
<b>2. Problématiques spécifiques découlant des traitements réalisés par le département Finances</b>	201
2.1. Gestion des sous-traitants	201
2.1.1. Qualification des parties prenant part à un traitement	201
2.1.2. Contractualisation de la sous-traitance et clauses obligatoires	205
2.1.3. Les sous-traitants (ou leurs employés et représentants) sont aussi des personnes concernées	207
2.2. Transferts de données en dehors de l'Espace économique européen	209
2.2.1. Rappel des principes	209
2.2.2. Nouvelles <i>Standard Contractual Clauses</i> de la Commission européenne	213
2.2.3. Impact de l'arrêt <i>Schrems II</i>	215
2.2.4. Impact du Brexit	218

2.3. Gestion des responsabilités et des risques	218
2.3.1. Peut-on aménager contractuellement la responsabilité découlant du RGPD ?	218
2.3.2. Peut-on s'assurer contre les amendes infligées en vertu du RGPD ?	220
<b>Conclusion</b>	222

## **GEGEVENS BESCHERMING EN BEDRIJFSLEVEN**

<b>Voorwoord</b> DIDIER REYNDERS	225
-------------------------------------	-----

<b>Inleiding</b> AXEL BEELEN EN NATHALIE RAGHENO	227
---	-----

<b>Gegevensbescherming in de HR-afdeling</b> ISABEL PLETS	229
--	-----

<b>Inleiding</b>	229
------------------	-----

<b>1. Rekrutering en gegevensbescherming</b>	230
--	-----

1.1. Wat mag je vragen van kandidaat?	230
1.1.1. Uittreksel uit het strafregister?	230
1.1.2. Referentieonderzoeken?	231
1.2. Management van cv's en motivatiebrieven	232
1.2.1. Online solliciteren	232
1.2.2. Hoelang bijhouden?	232
1.3. Samenwerking met externe rekruteringsbureaus	233

<b>2. Tewerkstelling en gegevensbescherming</b>	234
---	-----

2.1. <i>Onboarding: data protection notice</i> voor personeel	234
2.2. De adequate rechtsgrond in HR	235
2.3. Monitoring door de werkgever	236
2.4. Implementatie nieuwe HR-processen (bv. diversiteitsbeleid, toegangsmanagement op grond van biometrische gegevens, verwerking gezondheidsgegevens...): waaraan denken op het vlak van AVG?	238
2.4.1. Algemeen	238
2.4.2. Verwerking gevoelige persoonsgegevens	239
2.4.3. DPIA?	240

2.4.4.	Aanstelling DPO	241
2.5.	Opleiding en sensibilisering van werknemers in het algemeen en HR-managers in het bijzonder	243
2.5.1.	Algemeen	243
2.5.2.	Bijzonder voor HR	243
2.6.	Betrokkenheid van overlegorganen?	245
<b>3.</b>	<b>Ontslag en gegevensbescherming</b>	<b>246</b>
3.1.	<i>To do's</i> bij ontslag	246
3.1.1.	Afsluiten mailbox	246
3.1.2.	Beheer van informatie op bedrijfswebsite/sociale media	248
3.1.3.	Communicatie over ontslag	249
3.1.4.	Hoelang mogen persoonsgegevens voor HR worden bijhouden?	249
3.2.	Wees voorbereid op de uitoefening van rechten door het personeel	250
3.2.1.	Algemeen	250
3.2.2.	Grenzen aan de rechten	253
3.2.3.	Recht op toegang tot en inzage in specifieke persoonsgegevens	254
<b>Besluit</b>		<b>255</b>
<b>De AVG voor productmanagers</b>		<b>257</b>
LIESA BOGHAERT EN BERND FITEN		
<b>1.</b>	<b>De algemene verordening gegevensbescherming voor productmanagers</b>	<b>257</b>
1.1.	Voor wie?	257
1.2.	De productmanager van ontwerp tot nazorg	258
<b>2.</b>	<b>Wat is de algemene verordening gegevensbescherming (AVG)?</b>	<b>258</b>
2.1.	Een Europese verordening	258
2.2.	De verwerking van persoonsgegevens	259
2.2.1.	Wat zijn “persoonsgegevens”?	259
2.2.2.	Wat is “verwerken”?	260
2.3.	Het belang van de AVG voor de productmanager	260
<b>3.</b>	<b>De ontwerpfasen</b>	<b>261</b>
3.1.	Inleiding	261



3.2.	We hebben (opnieuw) een verwerkingsplan nodig!	262
3.3.	Wat is de rol van de organisatie?	263
3.3.1.	Waarom is de juiste rol van belang?	263
3.3.2.	Verantwoordelijke voor de verwerking ( <i>data controller</i> ) en de rechtsgrondslag	263
3.3.3.	Verwerker ( <i>data processor</i> ) en het verwerkingscontract	266
3.3.4.	Gezamenlijke verantwoordelijken ( <i>joint controllers</i> )	268
3.4.	<i>Privacy by design</i> en <i>privacy by default</i>	269
3.5.	De mogelijke risico's in kaart brengen	270
3.5.1.	Wat is een gegevensbeschermingseffectbeoordeling (GEB)?	270
3.5.2.	Is een GEB verplicht?	271
3.5.3.	Wanneer moet een GEB worden uitgevoerd?	274
3.5.4.	Moet de GBA worden gecontacteerd?	274
3.6.	De productmanager als functionaris voor gegevensbescherming (FG)?	274
3.6.1.	Wat doet een FG?	274
3.6.2.	Is een FG verplicht?	275
3.6.3.	Wie kan optreden als FG?	275
3.6.4.	Aanmelden van de FG	276
<b>4.</b>	<b>De productie- en ontwikkelingsfase</b>	<b>277</b>
4.1.	Inleiding	277
4.2.	Persoonsgegevens bij de productie en ontwikkeling	277
4.2.1.	Contractueel kader	277
4.2.2.	Doorgifte van persoonsgegevens	277
4.3.	Persoonsgegevens bij het testen	278
4.3.1.	Testen van software	278
4.3.2.	<i>Proof of concept</i> (PoC)	279
<b>5.</b>	<b>De verkoopfase</b>	<b>280</b>
5.1.	Inleiding	280
5.2.	Verzamelen en gebruiken van <i>leads</i>	280
5.2.1.	Netwerken	281
5.2.2.	Telemarketing	282
5.2.3.	Online leads generation	283
5.3.	Adverteren	286
5.3.1.	Direct marketing	286
5.3.2.	Tracking	289
5.3.3.	Profilering	292

5.3.4.	Targeted advertising via ‘ <i>Custom Audiences</i> ’ en ‘ <i>Lookalike Audiences</i> ’	293
5.3.5.	Influencers, bloggers en vloggers	294
5.4.	Getrouwheidsprogramma’s en klantenkaarten	295
5.5.	Informeren van de klant	297
5.5.1.	Het privacybeleid	297
5.5.2.	Het cookiebeleid	301
5.6.	Doorgifte van persoonsgegevens	302
5.6.1.	Doorgifte binnen de Unie	302
5.6.2.	Doorgifte buiten de Unie	303
<b>6.</b>	<b>De nazorgfase</b>	<b>311</b>
6.1.	Inleiding	311
6.2.	Vragen en klachten	311
6.2.1.	Vragen of klachten van de klant	311
6.2.2.	Het behandelen van vragen of klachten	312
6.3.	Verbeteren van producten en diensten	312
6.4.	Uitoefening van AVG-rechten en behandelen van AVG-verzoeken	313
<b>7.</b>	<b>Aandachtspunten in elke fase</b>	<b>314</b>
7.1.	Beginselen inzake verwerking van persoonsgegevens	314
7.1.1.	Rechtmatigheid, behoorlijkheid en transparantie	315
7.1.2.	Doelbinding	315
7.1.3.	Minimale gegevensverwerking	316
7.1.4.	Juistheid	316
7.1.5.	Opslagbeperking	316
7.1.6.	Integriteit en vertrouwelijkheid	317
7.1.7.	Verantwoordingsplicht	317
7.2.	Het verwerkingsregister	317
7.3.	Beveiliging en datalekken	318
<b>8.</b>	<b>Inbreuken op de AVG</b>	<b>319</b>
8.1.	Wat is het risico?	319
8.2.	Enkele voorbeelden van handhaving	319

<b>Gegevensbescherming voor marketeers</b>	323
BART VAN DEN BRANDE	
<b>1. Inleiding: zijn digitale marketing en gegevensbescherming gedoemd om water en vuur te zijn?</b>	323
<b>2. AVG basics voor marketeers</b>	324
2.1. De basisbeginselen in AVG en de betekenis ervan voor marketeers	324
2.1.1. Wat zijn “persoonsgegevens” en wat is “verwerking”?	324
2.1.2. De basis: <i>accountability</i>	327
2.1.3. Transparantie	328
2.1.4. Dataminimalisatie	331
2.1.5. Bepaalde bewaartermijnen of “opslagbeperking”	332
2.1.6. Doelgebondenheid	335
2.1.7. <i>Data security</i>	336
2.1.8. <i>To opt-in or not to opt-in</i> : over rechtsgronden voor verwerking van persoonsgegevens	338
2.1.9. Een Register van Verwerkingsactiviteiten (of kortweg dataregister) aanleggen en bijhouden	350
2.2. De AVG staat niet op een eiland: over de wisselwerking met andere regelgeving	354
2.2.1. ePrivacy (direct marketing en antispam) voor digitale marketing	354
2.2.2. Bel-me-niet-meer voor telemarketing	356
2.2.3. De Robinsonlijst voor papieren direct mailings	357
<b>3. Praktische AVG-topics voor marketeers</b>	357
3.1. De nood aan een geïntegreerd marketingbeleid en -plan op lange termijn: vraag vandaag de opt-ins voor morgen	357
3.2. Samenwerken met je bureau of <i>agency</i> rond data	359
3.2.1. Verwerker of verantwoordelijke?	359
3.2.2. Aandachtspunten voor verwerkersovereenkomsten	361
3.2.3. Gebruik van niet-Europese partners voor dataverwerking	364
3.3. Data kopen, huren en uitwisselen	367
3.4. Profileren en segmentatie	371
3.5. Cookies	372
<b>4. Toekomstige uitdagingen voor marketeers</b>	375

<b>De rol van het IT-departement</b>	377
STÉPHANIE DE SMEDT	
<b>1. Inleiding</b>	377
<b>2. De sleutelrol van het IT-departement bij een rechtmatige verwerking van persoonsgegevens</b>	377
2.1. Beveiliging van persoonsgegevens	377
2.2. Opsporen, melden en remediëren van datalekken	381
2.3. Beoordeling en audit van dienstverleners-verwerkers	386
2.4. Opvolging van bewaartermijnen en anonimiseren/vernietigen van persoonsgegevens	387
2.5. De bijzondere rol van het IT-departement van een verwerker	390
<b>3. De verhouding tussen het IT-departement en de functionaris voor gegevensbescherming</b>	391
<b>4. Verwerkingen van persoonsgegevens door het IT-departement</b>	394
4.1. Toegangscontrole	394
4.2. Camerabewaking	396
4.3. Monitoren van IT-tools die binnen het bedrijf gebruikt worden en beheer van mailboxen van werknemers	398
4.4. Beheer van de website en socialemediakanalen van de onderneming	400
4.5. Voorbeeld register verwerkingsactiviteiten	401
<b>De rol van de afdeling Financiën in de AVG-complianceketen</b>	405
MAARTEN STASSEN	
<b>1. Inleiding</b>	405
<b>2. De afdeling Financiën als gatekeeper</b>	406
<b>3. De taken van de dienst Financiën binnen een AVG-complianceprogramma</b>	407
3.1. Register van verwerkingsactiviteiten	407
3.1.1. Loonadministratie	408
3.1.2. Beheer arbeidsongevallenverzekering	409
3.1.3. Fiscale verplichtingen tewerkstelling	411
3.1.4. Leveranciersbeheer	412

---

3.1.5.	Beheer en bewaring boekhoudkundige en fiscale documenten	413
3.1.6.	Overzicht handtekeningbevoegdheid	414
3.1.7.	AML-verplichtingen	415
3.1.8.	Betwistingen	416
3.2.	Technische en organisatorische maatregelen	417
<b>4.</b>	<b>Leveranciersbeheer</b>	<b>419</b>
4.1.	Bepaling verwerking persoonsgegevens	419
4.2.	Bepaling rollen en verantwoordelijkheden	420
4.2.1.	Gezamenlijke verwerkingsverantwoordelijke	421
4.2.2.	Aparte verwerkingsverantwoordelijke	422
4.2.3.	Verwerker	422
4.2.4.	Subverwerker	424
4.3.	Internationale doorgiftes van persoonsgegevens	425
4.3.1.	Aanvullende maatregelen	427
4.3.2.	Standaardbepalingen	428
<b>5.</b>	<b>Transparantieplichtingen</b>	<b>429</b>
<b>6.</b>	<b>Beheer contractuele verplichtingen</b>	<b>429</b>
<b>7.</b>	<b>Cyberverzekering</b>	<b>430</b>
<b>8.</b>	<b>AVG-specifieke reserves</b>	<b>430</b>
<b>9.</b>	<b>Boekhouding</b>	<b>431</b>