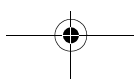
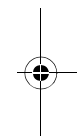
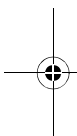
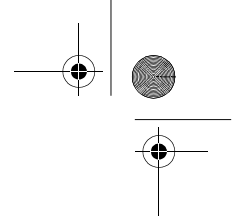




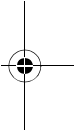
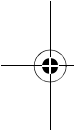
TABLE DES MATIÈRES

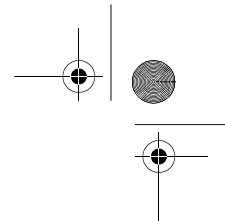
LES AUTEURS (PAR ORDRE ALPHABÉTIQUE)	7
1. AVANT-PROPOS	9
2. POSITIVER LA MISE EN CONFORMITÉ AU RGPD ? OUI, C'EST POSSIBLE !	13
2.1. Introduction	15
2.2. Les moyens et les objectifs	16
2.3. Le DPO : contrôle ou facilitation ?	19
2.4. Transformation : systémique et « positive attitude »	21
2.5. Leadership	27
2.6. L'influence des outils	28
2.7. Conclusion	29
3. LE DPO INTERNE DANS LES POUVOIRS LOCAUX : SEUL SUR SON ÎLE ?	31
3.1. Préambule	33
3.2. Particularités d'un pouvoir local	33
3.3. La définition du responsable de traitement	34
3.4. Obligations du responsable de traitement envers le DPO	35
3.5. Intégration du RGPD dans les outils de management des pouvoirs locaux	39
3.6. Positionnement et lettre de missions du DPO dans l'administration	40
3.7. Le DPO doit aider l'autorité publique dans la mise en conformité au RGPD	43
3.8. Particularités de l'environnement de travail	45
3.8.1. Prérequis : le DPO doit avoir une bonne connaissance des rouages de son administration	45
3.8.2. Définition d'une organisation de travail	48
3.8.3. Collaboration avec les services centraux et création de groupes de travail	49
3.9. Exemple de l'expérience provinciale : synthèse de la mise en place de la cellule DPO provinciale et de l'organisation de travail	51
3.10. Conclusion	51
4. COMMENT UTILISER L'ANALYSE D'IMPACT RELATIVE À LA PROTECTION DES DONNÉES COMME OUTIL DE MISE EN CONFORMITÉ ?	53
4.1. Introduction	55
4.2. Analyse d'impact relative à la protection des données (art. 35 et 36 RGPD)	55



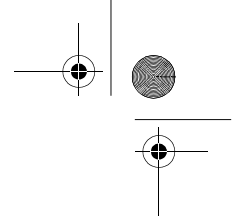


4.3.	Traitements concernés par la réalisation d'une AIPD	57
4.3.1.	Période concernée	57
4.3.2.	Type de traitement concerné	58
4.3.3.	Traitements considérés comme étant à risque élevé	59
4.3.3.1.	Traitements mentionnés à l'article 35.1 et 35.3 du RGPD	59
4.3.3.2.	Les traitements mentionnés dans les listes de l'autorité de contrôle	59
4.3.4.	Critères permettant de déterminer le caractère de risque élevé pour les droits et libertés des personnes concernées	61
4.4.	Traitements non concernés par l'AIPD	64
4.4.1.	Traitements qui figurent sur la liste de l'APD relative aux traitements pour lesquels une AIPD n'est pas obligatoire (art. 35.5 du RGPD)	64
4.4.2.	Traitements similaires (au regard de leur nature, de leur portée, de leur contexte, de leurs finalités) à un traitement pour lequel une AIPD a déjà été menée par le RT	65
4.4.3.	Article 35, § 10 : exemption à l'obligation de réaliser une AIPD préalable	65
4.5.	Éléments essentiels d'une AIPD	66
4.5.1.	Description détaillée des opérations et finalités (art. 35, § 7, pt a)	66
4.5.2.	Évaluation de la nécessité et de la proportionnalité en fonction des finalités (art. 35, § 7, pt b)	66
4.5.3.	Appréciation des risques pour les droits et libertés des personnes concernées (art. 35, § 7, pt c)	67
4.5.4.	Mesures envisagées pour traiter ces risques (art. 35(7)(d) et cons. n° 90)	69
4.5.5.	Conseil du délégué à la protection des données (DPO) (art. 35(2))	71
4.5.6.	Avis des personnes concernées ou de leurs représentants (art. 35, § 9)	71
4.5.7.	Formalisation de la validation de l'AIPD	71
4.5.8.	Suivi du plan d'action éventuel	71
4.6.	Moment pour mener une AIPD et révision des AIPD réalisées	72
4.7.	Acteurs de l'AIPD	72
4.8.	Méthode et outils pour mener une AIPD	75
4.9.	Publication de l'AIPD	79
4.10.	Avis de l'APD sur le projet de traitement à risque élevé (art. 36 RGPD)	79
4.11.	Une AIPD pour plusieurs traitements	80
4.12.	Conclusion	81





5. LA FUITE DE DONNÉES, LES ASPECTS PRATIQUES DANS UNE GRANDE ADMINISTRATION PUBLIQUE : LE SPF FINANCES	83
5.1. Introduction	85
5.2. Qu'est-ce qu'une violation de données ?	86
5.3. Constatation et traitement d'une fuite de données	89
5.3.1. La signalisation de l'incident	90
5.3.2. Le traitement de la fuite de données	93
5.3.3. L'information des tiers concernant la fuite de données	97
5.3.3.1. La notification à l'Autorité de protection des données	97
5.3.3.2. La communication à la personne concernée	99
5.3.3.3. D'autres types de notifications	101
5.3.4. La clôture du dossier	101
5.3.5. Sanctions	102
5.4. Conclusion	103
6. LA GESTION DES SOUS-TRAITANTS DANS LE SECTEUR PUBLIC	105
6.1. Introduction	107
6.2. Les différents acteurs	108
6.2.1. Les responsables de traitement successifs ou destinataires	109
6.2.2. Le sous-traitant	110
6.2.3. Le tiers	111
6.3. Responsabilité du choix du sous-traitant	111
6.4. Identifier et gérer les sous-traitants existants	111
6.5. Gérer les futurs sous-traitants dans le cadre des appels d'offres	112
6.6. Les aspects de confidentialité chez le sous-traitant	115
6.7. La collaboration du sous-traitant à l'analyse de risque	116
6.8. Révision périodique des relations de sous-traitance	116
6.9. Les sous-traitants étrangers et notamment américains	117
6.10. Conclusion	117
7. LE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL RELEVANT D'AUTRES RÉGIMES JURIDIQUES : LES TRAITEMENTS POLICIERS	119
7.1. Introduction	121
7.2. Cadre général	122
7.2.1. Champ d'application du titre 2	123
7.2.2. Champ d'application du titre 3	124
7.2.3. Interactions entre les trois régimes	125
7.3. Autorités de contrôle	126
7.3.1. APD – COC – Comité R (Comité P)	126
7.3.2. Autorité de contrôle spécifique	127
7.4. Aspects du traitement des données par les services de police	129
7.4.1. Différences entre le RGPD et le titre 2 de la LPD/complexité des différents régimes	129



7.4.2. Traitement de l'information policière au sein de la police intégrée	130
7.4.3. DPO au sein des services de police	131
7.4.4. Registre des traitements	132
7.4.5. Droits des personnes concernées	133
7.4.6. Analyse d'impact relative à la protection des données (« DPIA »)	134
7.4.7. Durée de conservation des données	135
7.4.8. Journalisation	135
7.4.9. Conclusions	136

