Table des matières

Avant-propos 1

Les mots et notions à maîtriser pour gérer le RGPD 3

Partie I
Mise en œuvre et champ d'application du RGPD 6

1. Bref historique situant le contexte 7
   1.1. Évolution du droit européen 7
   1.2. Caractère obligatoire du RGPD 7
   1.3. Entrée en application progressive 8
   1.4. Refonte de la loi de 1978 8
2. Champ d'application du RGPD 9
   2.1. Traitement de données 9
   2.2. Données à caractère personnel 10
   2.3. Traitements non concernés 11
   2.4. Responsable de traitement 11
   2.5. Un guichet unique : une amélioration à souligner ! 13
3. Concrètement, pour moi, dirigeant, qu'est-ce qui doit changer ? 15
   3.1. D'abord, suis-je concerné ? 15
   3.2. Mettre en place l'autocontrôle 15
   3.3. Les trois défis à relever 16
   3.4. La démarche à suivre se décline en six étapes 17
   3.5. Ressources conseillées 18

Partie II
Conditions de validité des traitements de données
à caractère personnel 19

1. Les six fondamentaux pour collecter et traiter les données 20
   1.1. Validité du traitement 21
   1.2. Traitement des données « sensibles » 23
   1.3. Traitement des données relatives aux condamnations pénales et infractions 25
   1.4. Profilage 25

Partie III
Les obligations du responsable du traitement 27

1. Le dirigeant doit s'impliquer ! 28
2. Les conséquences de l'autocontrôle 28
   2.1. Disparition des déclarations de traitements à la CNIL 29
   2.2. Les conditions de l'autocontrôle 29
   2.3. Qui doit gérer cet autocontrôle ? 30

3. Sous-traitance du traitement 30
3.1. Définition 30
3.2. Quelles obligations générales incombent aux sous-traitants ? 31
3.3. Quelles obligations spécifiques ? 32
3.4. Contrat de sous-traitance 34
3.5. Sous-traitance en chaîne 34
4. Protection des données 35
4.1. Principe de base : la minimisation 35
4.2. Protection des données dès la conception 35
4.3. Protection par défaut 35
4.4. La « pseudonymisation » des données 36
4.5. Pièges à connaître 37
5. Analyse d'impact (PIA) 37
5.1. Qui est concerné ? 37
5.2. Comment mener une analyse d'impact ? 38
6. Délégué à la protection des données (DPO) 38
6.1. Rôle et moyens d'action du DPO 39
6.2. La responsabilité du DPO 41
6.3. La protection du DPO 41
7. Registre des activités de traitement 42
7.1. Qui doit tenir un registre ? 42
7.2. Que doit contenir le registre ? 43
7.3. Quelles sanctions si le registre n'est pas ou mal tenu ? 44
8. Sécuriser les données personnelles 45
8.1. Objectiver les fichiers 45
8.2. Vérifier la pertinence des données 46
8.3. Limiter la conservation des données 48
8.4. Respecter les droits des personnes 49
8.5. Sécuriser les données 53

Partie IV
Les droits de la personne concernée 55

1. Droit à l'information 56
2. Droit d'accès 60
3. Droit de rectification 62
4. Droit d'opposition 63
5. Droit à l'oubli 65
6. Droit à la limitation du traitement 67
7. Droit à la portabilité des données 68
8. Exercice des droits par la personne concernée 72

Partie V
Missions et contrôle de la CNIL 75

1. Missions de la CNIL 76
2. Mesures correctrices 77
3. Sanctions 78
4. Autorité « chef de file » 80

Partie VI
Check-list opérationnelle en six étapes 83

1. Désigner votre DPO 84
   1.1. Désignation obligatoire... 84
   1.2. Désignation fortement conseillée... 85
   1.3. Où trouver un DPO ? 86
   1.4. Qui peut être DPO ? 86
   1.5. Conseils pratiques 88
   1.6. La validation de l'étape « DPO » 88
2. Auditer vos traitements de données personnelles 88
   2.1. Que faut-il auditer ? 89
   2.2. Le registre des activités de traitement 90
   2.3. Les six bonnes questions à se poser pour tenir le registre 93
   2.4. La validation de l'étape « audit » 94
3. Organiser les démarches à suivre 94
   3.1. Agir en deux temps 94
   3.2. Points significatifs d'attention à signaler 95
   3.3. Prudence et vigilance si... 95
   3.4. Validation des démarches à suivre 97
4. Gérer vos risques via un PIA 97
   4.1. Qu'est-ce qu'un risque sur la vie privée ? 97
   4.2. L'analyse d'impact sur la protection des données (PIA) 98
   4.3. Quand mener un PIA ? 99
   4.4. Qui participe à l'élaboration de l'analyse d'impact ? 100
   4.5. Le résultat du PIA 102
   4.6. Quelles mesures prendre pour traiter et limiter les risques ? 102
   4.7. Quid des atteintes potentielles à la vie privée ? 103
   4.8. Quid des menaces ? 104
   4.9. Quand faut-il transmettre son analyse d'impact à la CNIL ? 104
   4.10. Validation du PIA 105
5. Organiser vos processus internes 105
   5.1. La démarche globale à suivre 106
   5.2. Évaluation des violations 107
   5.3. Comment réagir en cas de violation de données à caractère personnel ? 109
   5.4. Validation de la mise en place des processus internes 112
6. Documenter votre conformité au RGPD 112
   6.1. Documentation sur vos traitements de données personnelles 112
   6.2. Information des personnes concernées 113
   6.3. Documents définissant les rôles et les responsabilités des acteurs . . . 113
   6.4. Validation de la mise en place des processus internes 113

En guise de conclusion... 114

Ne dramatisez pas ! 114
Et pourquoi ne pas faire d'une pierre deux coups ? 114