

Table des matières

Préface	7
Introduction	11
Qui est concerné par la protection des données personnelles ?	12
Que sont les données personnelles ?.....	13
Comment s'applique le RGPD ?.....	15
Droit français : ordonnance du 12 décembre 2018	16
Directive vie privée et communications électroniques (ePrivacy)	17
Méthode	19
CHAPITRE I	
La réglementation à mettre en œuvre	21
I. Les dispositions classiques	23
A. <i>Droits des personnes</i>	23
1. Droit d'information.....	23
1.1. Information spontanée.....	24
1.2. Information demandée	29
2. Droit d'accès.....	30
3. Droit à la rectification	31
4. Droit d'opposition	31
4.1. Premier cas	31
4.2. Second cas.....	32

4.3. Conséquences	32
4.4. Exceptions	33
B. Principes de traitement des données	34
1. À quelles conditions un traitement de données est-il licite ?	34
1.1. Non exclusivité du consentement.....	35
1.2. Licéité fondée sur le consentement.....	36
1.3. Autres fondements.....	37
2. Quels sont les principes relatifs au traitement des données personnelles ?	37
C. Exceptions.....	39
II. Les dispositions nouvelles.....	40
A. Droits des personnes	40
1. Droit à l'effacement (droit à l'oubli)	40
1.1. Dans quels cas le droit à l'effacement s'applique ?	41
1.2. Dans quels cas le droit à l'effacement ne s'applique pas ?	41
2. Droit à la limitation du traitement	42
3. Droit à la portabilité des données	43
3.1. Qu'est-ce que le droit à la portabilité des données ?.....	43
3.2. Quelle est la conséquence du droit à la portabilité des données ?.....	43
4. Droit aux notifications personnelles	44
4.1. Quels sont les cas de notifications personnelles ?	44
4.2. Quel est le temps de la notification ?.....	45
4.3. Quelle est la forme de la notification ?	45
4.4. Quels sont les cas dans lesquels la notification n'est pas nécessaire ?.....	45
B. Responsabilités	47
1. Qu'est-ce que le principe de responsabilité (ou <i>accountability</i>) ?	47
2. Le responsable de traitement	47
2.1. Qui est le responsable du traitement ?	47
2.2. Que doit faire le responsable du traitement ?	48
3. Le co-responsable	48
4. Le sous-traitant.....	49
4.1. Qui est le sous-traitant ?	49
Focus n°1. Maison mère et filiales.....	51

Focus n°2. Gestion des données personnelles par les collectivités territoriales	51
4.2. Comment choisir le sous-traitant ?	57
4.3. Peut-on recourir à un sous-sous-traitant ?	57
4.4. Quelles sont les obligations du sous-traitant ?	58
Focus n°3. Fusions et scissions de sociétés	59
C. Sanctions	61
1. Sanctions prononcées par la Commission Nationale de l'Informatique et des Libertés (CNIL)	61
1.1. Les mesures correctrices.....	61
1.2. Les amendes administratives	62
2. Dommages-intérêts.....	64
2.1. Responsabilité	64
2.2. Responsabilité solidaire	64
3. Sanctions pénales	65
3.1. Code pénal	65
3.2. Loi Informatique et Libertés	70
III. Enjeux pour les organisations	71
A. Renforcement de la protection et opportunités commerciales	71
B. Mise en conformité	72
C. Valorisation des données et compétitivité	72
D. Réputation	73

CHAPITRE II

La mise en œuvre de la réglementation..... 75

I. Mesures organisationnelles.....	77
A. Désigner un délégué à la protection des données	77
1. Les cas de désignation	77
1.1. Cas de désignation obligatoire.....	77
1.2. Désignation facultative	78
2. La personne du délégué.....	78
2.1. Qualités	78
2.2. Origine	79
3. La fonction du délégué à la protection des données.....	80
3.1. Statut	80

3.2. Droit du travail.....	80
3.3. Responsabilité	81
4. Les missions du délégué à la protection des données	81
B. Collaborer.....	82
1. Avec les sous-traitants.....	82
2. Avec les personnes concernées	85
3. Avec la Commission Nationale Informatique et Libertés (CNIL).....	86
3.1. Consulter préalablement la CNIL en cas de risque élevé	86
3.2. Accomplir des formalités préalables	87
Témoignage. Le RGPD et la santé. Thomas Duong, Juriste à l'Institut national des données de santé	88
3.3. Notifier à la CNIL les violations de données	91
C. Prouver la conformité	96
1. Les certifications	96
2. Les codes de conduite	97
II. Mesures structurelles	99
A. Créer un registre des traitements des données.....	99
1. Qu'est-ce que le registre des traitements des données ? ..	99
2. Qui doit tenir le registre ?	99
3. Dans quels cas la tenue d'un registre est obligatoire ?....	100
4. Quel est le contenu du registre ?	101
5. Quand mettre à jour le registre ?.....	103
B. Identifier les données traitées	103
1. Recenser les données personnelles traitées	103
Focus n°4. Collecte du numéro de sécurité sociale (Numéro d'Inscription au Répertoire).....	108
2. Identifier le nombre de données traitées	108
3. Déterminer qui a accès aux données	109
4. Déterminer la durée de conservation des données	109
Focus n°5. Intelligence artificielle et droit des données personnelles....	110
Focus n°6. Données bancaires.....	115
Cas pratique n°1. Droit à l'image et droit des données personnelles ...	117
5. Identifier les finalités du traitement des données.....	118

Cas pratique n°2. Données nécessaires aux services ressources humaines pour le recrutement.....	118
Cas pratique n°3. Gestion du personnel.....	120
Cas pratique n°4. Directive vie privée et communications électroniques/RGPD.....	122
Focus n°7. Transfert international de données.....	123
Cas pratique n°5. Situation internationale.....	127
Focus n°8. Le Privacy shield.....	130
6. Identifier le fondement juridique du traitement des données.....	131
C. Réaliser une étude d'impact.....	131
1. Quand réaliser une étude d'impact ?.....	131
2. Dans quels cas une analyse d'impact n'est pas exigée ?..	133
3. À quel moment mener une étude d'impact ?	134
4. Quel est le contenu d'une analyse d'impact ?.....	134
D. Élaborer des procédures internes.....	135
Cas pratique n°6. Vidéosurveillance sur le lieu de travail.....	136
Cas pratique n°7. Géolocalisation des voitures de salariés.....	137
Cas pratique n°8. Accès aux locaux professionnels par badge.....	141
Cas pratique n°9. Vente en ligne, cookies.....	142
III. Mesures techniques.....	145
A. Assurer la sécurité du traitement des données.....	146
1. Sécuriser les locaux.....	146
2. Sécuriser les postes de travail.....	146
3. Sécuriser le réseau local.....	148
4. Sécuriser les données sauvegardées.....	148
5. Pseudonymiser.....	149
6. Développer le personnel.....	150
B. Protéger dès la conception/par défaut.....	150
Bibliographie.....	153
Index.....	157