

### Introduction

<b>1. Introduction</b>	<b>5</b>
<b>2. Zoom sur la loi Informatique et Libertés</b>	<b>6</b>
<b>3. Zoom sur le RGPD</b>	<b>14</b>
3.1 Rappel du contexte du RGPD	15
3.2 La nécessité de maîtriser ses données	20
<b>4. Applicabilité de la loi Informatique et Libertés</b>	<b>22</b>
4.1 Applicabilité matérielle de la Loi Informatiques et Libertés	22
4.2 Qui contrôle le respect de la loi LIL3 ?	23
4.3 Qu'est-ce que je risque si je ne respecte pas LIL3 ?	24
4.3.1 Procédure de sanction	25
4.3.2 Typologie des sanctions	25
4.3.3 Sanctions pécuniaires	26
4.3.4 Sanctions pénales	30
4.3.5 Atteinte à l'image	33
4.4 Recours	34
<b>5. Qu'est-ce que l'Accountability ?</b>	<b>35</b>

5.1 Documentation et procédure en matière de sécurité	38
5.2 Documentation et procédure en matière de respect des droits des personnes	40
5.3 Documentation et procédure en matière de formation et de sensibilisation du personnel	40
5.4 Documentation et procédure en matière de conformité des traitements	41
5.5 L'Accountability, nouvel indice de détermination des sanctions	42

## Identifier les traitements

<b>1. Introduction</b>	<b>43</b>
<b>2. Comment identifier une donnée personnelle ?</b>	<b>44</b>
<b>3. Les cas où la donnée personnelle perd son pouvoir identifiant</b>	<b>47</b>
<b>4. Interdiction de traitement de certaines données personnelles</b>	<b>48</b>
<b>5. Comment identifier un traitement de données personnelles ?</b>	<b>54</b>
<b>6. Les obligations du responsable de traitement de données</b>	<b>55</b>
6.1 Qui est le responsable du traitement ?	55
6.2 La responsabilité	56
6.2.1 La responsabilité du responsable de traitement	58
6.2.2 La responsabilité pénale des dirigeants	61
6.2.3 Les responsables conjoints de traitement	

64

### **7 Le sous-traitant**

66

### **8. Le Délégué à la protection des données**

72

## S'assurer de la licéité de vos traitements

### **1. Introduction**

75

### **2. Les étapes clés en amont du traitement**

76

#### 2.1 Les finalités du traitement

77

#### 2.2 La qualité des données (principes de minimisation, d'exactitude et de mise à jour)

78

#### 2.3 La définition de la durée de conservation des données

81

#### 2.4 Le recensement du traitement dans le registre des activités de traitement

83

### **3. La mise en œuvre du traitement**

83

#### 3.1 Le principe de transparence

83

#### 3.2 L'information des personnes

85

#### 3.3 Le consentement des personnes

90

#### 3.4 Le respect des droits des personnes

96

##### 3.4.1 Les droits maintenus et renforcés

96

##### 3.4.2 Les nouveaux droits issus du RGPD

104

3.5 Les flux transfrontières	114
------------------------------	-----

## Les outils de la Compliance

<b>1. Vous avez dit Privacy by design et Privacy by default ?</b>	<b>121</b>
1.1 Privacy by design	121
1.1.1 La genèse du concept	121
1.1.2 L'émergence de la notion	122
1.1.3 La consécration du principe	122
1.2 Privacy by default	123
<b>2. Comment respecter le principe de Privacy by design ?</b>	<b>125</b>
2.1 Tenir un registre des traitements	125
2.2 Réaliser une étude d'impact sur la vie privée (PIA)	129
2.2.1 Contenu de la PIA	130
2.2.2 Description du traitement et de ses finalités	131
2.2.3 Évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités	132
2.2.4 Description des mesures pour faire face aux risques	133
2.2.5 Une évaluation des risques pour les droits et libertés des personnes concernées	134
2.2.6 Les résultats de l'EIVP	135
2.3 Nommer un délégué à la protection des données (DPO)	137

2.3.1 Désignation du DPO	137
2.3.2 Fonctions du DPO	146
2.3.3 Responsabilité du DPO	149
2.3.4 Missions du DPO	150
2.4 Adopter des certifications, labels et codes de conduite	154
2.4.1 La certification	154
2.4.2 Fin des labels CNIL	157
2.4.3 Les codes de conduite	158

## Sécuriser les traitements

<b>1. Introduction</b>	<b>161</b>
<b>2. Qui est concerné par l'obligation de sécurité ?</b>	<b>162</b>
<b>3. Pourquoi mettre en place des mesures de sécurité ?</b>	<b>164</b>
<b>4. Que dois-je faire pour sécuriser mon traitement ?</b>	<b>167</b>
4.1 Mener un audit de sécurité complet	169
4.2 Mettre en place des mesures techniques	169
4.2.1 Sécuriser l'accès physique aux locaux	170
4.2.2 Sécuriser les postes de travail	171
4.2.3 Sécuriser le réseau local	

4.2.4 Sécuriser les données sauvegardées	175
4.2.5 La pseudonymisation	176
4.3 Mettre en place des mesures organisationnelles	176
4.3.1 Élaborer un référentiel de sécurité complet	181
4.3.2 Adopter une logique Privacy by design	181
4.3.3 Mener des études d'impact et des tests d'intrusion	185
4.3.4 Tenir un registre des failles de sécurité	185
4.3.5 Sécuriser la confidentialité et la sécurité des données avec les prestataires et sous-traitants	186
4.3.6 Former son personnel au travers d'actions de sensibilisation	189
4.3.7 Nommer un RSSI	190
	191

## Annexes

<b>1. Quizz : Avez-vous le profil compliance ?</b>	<b>197</b>
<b>2. Bibliographies, liens utiles</b>	<b>200</b>