

Le but de ce guide est de compiler les questions que se posent les DPO, et d'y apporter une réponse pratique. Les solutions se baseront sur les questions que nous avons eues lors des formations que nous avons données, lors de contacts avec d'autres DPO, ou avec des représentants des autorités, que ce soit au niveau national ou européen.

Ce guide est un ouvrage pratique, répondant aux questions concrètes que se posent celles et ceux qui s'intéressent au RGPD, et qui souvent sont confrontés à des questions sans réponses. Ce n'est donc ni un ouvrage de droit, ni de sécurité de l'information, mais un guide pratique dont le but est d'aider les praticiens à avancer dans la mise en conformité de leurs organisations.

Ce guide sera suivi et adapté chaque année, afin de constituer un guide pratique toujours actualisé compilant l'ensemble des questions pratiques qui se posent aux praticiens. Nous prévoyons donc, avec optimisme, une version adaptée chaque année car le RGPD est une matière mouvante et en évolution constante.

Le guide sera composé d'une série de questions concrètes qui vous permettront de mettre en place des solutions pratiques et concrètes.

Vous trouverez à de nombreuses reprises, parmi les questions qui se posent des phrases commençant par NOTRE CONSEIL, qui reprendront ce que nous vous recommandons en nous basant sur la pratique.

Nous espérons que vous trouverez des réponses à vos questions et si vous voulez enrichir la version 2023, n'hésitez pas à nous envoyer un email à jacques@gdprfolder.eu



Sommaire

Préface	5
Liminaire	7
Introduction	11
Le RGPD	19
1. Le RGPD c'est quoi ?	19
2. Quelques définitions de base	20
3. Qu'est-ce que le profilage ?	24
4. Qu'est-ce que la pseudonymisation des données ?	24
5. Qu'est-ce qu'une donnée génétique ou biométrique ?	25
6. Quand devons-nous être en ordre par rapport au RGPD ?	25
7. Qui doit se soucier du RGPD et se mettre en ordre ?	26
8. Qui peut m'aider à me mettre en ordre ?	27
9. Y a-t-il des traitement de données personnelles qui ne sont pas concernés par le RGPD ?	27
10. Le RGPD s'applique-t-il uniquement en Europe ?	28
11. Quelle autorité est en charge de faire respecter le RGPD ?	29
Le dossier RGPD : le but à atteindre	31
1. Quelle est la table des matières du dossier RGPD ?	32
2. Quand sera-t-on certain que le dossier RGPD est définitivement complet ?	33
Les bases légales des traitements de données	35
1. Quelles sont les bases légales pour effectuer un traitement de données ?	35
2. Comment gérer le consentement ?	36
3. Comment gérer les traitements de données personnelles collectées sur la base d'un contrat ?	41
4. Comment gérer les données personnelles collectées sur la base d'une obligation légale ?	44
5. Comment gérer les traitements de données personnelles basés sur la sauvegarde de l'intérêt vital ?	45
6. Comment gérer les traitements basés sur l'intérêt légitime ?	46
7. Comment gérer les traitements de données personnelles basés sur la mission d'intérêt public ?	48

Quelles sont les règles qui encadrent l'utilisation des données personnelles ? 51

1. Y a-t-il des limites à la collecte des données ? 51
2. Comment être certain que le traitement est licite loyal et transparent ? 52
3. Que veut dire l'expression « finalités déterminées explicites et légitimes » ? 53
4. Comment gérer les traitements ultérieurs ? 53
5. Comment être certain que les données sont adéquates, pertinentes et limitées à ce qui est nécessaire ? 54
6. Comment être certain que les données conservées sont exactes et mises à jour ? 55
7. Comment gérer la durée de conservation des données ? 55
8. Comment vérifier si la sécurité des données est « appropriée » ? 56
9. Les données personnelles d'une personne décédée sont-elles soumises au RGPD ? 58
10. Qu'est-ce que la finalité du traitement ? 58
11. Quel est le lien entre finalité et base légale ? 59

Le Data Privacy Officer 61

1. Qu'est-ce qu'un DPO ? 61
2. Un DPO est-il responsable personnellement du respect du RGPD ? 62
3. Le DPO interne peut-il se voir infliger des sanctions ? 63
4. Le DPO externe peut-il voir sa responsabilité engagée ? 64
5. Le DPO ou le responsable de traitement peuvent-ils souscrire des polices d'assurance en responsabilité ? 64
6. Dans quels cas une organisation doit-elle nommer un DPO ? 65
7. Que sont les « autorités publiques ou organismes publics » qui doivent nommer un DPO ? 65
8. Dans quels cas une organisation doit-elle considérer que « ses activités de base consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées » et donc nommer obligatoirement un DPO ? 70

Comment formaliser la décision de nommer ou de ne pas nommer un DPO ? 81

1. Quel modèle de texte utiliser pour décider de ne pas désigner de DPO ? 82
2. Quel modèle de texte utiliser pour décider qu'un DPO est nécessaire ? 83
3. Quel modèle de texte utiliser pour formaliser la décision motivée de nomination du DPO choisi ? 84
4. Quelle publicité doit-on donner à la nomination du DPO ? 88
5. Peut-on désigner un DPO uniquement pour une partie de la mission ? 89
6. Peut-on nommer plusieurs DPO au sein d'une organisation ? 89

7. Quelles sont les sanctions en cas de non-respect des règles liées à la nomination du DPO ? 89
8. L'autorité doit-elle valider la nomination des DPO ? 90
9. Quel modèle de texte utiliser pour informer les collaborateurs de l'existence, de la mission et des fonctions du DPO ? 91

Comment choisir le DPO ? 95

1. Quelles sont les compétences nécessaires pour être DPO ? 95
2. Faut-il être universitaire ou détenir un diplôme spécifique pour être DPO ? 98
3. Quel est le profil d'un DPO en général ? 99
4. Quelles sont les qualités professionnelles nécessaires pour être DPO ? 99
5. Un avocat peut-il être DPO ? 101
6. Un élu local peut-il être DPO de l'organisation publique pour laquelle il est élu ? 102
7. Quelles sont les qualités humaines nécessaires pour être DPO ? 102
8. Les qualités nécessaires pour être DPO sont-elles identiques pour toutes les organisations ? 106
9. Existe-t-il des DPO « certifiés » ? 107
10. Le DPO est le contact privilégié de l'autorité nationale de protection des données 109
11. Comment éviter les conflits d'intérêts lors de la nomination d'un DPO interne ou externe ? 109
12. Vaut-il mieux choisir un DPO interne ou externe, à temps plein ou à temps partiel ? 112
13. Le DPO d'une autorité publique est-il nécessairement le DPO des entités gérées ou contrôlées par cette autorité ? 121
14. Interdiction de licenciement 123
15. Comment gérer la confusion quant aux titres : DPO, chef de projet, consultant,... ? 127
16. Peut-on nommer le même DPO pour un groupe d'organisations privées ? 127
17. Peut-on nommer le même DPO pour plusieurs organisations publiques ? 127
18. Y-a-t-il une limite au nombre d'organisations pour lesquelles le même DPO est responsable ? 127

Comment formaliser la relation avec le DPO ? 133

1. La nomination du DPO est-elle à durée déterminée ? 133
2. Quelle est la position hiérarchique du DPO interne ? 133
3. Quelles coordonnées du DPO doit-on communiquer publiquement ? 133
4. Le DPO est-il soumis à un secret professionnel ? 133

Quelles sont les droits et obligations de la direction par rapport au DPO ?	135
1. Quelles sont les ressources nécessaires que doit apporter l'organisation au DPO ?	135
2. Les courriers adressés au DPO sont-ils confidentiels ?	136
3. Quand la direction doit-elle consulter le DPO ?	136
4. Comment le DPO doit-il être associé aux questions relatives aux données personnelles ?	138
5. Quels soutiens et ressources la direction doit-elle fournir au DPO ?	141
6. La direction peut-elle décider de ce que le DPO va faire dans le cadre de sa mission ?	142
7. Que se passe-t-il en cas de désaccord entre le DPO et la direction ?	143
8. Que faire si un département refuse qu'un DPO effectue un contrôle ?	145
9. La direction peut-elle licencier le DPO du fait de sa mission ?	146
10. Qui est le responsable hiérarchique du DPO ?	147
11. Le DPO peut-il imposer des décisions à la direction de l'organisation ?	148
12. Que doit faire le DPO si la direction ne suit pas un de ses conseils ?	149
13. Que peut faire le DPO s'il n'est pas associé de façon appropriée et en temps utile aux décisions relatives aux données personnelles ?	150
Quelle est la fonction du DPO ?	151
1. Quelles sont les différentes missions du DPO ?	152
2. Que signifie l'approche fondée sur les risques pour la mission du DPO ?	153
3. Que signifie réellement le rôle de conseil du DPO ?	154
4. En quoi consiste le rôle d'information et de sensibilisation du DPO ?	157
5. Quel est la mission du DPO face au principe de responsabilisation ?	160
Qu'est-ce qu'un sous-traitant ?	161
1. Comment identifier qui est sous-traitant au sens du RGPD ?	162
2. Que faire avec les sous-traitants identifiés ?	162
3. Que faire si un sous-traitant existant refuse de signer un contrat ?	162
4. Que faire pour de futurs sous-traitants ?	163
5. Quelle est la mission du DPO face aux sous-traitants ?	164
6. Comment gérer les aspects de confidentialité chez le sous-traitant ?	167
7. Comment identifier si un nouveau fournisseur est un sous-traitant ?	169
8. Que comprend un contrat de sous-traitance ?	169
9. Les contrats de sous-traitance sont-ils négociables ?	170
10. À quelle périodicité doit-on analyser les contrats de sous-traitance ?	172
11. Qui doit conserver la copie des contrats de sous-traitance ?	172
12. Que faire avec les sous-traitants non européens et en particulier les sous-traitants américains ?	172

Peut-on avoir des responsables de traitement successifs pour le même traitement de données ?	175
Qu'est-ce qu'une violation de données à caractère personnel ?	177
1. Comment mettre en place une procédure de gestion des violations de données ?	178
2. Comment informer le personnel en amont quant aux violations de données ?	180
3. Comment gérer un incident de sécurité ?	182
4. Quelles sont les décisions possibles en cas d'accident de sécurité ?	184
5. Comment anticiper une communication de crise en cas de perte de données ?	187
6. Comment rédiger le plan de gestion des incidents et le registre des incidents	188
Comment gérer le droit d'accès des personnes concernées ?	191
1. Modèle de gestion pratique des demandes de droit d'accès	193
2. Comment gérer le droit de rectification ?	195
3. Comment gérer le droit à l'effacement ?	195
Que doit faire le DPO pour la mise en place du registre des traitements ?	197
Comment aider le département des ressources humaines à se mettre en conformité ?	201
1. Pour les ressources humaines, sommes-nous face à la gestion de consentements ?	204
Le site internet	205
1. Combien de politiques de vie privées sont-elles nécessaires ?	205
2. Comment gérer les bases légales ?	206
3. Comment gérer les finalités ?	207
4. Comment conserver les preuves d'acceptation ou de prise de connaissance des politiques de vie privée ?	208
Privacy by design	209
Qu'est-ce qu'une analyse d'impact ?	211
1. Dans quels cas doit-on réaliser une analyse d'impact ?	212
2. Dans quels cas une analyse d'impact relative à la protection des données n'est-elle pas requise ?	215
3. Quel est le rôle du DPO quant à la nécessité de réaliser une analyse d'impact ?	219
4. Comment réaliser une analyse d'impact ?	222

5. Quel est le rôle du sous-traitant dans le cadre d'une analyse d'impact ?
6. Doit-on communiquer ou publier une analyse de risques ?
7. Que doit faire le DPO après avoir transmis son rapport ?
8. Faut-il refaire périodiquement les analyses d'impact ?

Quel est le rôle du DPO au sujet de l'archivage ?

Quel est le rôle du DPO en tant que point de contact pour les autorités nationales de protection des données ?

Quel est le rôle du DPO en tant que point de contact des personnes concernées ?

Quelle est l'obligation de confidentialité du DPO ?

Liste des abréviations

**Annexe 1 : Registre des traitements
– Contenu d'une fiche de traitements**

1. Informations valables pour tous les traitements
2. Fiche de traitement

Annexe 2 : Décision quant à la réalisation d'une Analyse d'impact quant à la protection des données (AIPD)

1. Réglementation
2. Description du traitement
3. Recommandation du DPO
4. Décision de la direction

Annexe 3 : Justification du recours à l'intérêt légitime pour un traitement de données

**Annexe 4 :
Les questions clés à se poser lors de la désignation d'un DPO**