

Table des matières

CHAPITRE 1 - Introduction9

- 1.1. Un contenu juridique, une approche pratique..... 9
- 1.2. Les objectifs de cet ouvrage..... 11
- 1.3. Le contenu et ses limites 12
- 1.4. Comment lire ce livre ? 14

CHAPITRE 2 - Etape 1 : apprivoisez les enjeux du Règlement17

- 2.1. La vie privée, un enjeu majeur..... 18
 - 2.1.1. Une valeur fondamentale 18
 - 2.1.2. Le juste équilibre entre des intérêts qui s'opposent 22
 - 2.1.3. Les concepts de « protection dès la conception » et « protection par défaut » 23
 - 2.1.4. Le consentement du citoyen 25
- 2.2. Le besoin de réforme face au numérique 26
 - 2.2.1. Les lacunes du régime légal existant..... 26
 - 2.2.2. Un règlement directement applicable dans toute l'Union européenne..... 30
 - 2.2.3. Les nouveaux enjeux du Règlement..... 32
 - 2.2.4. Les opportunités en marge du Règlement 33

CHAPITRE 3 - Etape 2 : recensez les données que vous collectez actuellement ...35

- 3.1. De quoi parle-t-on exactement ? 35
 - 3.1.1. Les données à caractère personnel 36
 - 3.1.2. Les personnes concernées 37

3.1.3. Le traitement des données	40
3.1.4. Les données sensibles	47
3.1.5. Le consentement	49
3.1.6. Le traitement à grande échelle ou le « Big Data »	50
3.2. La cartographie des données collectées	53
3.2.1. Posez-vous les bonnes questions	54
3.2.2. L'analyse des différents départements	65

CHAPITRE 4 - Etape 3 : anticipez pour éviter les sanctions71

4.1. Ce qui rend le Règlement incontournable.....	71
4.1.1. La volonté du législateur	71
4.1.2. Les autorités nationales de protection des données.....	72
4.2. Les infractions et leurs sanctions	73
4.2.1. Les sanctions jusqu'à 10 millions d'euros ou 2% du chiffre d'affaires	73
4.2.2. Les sanctions jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires	74
4.2.3. Mieux vaut donc prévenir que guérir	76
4.3. Les critères de détermination des sanctions	76
4.3.1. La nature, la gravité et la durée de la violation	77
4.3.2. L'acte intentionnel ou la négligence	78
4.3.3. Les mesures prises pour atténuer le dommage subi	78
4.3.4. Le degré de responsabilité du responsable du traitement ou du sous-traitant	79
4.3.5. La récidive	79
4.3.6. Le degré de coopération avec l'autorité de contrôle	79
4.3.7. Les catégories de données	80
4.3.8. La notification de la violation	80
4.3.9. Les mesures préventives	80
4.3.10. Les codes de conduite et mécanismes de certification	81
4.3.11. Autres circonstances aggravantes ou atténuantes	82
4.3.12. Tableau récapitulatif.....	82
4.4. Que faire en pratique ?	83
4.4.1. La préparation et la mise en œuvre de moyens adéquats....	83
4.4.2. La coopération avec l'autorité de protection des données ..	84
4.5. Et si le danger venait d'ailleurs ?	85

4.5.1. Les personnes concernées et les recours à leur disposition... 85
4.5.2. Les concurrents et les actions pour concurrence déloyale ... 86

CHAPITRE 5 - Etape 4 : adaptez votre façon de collecter des données89

5.1. Les grands principes du Règlement	89
5.1.1. Le principe de la licéité, de la loyauté et de la transparence du traitement	90
5.1.2. Le principe de la limitation des finalités	90
5.1.3. Le principe de minimisation des données	91
5.1.4. Le principe d'exactitude des données	91
5.1.5. Le principe de la limitation de la conservation des données ..	92
5.1.6. Le principe de l'intégrité et de la confidentialité des données	92
5.1.7. Le principe de responsabilité	93
5.2. La collecte et le traitement tels que prévus par le Règlement	93
5.3. Le consentement, porte ouverte à tous types de traitement des données.....	95
5.3.1. Les critères d'un consentement valide	95
5.3.2. Le retrait de consentement.....	101
5.3.3. Le consentement avant le 25 mai 2018	101
5.3.4. Check-list.....	102
5.4. Prouver l'obtention du consentement	103
5.4.1. Les différentes façons de prouver le consentement.....	103
5.4.2. Le consentement en ligne	104
5.4.3. La déclaration de consentement	109
5.5. Relevé des cas où le traitement est permis en cas de consentement valable	110
5.5.1. Les données à caractère personnel de manière générale ...	111
5.5.2. Les données sensibles	111
5.5.3. Les données traitées de manière automatisée dans le cadre du profilage	112
5.6. Le cas spécifique des enfants	112

CHAPITRE 6 - Etape 5 : apprenez à traiter les données conformément au Règlement115

6.1. Les critères du traitement licite	115
6.1.1. Le consentement de la personne concernée.....	116
6.1.2. La relation contractuelle ou précontractuelle.....	116
6.1.3. Les obligations légales imposées au responsable du traitement ...	118
6.1.4. La sauvegarde des intérêts vitaux de la personne concernée	118
6.1.5. L'exécution d'une mission d'intérêt public.....	119
6.1.6. Les intérêts légitimes poursuivis par le responsable du traitement ...	119
6.2. Le traitement des données sensibles	121
6.2.1. Le principe de l'interdiction.....	121
6.2.2. Les exceptions.....	122
6.3. Le traitement à grande échelle.....	126
6.3.1. Le principe.....	126
6.3.2. Les obligations du responsable du traitement	126

CHAPITRE 7 - Etape 6 : respectez les droits des personnes concernées129

7.1. L'équilibre des intérêts.....	129
7.2. Les droits des personnes concernées	130
7.2.1. Le droit à la transparence.....	130
7.2.2. Le droit d'accès.....	131
7.2.3. Le droit de rectification	133
7.2.4. Le droit à l'effacement ou le droit à l'oubli	134
7.2.5. Le droit à la limitation du traitement	135
7.2.6. Le droit à la portabilité des données	137
7.2.7. Le droit d'opposition.....	138
7.2.8. Le droit de ne pas faire l'objet d'un profilage	139

CHAPITRE 8 - Etape 7 : exécutez vos obligations de responsable du traitement141

8.1. L'obligation de respecter le Règlement.....	141
8.2. La protection des données par défaut et dès la conception..	142
8.3. L'obligation d'information et de transparence.....	143
8.4. L'obligation de coopérer avec l'autorité de contrôle	148
8.5. L'obligation de sécuriser les données.....	148
8.5.1. La pseudonymisation des données à caractère personnel..	149
8.5.2. Les autres mesures techniques et organisationnelles.....	150
8.6. L'obligation de notification	151
8.6.1. L'obligation de notifier contenue à l'article 19.....	151
8.6.2. L'obligation de notifier contenue à l'article 34.....	152
8.6.3. L'obligation de notifier contenue à l'article 33.....	154

CHAPITRE 9 - Etape 8 : Organisez vos relations contractuelles157

9.1. La relation entre le responsable du traitement et son sous-traitant ..	157
9.1.1. Qui est le responsable du traitement ?	158
9.1.2. Qui est le sous-traitant ?	159
9.1.3. Vous êtes tour à tour responsable du traitement et sous-traitant	160
9.1.4. La relation contractuelle entre le responsable du traitement et le sous-traitant	161
9.2. Les relations de travail	164
9.2.1. Vis-à-vis de vos travailleurs	164
9.2.2. Vis-à-vis des personnes concernées.....	165
9.3. Les relations avec vos partenaires situés hors de l'Union européenne.....	166
9.3.1. Les transferts fondés sur une décision d'adéquation.....	168
9.3.2. Les transferts fondés sur des garanties appropriées	168
9.3.3. Les transferts fondés sur des dérogations pour des situations particulières	170

CHAPITRE 10 - Etape 9 : implantez les nouveautés du Règlement	173
10.1. Le délégué à la protection des données.....	174
10.1.1. Dans quels cas faut-il désigner un délégué ?	174
10.1.2. Quelle est sa fonction ?	175
10.1.3. Quelles sont ses missions ?	177
10.2. Le registre des activités de traitement des données.....	178
10.3. L'analyse d'impact	180
10.4 Les certifications et les codes de conduite	181
10.5. La charte de protection de la vie privée ou la « privacy policy ».....	182
CHAPITRE 11 - Conclusion	183
Bibliographie	187
Quelques ressources utiles disponibles en ligne	191