DPO-Connect

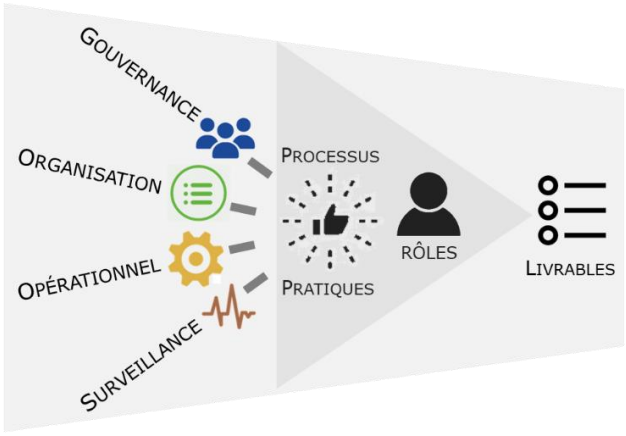
Renforcer la communication et la collaboration entre les DPO et l'APD à l'aide d'une plateforme digitale

Guide : Comment élaborer un programme de conformité au RGPD?

Florence de Villenfagne et Patrick Soenen

Co-funded by the European Commission

Le présent document est financé par le programme Droits, Égalité et Citoyenneté de l'Union européenne (2014-2020). Le contenu de ce livrable ne reflète que l'opinion de ses auteurs, sous leur responsabilité. La Commission européenne décline toute responsabilité quant à l'usage qui pourrait être fait des informations qu'il contient.



Comment élaborer un programme de conformité au RGPD?

Livrable D. 3.2

rédigé par DPO-pro dans le cadre du projet européen DPO-Connect[1]

3 juin 2022

Auteurs : Florence de Villenfagne et Patrick Soenen

Co-funded by the European Commission

DPO-Connect est un projet co-financé par la Commission Européenne (DG JUST) dans le cadre du programme Droits, Égalité et Citoyenneté de l'Union européenne (2014-2020).

Partenaires DPO-Connect : L'Autorité de Protection de Données belge (APD), l'Union professionnelle des DPOs de Belgique (DPO-pro) et la Vrije Universiteit Brussel (VUB)

[1] Le contenu de ce livrable ne reflète que l'opinion de ses auteurs, il n'est en aucun cas une prise de position officielle de la Commission européenne, de DPO-pro ou des autres partenaires du projet DPO-Connect. La Commission européenne et les auteurs déclinent toute responsabilité quant à l'usage qui pourrait être fait des informations qu'il contient.

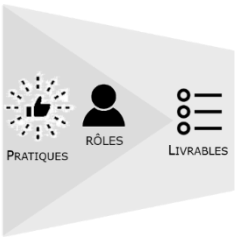
Préambule

Lorsqu'une juriste et un auditeur spécialisés en protection des données personnelles rédigent ensemble une étude sur un programme de mise en conformité au RGPD, le résultat est créatif et forcément différent de ce que l'on peut lire habituellement sur la mise en conformité au RGPD écrit par des juristes ou des spécialistes en sécurité.

L'idée de ce livrable est d'avoir un œil pratique et nouveau, de voir les choses d'un point de vue des responsabilités internes et de pouvoir ainsi aider concrètement les organisations à structurer leur mise en conformité au RGPD. Le Règlement Général sur la Protection des Données est un texte législatif trop général pour que les organisations puissent l'appliquer aisément. Comme les organisations structurent leurs activités en processus en précisant les rôles et les responsabilités des différents acteurs, cette publication a voulu transposer les exigences du Règlement en processus, accompagnés de matrices de responsabilités, en spécifiant les livrables ainsi générés.

Qui a la responsabilité des actions ? Qui doit agir ? Qui va apporter son aide et son conseil et qui doit absolument recevoir l'information pour que le RGPD soit finalement mis en place de façon efficace et pérenne ? Et quels livrables devraient sortir de l'exercice ? Voilà les questions auxquelles nous avons tenté de répondre.

Le cadre de référence des processus a été emprunté aux travaux réalisés par le groupe de travail RGPD de l'IFACI (Institut Français de l'Audit et du Contrôle Interne)[2], avec leur aimable autorisation.



Les pratiques, les matrices de responsabilités et les livrables ont été développés dans le cadre de cette publication.

Nous avons trouvé beaucoup de littérature qui explique le RGPD, présente les principes, détaille les obligations. Nous n'avions pas encore trouvé une présentation qui se place principalement du côté des rôles et responsabilités habituels dans les organisations.

Bien sûr notre travail est perfectible et nous n'assurons pas l'exhaustivité du résultat. Dans la logique de la méthodologie Plan-Do-Check-Act *qui nous est chère, nous serions d'ailleurs ravis d'avoir vos retours constructifs pour nous aider à compléter cette étude. En attendant, nous espérons que notre travail vous sera utile.*

Les auteurs

Florence de Villenfagne *Patrick Soenen*

[2] Cf. *Maîtriser et auditer les risques liés au RGPD*, **Groupe de travail RGDP de l'IFACI**, 2021, disponible pour les membres de l'IFACI uniquement. Le groupe de travail était composé de Qadir Abdul, Valérie Bonnel, Pascale Chabrillat-Trahin, Maud Choquenet, Gilles Le Beux, Marjorie Mengeaud et animé par Patrick Soenen.

Table des matières

1. Objectif et périmètre

L'objectif de la publication est de proposer l'ensemble des actions générales à réaliser par une organisation pour se mettre en conformité avec le RGPD dans une perspective des rôles et responsabilité des acteurs de l'organisation et des livrables à réaliser.

Le Règlement Général sur la Protection des Données3 (ci-après le « RGPD » ou « Règlement ») détermine les exigences en matière de protection des données à caractère personnel. Les lignes directrices du Comité Européen de la Protection des Données (« CEPD » ou « EDPB » en anglais) apportent des précisions concernant la compréhension des exigences, cependant elles n'expliquent pas comment mettre en œuvre de manière pratique ces exigences.

Cette publication propose un ensemble de processus qui sont structurés en 4 domaines : Gouvernance, Organisation, Gestion opérationnelle, Surveillance. Des (bonnes) pratiques[4] sont proposées pour chaque processus à mettre en œuvre au sein de l'organisation. Chaque pratique devra être détaillée en un certain nombre de tâches nécessaires pour les mettre en œuvre. Ces tâches ne sont pas reprises dans cette étude. Elles devront être définies en fonction de l'importance des traitements des données personnelles, du secteur d'activité, de la taille et de la structure interne de l'organisation, etc.

La publication ne prend pas en compte les spécificités découlant des législations nationales ou des déclinaisons en fonction de secteurs d'activité spécifiques, tels que, par exemple, les soins de santé qui impliquent le traitement d'une grande quantité de catégories particulières de données.

La mise en conformité au RGPD est un dispositif récent dans les organisations et cette mise en œuvre doit pouvoir s'intégrer et s'articuler dans les structures et les mécanismes de gouvernance et de contrôle en place. Son impact sur la gouvernance des données, la gestion des risques et la sécurité de l'information est conséquent et l'alignement continu avec les exigences réglementaires est incontournable.

En plus de la mise en place de la conformité, sa pérennité dans le temps doit être établie. Conformément au cycle de Deming, l'amélioration continue s'appuie sur 4 étapes :

- La planification, qui consiste à définir le travail à réaliser ;
- La réalisation, qui consiste à mettre en œuvre les activités ;
- Le contrôle, qui consiste à s'assurer que les activités se déroulent comme prévu ;
- L'action, qui consiste à ajuster le déploiement des activités.

2. Public visé

Ce guide est destiné principalement aux Délégués à la Protection des Données (DPO's) ou équivalents, mais également à toute personne concernée par la mise en œuvre du RGPD.

[3] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre à la libre circulation de ces données, et abrogeant la directive 95/46/CE

[4] Dans ce document, nous entendons par *'pratiques'*, les actions nécessaires pour atteindre l'objectif du processus.

3. Rôles et responsabilités

Par processus, et pour chaque pratique - une action contribuant à la réalisation de l'objectif du processus - une matrice de responsabilité est proposée en utilisant le modèle RASCI avec les définitions suivantes :

- ***R - Responsible* (Réalise)** : Le rôle qui réalise le travail pour accomplir l'activité. Un ou plusieurs rôles peuvent réaliser le travail
- ***A - Accountable* (Approuve et assume)** : Le rôle qui valide l'activité, rend des comptes et assume la responsabilité. Chaque pratique a une seule personne qui est « accountable », distincte de celles qui réalisent l'activité.
- ***C - Consulted* (Consulté)** : Le(s) rôle(s) qui est (sont) consulté(s) et fournit (fournissent) des informations.
- ***I - Informed* (Informé)** : Le(s) rôle(s) qui est (sont) tenu(s) au courant des résultats des activités.
- **S - *overSight* (Surveille)** : Le(s) rôle(s) qui vérifie(nt) la réalisation des activités et/ou le respect de la réglementation

Pour les organisations qui disposent de structures de gouvernance et de contrôle étendus, des pratiques spécifiques à ces structures sont proposées. Cependant les organisations qui ne disposent pas de fonctions spécifiques devront déterminer quel rôle exercera les responsabilités.

Les rôles suivants sont repris dans les matrices de responsabilité :

Rôle	Description
ACTEURS INTERNES	
Responsable du traitement (RT)	La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui détermine les finalités et les moyens du traitement[5].
Organe d'administration	Souvent dénommé conseil d'administration, celui-ci poursuit une création de valeur durable en arrêtant la stratégie de la société, en mettant en place un leadership effectif, responsable et éthique et en supervisant les performances de la société. Il approuve le cadre référentiel de contrôle interne et de gestion des risques proposé par le management exécutif et examine la mise en œuvre dudit cadre.[6]
Le management exécutif[7]	• Est en charge de la direction opérationnelle • Met en place des contrôles internes sur la base du cadre approuvé par l'organe d'administration • Soumet les états financiers et prépare leur publication réglementaire

[5] Voir la définition à l'article 4 (7) du RGPD
[6] Voyez *Le code belge de gouvernance d'entreprise*, Principe 2 Conseil – Stratégie – Surveillance, **Commission Corporate Governance**, 2020, (https://www.corporategovernancecommittee.be/assets/pagedoc/1327585529-1651062342_1651062342-code-belge-de-gouvernance-dentreprise-2020-0.pdf - consulté le 3 juin 2022)
[7] Cf. *Le code belge de gouvernance d'entreprise*, Principe 2 Management exécutif, **Commission Corporate Governance**, 2020, *op.cit.*

Rôle	Description
	• Fournit à l'organe d'administration les informations nécessaires à l'exercice de ses responsabilités • Rend compte à l'organe d'administration
Comité d'audit	Ce comité aide l'organe d'administration à veiller à l'exactitude et à la sincérité des comptes, ainsi qu'à la pertinence et à l'efficacité des systèmes de contrôle interne et de maîtrise des risques de l'organisation. Il assure le suivi de l'audit interne et du contrôle externe. Le Comité d'audit ou « d'audit et de gestion des risques »[8] est établi par l'organe d'administration.
Délégué à la Protection des Données (DPO) ou Privacy Officer (PO)	Le DPO est chargé d'informer et conseiller le responsable du traitement qui l'a désigné sur les obligations qui lui incombent en vertu du RGPD. Il a aussi un rôle de contrôle du respect du règlement. Alors que le DPO est un rôle défini par le RGPD, le Privacy Officer est un rôle non officiel et non défini par le Règlement. Si le Responsable du traitement a l'obligation de nommer un DPO en vertu du RGPD, il ne peut que le nommer « DPO » et celui-ci aura les fonctions et missions prévues par le RGPD. Si le Responsable du traitement n'a pas cette obligation, il peut tout de même choisir de nommer une personne en charge de vérifier le respect du RGPD et de le conseiller à ce sujet. Il peut l'appeler « PO » ou autrement. Le PO peut donc assurer des fonctions similaires au DPO ou seulement une partie de celles-ci. C'est au choix du Responsable du traitement. Si le Responsable du traitement n'est pas obligé de nommer un DPO, mais en nomme tout de même un en lui donnant le nom de « DPO », celui-ci devra répondre à tous les critères prévus par le RGPD pour le DPO (articles 37 et suivants du RGPD).
Référent RGPD	Collaborateur éventuellement désigné dans un département pour relayer les informations du DPO aux collaborateurs, les conseiller, veiller au respect des exigences RGPD au quotidien, appliquer le plan d'action et remonter les demandes ou incidents au DPO. Certains l'appellent autrement (« data steward », « privacy contact point » …). Nous avons décidé de l'appeler « référent RGPD ».
Responsable de la Sécurité des Systèmes d'Information (RSSI)	Personne responsable de la mise en œuvre de la politique de sécurité de l'information et de sa supervision. Les dénominations Conseiller en sécurité ou Chief Information Security Officer (CISO) sont également utilisés.
Département traitant des Données à Caractère Personnel (Dpt DCP)	Tout département qui traite des données à caractère personnel dans le cadre de ses activités opérationnelles.

[8] Cf. *Le code belge de gouvernance d'entreprise*, Principe 4 Comité d'audit. **Commission Corporate Governance**, 2020, *op.cit.*

Rôle	Description
Service juridique	Département chargé des questions de droit qui se posent dans une organisation. Certaines organisations nomment le DPO au sein du service juridique.
Direction Informatique (IT)	La Direction Informatique est responsable de la gestion des systèmes d'information de l'organisation. Elle a la charge de définir l'architecture du système d'information, de concevoir, installer et déployer et exploiter le système d'information. Dans ce cadre, elle intervient souvent dans la conception des solutions pour les traitements des données personnelles. Ces fonctions sont incompatibles avec celle du DPO.
Bureau Projet (*Project Management Office*) (PMO)	La structure organisationnelle qui centralise tout ou partie du pilotage et du support de la gestion des projets, des programmes, et des portefeuilles de projets de l'organisation.
Département des Ressources Humaines (RH)	Les services des ressources humaines se divise en deux activités principales, d'une part le côté administratif de la gestion des ressources humaines qui couvre la paie, les aspects juridiques, les contrats de travail… et d'autre part le développement des ressources humaines qui comprend la gestion des carrières, la gestion des compétences et des performances, le recrutement, la formation
Contrôle Interne (CI)	Dans les organisations où il existe, le Contrôle Interne a la responsabilité de la mise en place et la gestion d'un système de contrôle interne[9] qui comprend l'ensemble des moyens, comportements, procédures et actions, qui contribuent à la maîtrise des activités, à l'efficacité des opérations et à l'utilisation efficiente des ressources. Le Contrôle interne doit prendre en compte de manière appropriée les risques significatifs, qu'ils soient opérationnels, financiers ou de conformité.
Gestionnaire de la conformité (*Compliance Officer*)	Le Gestionnaire de la conformité gère et supervise le respect des lois et des règlements au sein de l'organisation. Il fait l'inventaire de exigences légales et réglementaires applicables. Il doit veiller à ce que les acteurs métier et de support aient la connaissance de ces exigences pour qu'ils s'y conforment de manière effective. Il fait du reporting à la direction, au régulateur, aux autorités. Il répond aux questions posées par le régulateur, dont il est le premier contact.
Gestionnaire des risques (*Risk Manager*)	Le gestionnaire des risques aide l'organisation à identifier ses risques. En appui du management, il contribue à la couverture et à la maîtrise de ces risques. Il met à disposition des métiers la méthodologie pour évaluer les risques. Il accompagne les métiers dans l'application de la

[9] Le référentiel de base est le COSO (référentiel américain de contrôle interne structuré en 5 composantes). Ce rôle existe surtout dans les grandes entreprises multinationales, le secteur financier… rarement dans les PME.

Rôle	Description
	méthodologie, collecte l'information, valide et fait du reporting au management. Il n'évalue pas le risque lui-même.
Audit interne (AI)	L'activité indépendante et objective pour donner l'assurance que les risques sont maîtrisés et apporter des améliorations aux opérations de l'organisation.
ACTEURS EXTERNES	
Autorité de Protection des Données (APD)	Autorité de contrôle, Autorité publique indépendante chargée de surveiller l'application du RGPD, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union[10].
Personne concernée	Personne physique identifiée ou identifiable[11] à laquelle se rapportent des données à caractère personnel
Sous-Traitant (ST)[12]	La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.
Sous-Traitant ultérieur	Le Sous-Traitant d'un Sous-Traitant (*sub-processor*) qui traite des données à caractère personnel pour le compte du Responsable du Traitement, mais sur la base d'un contrat conclu avec le Sous-traitant.

[10] Voyez l'Article 51 (1) du RGPD
[11] Voyez la définition à l'Article 4 (1) du RGPD
[12] Voyez la définition à l'Article 4 (8) du RGPD

4. Modèle des lignes de maîtrise

Dans les organisations disposant de structures de contrôle, le modèle des trois lignes de maîtrise aide les organisations à identifier les structures et les processus optimaux pour réaliser leurs objectifs et renforcer leurs dispositifs de gouvernance et de gestion des risques, également en matière de gestion des données à caractère personnel.

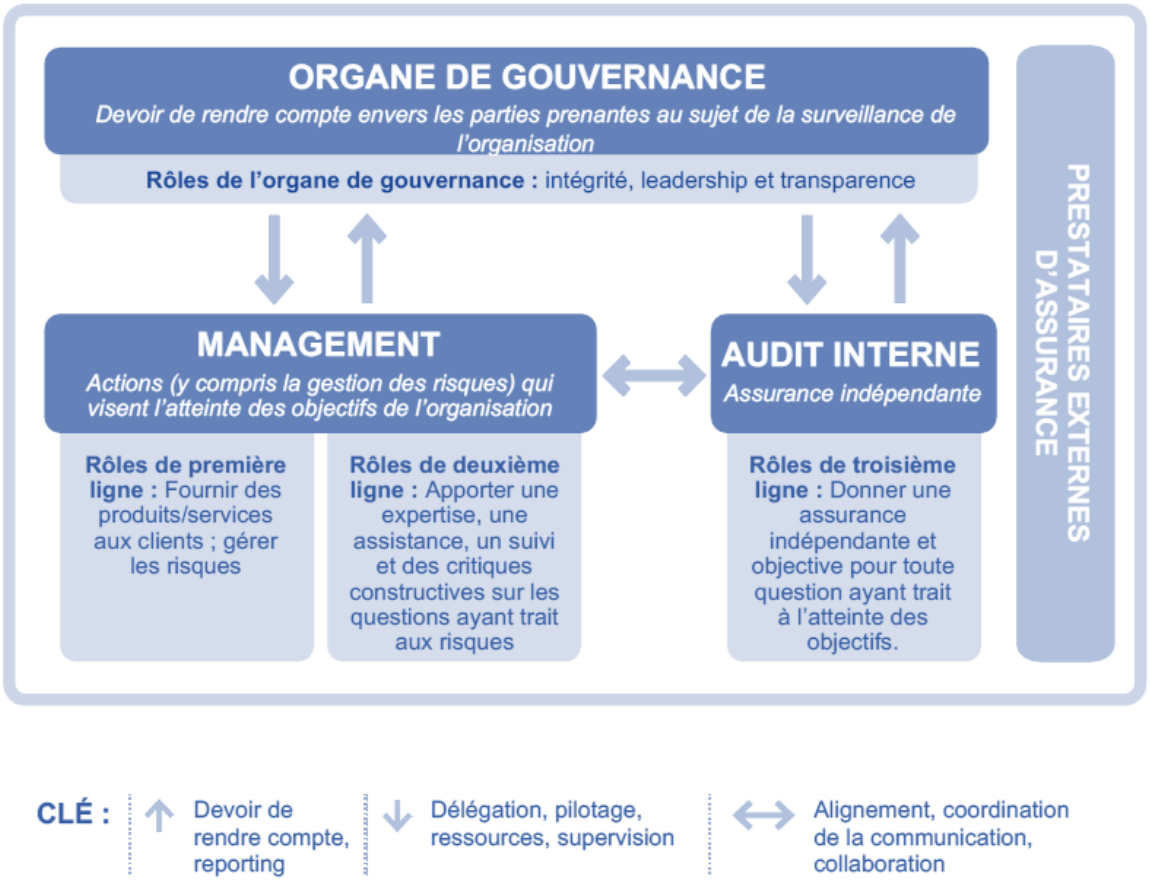


Schéma 1 - Modèle des 3 lignes de maîtrise[13]

La gouvernance d'une organisation doit reposer sur des structures et des processus appropriés en matière de gestion des données à caractère personnel permettant aux organes de gouvernance d'assumer leur devoir de rendre compte ; au management de mener les actions nécessaires pour réaliser les objectifs, grâce à une prise de décision fondée sur les risques et aux ressources disponibles ; et à une fonction d'audit indépendante.

En particulier, l'approche définit des tâches et responsabilités spécifiques à chaque ligne de maîtrise :

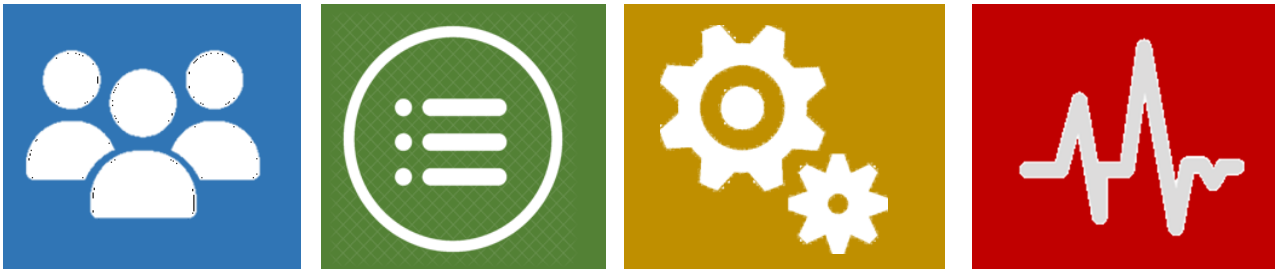
- Des activités de contrôle définies et mises en œuvre par les opérationnels, permettant, entre autres, la maîtrise des risques au jour le jour ;
- Un dispositif structuré et coordonné par la deuxième ligne de maîtrise, constituée des services fonctionnels responsables de domaines d'expertise et des fonctions dédiées à l'animation du dispositif global de maîtrise des risques (fonctions de gestion des risques, de contrôle interne, de conformité, le DPO, le RSSI[14], le responsable qualité...) ;

[13] Cf. *Le Modèle des Trois Lignes de l'IIA,* **The Institute of Internal Auditors,** 2020.
[14] Responsable de la Sécurité des Systèmes d'Information (ou CISO en anglais)

- Une évaluation globale et indépendante du dispositif conduite par la troisième ligne, assurée par la fonction d'audit interne indépendante et rattachée au plus haut niveau de l'organisation.

5. Les processus RGPD

La mise en œuvre d'un programme de mise en conformité au RGPD implique la mise en place de processus par toutes les parties prenantes concernées avec l'objectif de garantir une approche structurée couvrant les différentes exigences du RGPD. Ces processus peuvent être structurés en 4 domaines[15] :



A. Gouvernance	B. Organisation	C. Gestion opérationnelle	D. Surveillance
Rôles et responsabilités, organes de pilotage, politiques et directives qui permettent une gouvernance adéquate de la protection des données à caractère personnel au sein de l'organisation.	Mesures et processus à mettre en œuvre pour répondre aux exigences du règlement RGPD.	Processus et procédures à déployer pour rendre opérationnel la protection des données à caractère personnel de manière conforme au règlement RGPD.	Mécanismes de surveillance, de suivi, de revue et de contrôle du dispositif déployé selon les exigences du règlement RGPD et de ses lignes directrices. La surveillance vise à s'assurer que le dispositif fonctionne comme prévu et elle permettra de vérifier que la gestion du risque est efficace dans la durée.

Tableau 2 - Domaines des processus RGPD

Les 4 domaines se déclinent en 21 processus :

A. Gouvernance

- A1. Engagements du Responsable du Traitement (RT)
- A2. Politiques et organisation de la protection des données
- A3. Organes de gouvernance, rôles et responsabilités
- A4. Délégué à la Protection des Données (DPO)

B. Organisation du dispositif

- B1. Licéité du traitement (base légale & finalité)

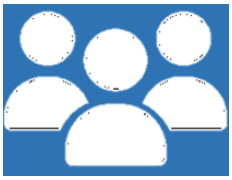
[15] La structure s'appuie sur celle développée dans la publication :
Maîtriser et auditer les risques liés au RGPD, **Groupe de travail RPGD de l'IFACI**, 2021. Document uniquement disponible aux adhérents de l'IFACI.

B2. Registre des activités de traitement
B3. Analyse d'impact relative à la protection des données (AIPD)
B4. Protection par conception et par défaut (« Data protection by Design/Default »)
B5. Utilisation et durée de conservation des données personnelles
B6. Gestion de la sous-traitance
B7. Transferts hors de l'Espace Economique Européen (EEE)
C. Gestion opérationnelle
C1. Pilotage et mise en œuvre
C2. Droits de la personne concernée
C3. Information et transparence
C4. Sensibilisation et formation
C5. Gestion de la continuité des activités et des services (PCA)
C6. Gestion et notification des violations des données personnelles
C7. Protection et sécurité des données personnelles
D. Surveillance et revue
D1. Suivi et revue du dispositif (par le DPO)
D2. Revue du dispositif RGPD (par les acteurs des lignes de maîtrise)
D3. Contrôle par l'Autorité de Protection de Données (APD)

Tableau 3 - Domaines et processus

Pour chaque processus, des (bonnes) pratiques sont proposées pour respecter les exigences du RGPD. Chaque pratique devra être détaillée en un certain nombre de tâches nécessaires pour les réaliser. Ces tâches ne sont pas reprises dans ce document. Elles devront être définies en fonction de la taille et la structure interne de l'organisation, l'importance des traitements des données personnelles, du secteur d'activité, etc.

A. Domaine de gouvernance



Les rôles et responsabilités, les organes de gouvernance, les politiques et lignes directrices permettent la mise en œuvre d'une gouvernance adéquate de la protection des données à caractère personnel au sein de l'organisation.

A1. Engagements du Responsable du Traitement (RT)

La mise en œuvre d'une gouvernance effective de la protection des données personnelles démarre au niveau des organes de gouvernance, notamment l'organe d'administration et la direction.

Bonnes pratiques et matrice des responsabilités :

La direction journalière désigne le rôle qui réalise (R) les pratiques.

Rôles / Pratiques	Responsable du traitement (RT)	[D]PO
Déterminer la nécessité ou non de nommer un DPO.	A	-
Désigner un Data Protection Officer (DPO) dans le respect des exigences du RGPD (indépendance, absence de conflit d'intérêt…) ou d'un Privacy officer (PO)[16]	A	-
Attribuer les moyens nécessaires permettant au [D]PO d'exercer adéquatement ses responsabilités dans l'optique d'une conformité au RGPD	A	C/I
Positionner adéquatement le [D]PO dans les structures organisationnelles donnant accès aux organes de direction (pour leur faire rapport directement) et disposant de l'autorité pour exercer ses responsabilités.	A	-
Formaliser les missions confiées au [D]PO : lettre de mission, engagement de confidentialité, budget, charge de travail, protection contre toute pénalisation pour l'exercice de ses missions…	A	C/I
Mettre à l'agenda des organes de direction le sujet de la protection des données personnelles.	A	C/I
Informer le [D]PO des sujets abordés aux comités de gouvernance, relatifs à la protection des données.	A	I
En cas de coresponsabilité dans le cadre d'un ou plusieurs traitements, signer une convention entre les coresponsables.	A	C

[16] Voyez l'explication de la différence entre « DPO » et « PO » à la section 3 – Rôles et responsabilités, où le terme « Délégué à la Protection des Données » est défini

Livrables

- Analyse de désignation d'un DPO
- Désignation du DPO par les organes de gouvernance
- Déclaration à l'APD
- Description de fonction du [D]PO
- Organigramme revu (comprenant le rôle de DPO)
- Contrat avec le DPO externe ou avenant au contrat de travail du DPO interne
- Budget DPO
- Extraits des procès-verbaux de organes de gouvernance et des pièces jointes, relatifs aux thèmes et traitements des données à caractère personnel
- Convention(s) de co-responsabilité

A2. Politiques de la protection des données

Art. 24.2

La gouvernance en protection des données personnelles et sécurité sera établie à l'aide de politiques adéquates approuvées par la direction et diffusées par les structures organisationnelles dans l'organisation.

Bonnes pratiques et matrice des responsabilités :

Rôles / Pratiques	Organe d' Administration	Responsable du traitement (RT)	[D]PO	RSSI	DRH	Dpt DCP
Adopter et mettre en place une politique (générale) interne (ou équivalent) de protection des données personnelles, qui définit la gouvernance de l'organisation en la matière.	A	R	C	C	C	
Approuver la politique interne.	A/R	R	C	C	C	
Établir et mettre en œuvre des politiques de protection des données personnelles, de sécurité des systèmes d'information (PSSI), des chartes de gouvernance des données	-	A	C	R	R/I	
Publier et communiquer les politiques aux parties prenantes	-	A	I	C	R/I	R/I
Intégrer la protection des données dans les contrats de travail et règlements d'ordre intérieur.	-	A	C	-	R	I

Livrables

- Politique générale de protection des données personnelles (gouvernance)
- Politique de Sécurité des Systèmes d'Information (PSSI) qui reflète la vision du Responsable du Traitement en matière de sécurité des systèmes d'information.
- Politiques spécifiques relatives à la protection des données et à la sécurité de l'information. Les politiques spécifiques couvrent le bon usage des moyens informatiques, la classification de l'information, la politique des habilitations, la gestion des mots de passe, l'utilisation de l'internet, du courriel et des médias sociaux, etc.
- Charte de gouvernance des données qui décrit les responsabilités et les pratiques de gestion des données dans le but d'assurer la qualité, l'intégrité, la disponibilité et la sécurité des données
- Plan de communication des chartes et politiques
- Articles du contrat de travail et/ou du règlement d'ordre intérieur intégrant l'obligation de respecter les politiques de sécurité et de protection des données personnelles

A3. Organes de gouvernance, rôles et responsabilités

Art. 24

Les organes de gouvernance « donnent le ton » dans l'organisation. Elles doivent s'engager à respecter les règles de protection des données et doivent en souligner l'importance auprès de toutes les parties prenantes susceptibles d'interagir avec ces données.

L'établissement des rôles et des responsabilités en matière de protection des données à caractère personnel au travers des canaux clairs de communication permet le déploiement des pratiques adéquates à tous les niveaux de l'organisation.

Bonnes pratiques et matrice des responsabilités :

Rôles / Pratiques	Direction journalière	Responsable du traitement (RT)	[D]PO	RSSI	PMO	Contrôle interne	Audit interne
Etablir des matrices de responsabilités pour les acteurs impliqués dans les activités relatives à la protection et à la sécurité des données personnelles.	R	A	C	C			
Intégrer la protection des données personnelles dans, par exemple, les : o Comités de gouvernance ou de pilotage des projets des systèmes d'information. o Comités de gouvernance de données. o Activités récurrentes de contrôle interne o Activités d'audit	-	A	C	- R - -	R R - -	- - R -	- - - R
Informer les organes de gouvernance de la mise en œuvre du respect de la protection des données personnelles.	A	I	R	C	C	C	C/(R)

Livrables

- Matrice des responsabilités (RACI)
- Extraits des procès-verbaux des comités y compris les pièces jointes, relatifs aux thèmes et traitements des données à caractère personnel
- Communications relatives au respect des règles de protection des données aux organes de gouvernance

A4. Délégué à la Protection des Données (DPO)

Art. 37-39

Détermination et établissement du [D]PO ou d'un « champion[17] » de la protection des données à caractère personnel au sein de l'organisation, en rendant compte de manière régulière au Responsable du Traitement.

Bonnes pratiques et matrice des responsabilités :

Rôles / Pratiques	Responsable du Traitement (RT)	[D]PO	RSSI	IT/PMO	Dpt DCP	Contrôle interne Audit interne	Personne concernée	APD
Communiquer les coordonnées du DPO aux autorités de contrôle.	A/R	I	-	-	-	-	-	I
Communiquer la nomination du DPO aux parties prenantes (tant au sein qu'à l'extérieur de l'organisation).	A/R	-	I	I	I	I	-	-
Désigner éventuellement des référents RPGD[18]	-	C	I	I	R	I	-	-
Donner accès au [D]PO à toutes les informations nécessaires pour l'exercice de sa fonction	A	I	R	R	R	R	-	-
Établir un rapport annuel à l'attention des organes de gouvernance.	A	R	C	C		C	-	-
Informer les acteurs traitant des données personnelles au sujet des exigences RPGD	I	A/R	I	I	I	I	-	-
Contrôler la conformité au RGPD	C/I	A/R	C/I	C/I	C/I	C/I	-	-
Conseiller les acteurs au sujet de la protection des données personnelles	I	A/R	I	I	I	I	-	-
Coopérer avec l'Autorité de Protection des Données et le point de contact pour les personnes concernées	C/I	A/R	C/I	C/I	C/I	C/I	C/I	C/I

Livrables

- Notification du DPO à l'APD
- Information de la nomination du DPO aux parties prenantes (internes et externes)
- Rapport annuel
- Avis et conseils du DPO
- Programme de contrôle du respect du RGPD (voir aussi D.1)

[17] Voyez l'explication sur la différence entre un DPO et un « PO » à la section 3 – Rôles et responsabilités.
[18] Voir la définition de ce rôle à la section 3 – Rôles et responsabilités.

B. Domaine d'organisation

Mesures et processus à mettre en œuvre pour répondre aux exigences du règlement RGPD.

B1. Licéité du traitement (base légale et finalité)

Art. 6

Toutes les données à caractère personnel doivent être traitées de manière licite, loyale et transparente vis-à-vis de la personne concernée, collectées et traitées à des fins déterminées, explicites et légitimes. Ci-dessous, les pratiques liées à la licéité. La transparence est reprise au point C.3.

Bonnes pratiques et matrice des responsabilités :

Rôles / Pratiques	Responsable du traitement (RT)	[D]PO	RSSI	IT/PMO	Dpt DCP
Déterminer les fondements légaux (ou bases de licéité) et les finalités de tous les traitements des données personnelles.	A	C			R
Recueillir les consentements de manière conforme au RGPD[19].	A	C	C/I	I/R	R
Organiser la sauvegarde des preuves de consentement.	A	C	C/I	R	R
Documenter l'obligation légale si c'est la base légale du traitement	A	C			R
Justifier l'intérêt public si c'est la base légale du traitement	A	C			R
Justifier l'intérêt légitime si c'est la base légale du traitement (« triple test[20] »)	A	C			R
Ajuster éventuellement les traitements pour se conformer aux finalités et au fondement légal, et l'arrêt des traitements non conformes ou sans base de licéité.	A	C		I/R	R
Mettre en œuvre le principe de minimisation lors de la collecte des données (en fonction de la finalité du traitement). Voir aussi B.4.	A	C		I/R	R

[19] Il faudra aussi prévoir la possibilité du retrait des consentements à la demande des personnes concernées (voir le point C.2)
[20] Tests de finalité, de nécessité et de pondération

Livrables

- Inventaire des traitements, de leur finalité et des bases de licéité
- Procédure d'obtention, de conservation de preuve (et de retrait du consentement)
- (Modèle de) justification de l'intérêt légitime
- (Modèle de) justification de l'intérêt public (le cas échéant)

B2. Registre des activités de traitement

Art. 30

Les activités de traitement des données à caractère personnel sont reprises dans un registre.

Bonnes pratiques et matrice des responsabilités :

Rôles / Pratiques	Responsable du traitement (RT)	[D]PO	Référent RGPD	Dpt DCP
Inventoriser les traitements de données à caractère personnel existants	A	C	C	R
Créer le registre « Responsable de traitement » et/ou le registre « Sous-Traitant »	A	R	C	C
Déterminer et mettre en place une procédure de mise à jour du(des) registre(s)	A	R	I	I
Déterminer la nécessite d'inclusion des traitements dans le registre (art. 30.5 RGPD)	A	C	C	R
Déterminer l'affectation des traitements au registre « Responsable de Traitement » ou « Sous-Traitant ».	A	C	C	R
Organiser la formation et l'accompagnement éventuel des référents RGPD[21].	A	R	I	
Collecter l'ensemble des informations requises pour le registre	A	C	R/C	R
Mettre en œuvre une procédure de revue régulière du registre	A	C	C	R

Livrables

- Inventaire des traitements de données et toutes les informations les concernant
- Registre de responsable du traitement avec les informations requises par l'article 30 du RGPD –mis à jour
- Registre du sous-traitant, le cas échéant, avec les informations requises par l'article 30 du RGPD –mis à jour
- Procédure de mise à jour du (des) registre(s)
- Formation des référents DPO pour aider à compléter le registre

[21] Les référents doivent pouvoir conseiller les départements dans l'identification des traitements et aider pour la collecte des informations requises dans le registre

B3. Analyse d'impact relative à la protection des données (AIPD)

Art. 35

Assurer la réalisation d'analyses d'impact des opérations de traitement envisagées susceptibles d'avoir un risque élevé pour les droits et libertés des personnes concernées, afin de s'assurer que les risques d'atteinte à ces droits et libertés soient atténués.

Bonnes pratiques et matrice des responsabilités :

Rôles / Pratiques	Responsable du traitement (RT)	[D]PO	Référent RGPD	RSSI	Dpt DCP	Responsable projet[22]	APD
Déterminer les traitements éligibles à une AIPD, sur la base de l'article 35 du RGPD et notamment en appliquant les critères édictés par le CEPD[23] et les Autorités de contrôle compétentes (comme l'APD, par exemple).	A	C/R	R	C	R/C	C	
Déterminer et mettre en place une méthodologie de réalisation des AIPD	A	R/C	C	R/C			
Éventuellement, sélectionner et mettre en place un outil pour réaliser des AIPD	A/R	C					
Établir le planning de réalisation des AIPD	A	C/R	C	C	R	C	
Réaliser l'AIPD[24] et rédiger le rapport	A	C	C	C	R/C	C/I	
Identifier les mesures pour mitiger les risques et établissement d'un plan d'action, le cas échéant	A	C	I	R	R	R	
Mettre en œuvre le plan d'action et en assurer le suivi	A	I	I	R	R	R	
Consulter l'APD en cas de risques résiduels élevés	A	R					C

Livrables

- Liste des traitements éligibles à une AIPD
- Méthodologie AIPD
- Outil AIPD, éventuellement
- Planning de réalisation des AIPD
- AIPD, contenant par analyse réalisé les éléments suivants : Présentation du (des) traitement(s) considéré(s), liste de mesures mises en œuvre, évaluation et cartographie des risques, décision argumentée, éventuellement le plan d'action
- Plan d'action et suivi de réalisation : mesures, responsables, échéances
- Avis émis par l'APD, en cas de consultation pour risques résiduels élevés

[22] Dans le cadre d'un nouveau projet.
[23] Comité européen à la protection des données (*European Data Protection Board*)
[24] Pour une étude plus détaillée concernant les étapes de l'AIPD, consultez
Les guides AIPD de la CNIL, 2018, https://www.cnil.fr/fr/guides-aipd (consulté le 3 juin 2022)

B4. Protection dès la conception et par défaut (« *Data protection by Design/Default* »)

Art. 25

Veiller à ce que, dès la conception des activités de traitement des données à caractère personnel, les mesures techniques et organisationnelles appropriées soient prises ou prises en compte pour protéger de manière adéquate et réduire au minimum les données à caractère personnel.

Bonnes pratiques et matrice des responsabilités :

Rôles / Pratiques	Responsable du traitement (RT)	[D]PO	Référent RGPD	RSSI	IT/PMO	Dpt DCP	Responsables projet	Comité de pilotage
Définir une procédure/méthodologie de « Data protection by Design/Default » pour le respect dès la conception et par défaut des principes du RGPD (dont le principe de minimisation, par exemple)	A	C	C	C	C	R	C	I
Intégrer la procédure dans la méthodologie de gestion de projets	A	I	I	I	R	I	I	I
Former les chefs de projet et les acteurs clés à la méthodologie	A	C/I	C/I	I	R	I	I	I
Mettre en œuvre la méthodologie dans le cadre des projets traitant des données à caractère personnel	A	I	I	C	C	C/R	R	I
Revoir les résultats des analyses « Data protection by Design/Default »[25]	A	I	I	I	I	I	I	R
Déterminer les actions à mettre en œuvre	A	I/C	I/C	R	I	R	R	C/I
Mettre en œuvre le plan d'action et en assurer le suivi	A	I	I	R	I	R	R	I

Livrables

- Procédure / Méthodologie de gestion « Data protection by Design/Default »
- Support de formation à l'approche et la procédure de gestion « Data protection by Design/Default », éventuellement intégré dans les supports de formation à la méthodologie de gestion de projets
- PV des réunions avec le DPO sur le résultat des analyses « Data protection by Design/Default »
- Plan d'action des mesures à mettre en œuvre, par projet
- Suivi des plans d'actions : mesures, responsables, échéances

[25] Quand une nouvelle solution est conçue, une bonne pratique est de consulter le DPO sur la bonne application des principes DPbD/DPbDf. En général, on prévoit une réunion avec les concepteurs (ex : IT, le PMO) et le DPO pour qu'il puisse prendre connaissance de l'analyse réalisée dans le cadre du projet.

B5. Utilisation et durée de conservation des données personnelles

Art. 5.2 e)

Les données à caractère personnel doivent être utilisées pour la finalité pour la laquelle elles ont été collectées et ne pas être traitées ultérieurement d'une manière non compatible avec ces finalités. Elles ne peuvent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées, sauf justification complémentaire.

Bonnes pratiques et matrice des responsabilités :

Rôles / Pratiques	Responsable du traitement (RT)	[D]PO	Référent RGPD	IT/PMO	Dpt DCP
Inventoriser les (catégories de) données personnelles traitées par l'organisation – organisées par finalité de traitement (issu du registre)	A	C	C	C	R
Déterminer les durées de conservation des données selon la nécessité[26] (durée fixe ou dépendant de la réalisation d'un facteur)	A	C	C	I	R
Déterminer ce qu'il advient des données après la durée de conservation définie[27]	A	C	C	R/C	R
Mettre en œuvre les durées de conservation fixées (dans les systèmes informatiques, dans les systèmes de conservation des documents papiers, dans l'organisation des accès aux données)	A	C	C	R/C	R
Fournir les instructions de mise en œuvre des durées de conservation aux Sous-Traitants	A	C	C	R/C	R
Placer l'information concernant la durée de conservation dans le registre (ou faire un renvoi dans le registre vers cette information)	A	C	C	-	R

Livrables

- Document(s) reprenant les durées de conservation des données en fonction des finalités et les systèmes informatiques dans lesquels se trouvent ces données
- Instructions de mise en œuvre pour les Sous-Traitants

[26] Dans le respect du principe de minimisation
[27] Suppression ou conservation pour une autre finalité (licite)

B6. Gestion de la sous-traitance

Art. 28

Les activités des Sous-Traitants ainsi que des Sous-Traitants ultérieurs seront effectuées pour le compte du Responsable du Traitement et les responsabilités et obligations seront définies dans un contrat de sous-traitance conforme à l'article 28 du RGPD.

Bonnes pratiques et matrice des responsabilités :

Rôles / Pratiques	Responsable du traitement (RT)	[D]PO	Référent RGPD	RSSI	IT/PMO	Dpt DCP	Service juridique
Créer un modèle de contrat de sous-traitance incluant les clauses de l'article 28 du RGPD (ou utilisation du modèle européen) -	A	C/R					R
Inclure dans le modèle de Cahier Spécial des Charges les dispositions relatives au RGPD (uniquement valable pour les entités soumises à la règlementation des marchés publics)	A	C/R					R
Inventoriser les sous-traitants (ST) et identifier les traitements dans lesquels ces sous-traitants sont impliqués	A	C	C/R			R	
Inventoriser les contrats avec les ST et les clauses liées au RGPD incluses dans ces contrats	A	C	C/R			R	C/R
Déterminer les mesures de sécurité à imposer aux ST en fonction de la nature des données qu'ils traitent pour le compte du RT, des risques…	A	C		R		(R)	
S'assurer des garanties[28] qu'offre le ST pour respecter le RGPD dans le cadre du traitement dans lequel il intervient, des données qu'il traite pour le compte du RT et du risque pour les droits et libertés de la personne concernée	A	C	C/R	C		R	
Conclure les contrats de sous-traitance	A	C	C			R	C
Mettre en place d'une procédure de vérification et de suivi du respect des engagements du ST (« garanties suffisantes »), (programme d'audit)	A	C					
Inventoriser le lieu où les données sont traitées par le sous-traitant ou à partir d'où les données sont accessibles (identification de transferts vers des pays tiers - voir B.7)	A	C	C/R			R	
Reprendre les ST dans le registre (« destinataires »)	A	C	C/R			R	

[28] Le responsable du traitement « fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée. » Article 28.1 RGPD.

Livrables

- Modèle de contrat de sous-traitance article 28 RGPD (*Data processing Agreement)*
- Liste de mesures de sécurité techniques et organisationnelles que l'on pourrait imposer aux ST en fonction des circonstances (de la nature des données, des risques, de l'état de la technique, des coûts)
- Inventaire des ST
- Inventaire des contrats avec les ST et des clauses de protection de données incluses dans ces contrats
- Inventaire des transferts vers des « pays tiers » (voir B.7)
- Programme d'audit des ST

B7. Transferts hors de l'Espace Economique Européen (EEE)[29]

Chap V

Tout transfert de données à caractère personnel vers un pays tiers hors de l'EEE ou vers une organisation internationale doit respecter des garanties prévues par le RGPD.

Bonnes pratiques et matrice des responsabilités :

Rôles / Pratiques	Responsable du traitement (RT)	[D]PO	Référent RGPD	RSSI	IT/PMO	Dpt DCP
Inventoriser les transferts de données personnelles vers des « pays tiers » (hors de l'Espace économique européen) – voir B.6	A	C	C/R			R
Déterminer si les données sont envoyées vers un ST ou un RT	A	C/R	C/R			C
Déterminer la garantie qui permet le transfert (pays offrant une protection adéquate[30], garanties appropriées qui ne nécessitent pas d'autorisation de l'autorité de contrôle (Clauses contractuelles types et mesures additionnelles de protection ; Règles d'Entreprise Contraignantes…)[31], garanties appropriées qui nécessitent une autorisation de l'autorité de contrôle (clauses spécifiques…)[32], dérogations pour des situations particulières[33], ou des motifs légitimes impérieux[34]	A		C/R			R
En cas d'utilisation de Clauses Contractuelles Types • Réaliser une analyse de risques pour le transfert (DTIA)[35] et adopter des mesures additionnelles de protection en fonction du résultat • Vérifier si le nouveau modèle de clauses de juin 2021 est utilisé[36] ou s'il s'agit encore des anciennes clauses • Utiliser les nouvelles Clauses Contractuelles Types pour tout nouveau contrat depuis le 27 septembre 2021[37] • Lors de l'utilisation des nouvelles Clauses, déterminer le module à utiliser en fonction du type de transfert (transfert entre un RT et un ST, entre RT, entre ST, ou entre un ST et un RT)	A	C	C/R	C		R C R

[29] Les règles de protection des données s'appliquent à l'Espace Économique Européen, comprenant, outre les pays de l'Union Européenne, l'Islande, le Liechtenstein et la Norvège.
Cf: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/rules-international-data-transfers_fr
[30] Article 45 RGPD
[31] Article 46.2 RGPD
[32] Article 46.3 RGPD
[33] Article 49 RGPD
[34] Article 49.1§2 RGPD
[35] TIA ou DTIA – (data) transfer impact assessment
[36] https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX:32021D0914&locale=fr (consulté le 3 juin 2022)
[37] Les anciennes clauses doivent être remplacées par les nouvelles Clauses Contractuelles Types avant le 27 décembre 2022

Livrables

- Liste des transferts vers des pays tiers et les garanties utilisées
- Inventaire des contrats où les anciennes clauses contractuelles types sont encore utilisées
- Modèle de DTIA
- DTIA lors de l'utilisation de clauses contractuelles types pour le transfert

C. Domaine de gestion opérationnelle

Processus et procédures à déployer pour rendre opérationnel la protection des données à caractère personnel de manière conforme au RGPD.

C1. Pilotage et mise en œuvre

Art. 24

Mise en place d'un pilotage disposant des moyens nécessaires et des compétences requises pour garantir la mise en œuvre opérationnelle du dispositif RGPD.

Bonnes pratiques et matrice des responsabilités :

Rôles / Pratiques	Responsable du traitement (RT)	[D]PO	Référent RGPD	RSSI	IT/PMO	Dpt DCP
Établir un programme de mise en conformité au RPGP	A	R/S[38]	C/I	C/I	R	C/I
Désigner l'équipe de gestion du programme	A/R	I	I	I	I	I
Prioriser et planifier les activités de mise en conformité	A	R/S[39]	C/I	C/I	R	C/I
Animer le réseau de référents RGPD pour le déploiement du dispositif de mise en conformité	A	R	C	C	R	
Organiser les processus internes pour garantir la prise en compte de la protection des données	A	C/S	C	C	R/C	R
Gérer les risques liés aux traitements des données à caractère personnel	A	C/S	C	C	C	R
Déterminer les indicateurs et les tableaux de bord de suivi de de mise en conformité au RGPD	A	R/S	C/I	C/I	R	C/I

Livrables

- Programme de mise en conformité au RGPD
- Documentation du programme RGPD : objectif, ressources, budget, échéance, risques, suivi
- PV des réunions de pilotage
- Descriptions et mise à jour des processus et des procédures
- Registre des risques
- Indicateurs de suivi
- Tableau de bord de suivi de la mise en œuvre

[38] La CNIL mentionne le DPO en tant que pilote / chef d'orchestre (- consulté le 3 juin 2022)
[39] Idem

C2. Droits de la personne concernée

Art. 12-23

Le Responsable du Traitement doit mettre en œuvre des processus et procédures pour permettre l'exercice des droits d'accès, de rectification, d'effacement, d'opposition, de limitation du traitement et pour garantir la portabilité des données à caractère personnel de la personne concernée.

Bonnes pratiques et matrice des responsabilités :

Rôles / Pratiques	Responsable du traitement (RT)	[D]PO	Référent RGPD	IT/PMO	Dpt DCP
Déterminer les droits applicables (en fonction des bases légales)	A	C			R
Établir un répertoire d'enregistrement des requêtes	A	R	C/R		C/R
Définir et mettre en œuvre les procédures pour répondre à l'exercice de chacun des droits, en fonction de la catégorie de personnes concernées [40]	A	S/C	C	C	R
Déterminer les mesures à mettre en place pour l'authentification des demandeurs	A	S/C	C		R
Inventoriser les systèmes dans lesquels des données personnelles sont reprises et déterminer la manière dont on peut respecter la demande dans chacun des systèmes	A	S/C	C	R/C	R/C
En cas de demande d'effacement des données, déterminer la procédure pour vérifier si les données peuvent effectivement être effacées et réaliser l'effacement le cas échéant.	A	S/C	C	R/C	R/C
Former le personnel qui répond aux demandes d'exercice des droits (front office, service de support…)	A	S/C	C		R
Établir la procédure encadrant la gestion d'une plainte	A	S/C	C		R
Réaliser des indicateurs clés et/ou de rapports d'analyse et de suivi des requêtes	A	R	C/I		C/I

[40] Le cas échéant, mise en œuvre d'un portail de self-management pour les personnes concernées.

Livrables

- Par catégorie de personne concernée (clients/citoyens/patients/employés/ fournisseurs), procédure de gestion de chacun des droits applicables
  - Accès (y compris communication d'information et copie de données)
  - Rectification
  - Effacement
  - Droit à l'oubli
  - Limitation du traitement
  - Portabilité
  - Opposition
  - Retrait de consentement
  - Décision individuelle automatisée
- Procédure d'authentification de la personne qui demande l'exercice de ses droits
- Inventaire des systèmes avec modalités de réalisation des requêtes
- Procédure de gestion des plaintes
- Matériel de formation du personnel
- Indicateurs et rapports de suivi

C3. Information et transparence

Art. 12-14

Il convient de mettre en œuvre des mesures appropriées pour fournir aux personnes concernées les informations requises sur le traitement des données à caractère personnel les concernant.

Bonnes pratiques et matrice des responsabilités :

Rôles / Pratiques	Responsable du traitement (RT)	[D]PO	Référent RGPD	DRH	Dpt DCP
Déterminer les catégories de personnes concernées à informer	A	C	C	R	R
Déterminer les canaux de collecte et de communication appropriés avec ces personnes concernées (site web, intranet, charte interne, annexe contrat de travail, règlement de travail…)	A	C	C	R	R
Par catégorie de personnes concernées, identifier les traitements les concernant (à reprendre du registre)	A	C	C	R	R
Inclure la durée de conservation des données dans l'information à la personne concernée	A	C	C	R	R
Développer une « déclaration de confidentialité » ou une « charte de respect de la vie privée » qui reprend les informations des articles 13 ou 14 du RGPD	A	C	C	R	R/I
Publier et communiquer les chartes aux parties prenantes	A	C	C	R	R/I
En cas de collecte directe, informer les personnes concernées des traitements au moment de la collecte (voir informations à communiquer à l'article 13 du RGPD).	A	C			
En cas de collecte indirecte, informer le plus rapidement possible, et au plus tard lors de la première communication, mais toujours dans le mois (voir les informations à communiquer à l'article 14 RGPD)	A	C			

Livrables

- « Déclaration de confidentialité » ou « charte de protection des données personnelles », publiée notamment sur le site internet
- Liste des canaux de collecte et de communication avec les personnes concernées
- Liste des traitements par personne concernée
- Information interne (pour les employés et les collaborateurs internes)

C4. Sensibilisation et formation

Art. 24

Organisation des activités de sensibilisation et de formation des collaborateurs (internes et externes) de manière régulière concernant la compréhension des traitements, les risques, les mesures de protection des données et les droits des personnes concernées.

Bonnes pratiques et matrice des responsabilités :

Rôles / Pratiques	Responsable du traitement (RT)	[D]PO	Référent RGPD	RSSI	IT/PMO	RH	Dpt DCP
Déterminer les catégories de public cible et définir par catégorie : les besoins de sensibilisation ou de formation en la matière	A	R/S	C	C	C	R/C	R/C
Préparer les sensibilisations et les formations	A	R/S	C	R	C	R	C
Organiser les formations par catégorie de public cible	A	R/S	R	I	(R)	I	R
Conserver les preuves de sensibilisation et de formation, et la liste des personnes qui en ont bénéficié	A	R/S	R		C	C	C
Mettre à jour ou répéter les sensibilisations/formations et conservation des preuves	A	R/S	C	R	C	R	C
Réaliser des tests ou quiz réguliers de vérification des connaissances	A	R/S	C	C		C	I

Livrables

- Matrice des besoins en sensibilisation et formation – par public cible
- Supports de sensibilisation (RGPD et sécurité)
- Supports de formation (RGPD et sécurité)
- Preuves de suivi de formations
- Preuve de sensibilisation de publics cibles
- Preuve de mise à jour et formation/sensibilisation continuée
- Résultats des tests de connaissance

C5. Gestion de la continuité des activités et des services (PCA)

Art. 32

Des mesures appropriées seront mises en place pour assurer la continuité des activités relatives aux données à caractère personnel à l'égard des personnes concernées.

Bonnes pratiques et matrice des responsabilités :

Rôles / Pratiques	Responsable du traitement (RT)	[D]PO	Référent RGPD	RSSI	Gestionnaire de continuité d' activité[41]	Dpt DCP
Identifier les besoins de continuité dans les traitements des DCP, notamment en établissant un Bilan d'Impact sur l'Activité (BIA)	A	C/I	C	C	R	C
Évaluer les risques en termes de continuité et établissement des interruptions maximales de service (RTO) et des pertes maximales de données personnelles (RPO)	A	C/I	C	C	R	C
Intégrer les actions de continuité et de restauration des DCP dans le Plan de Continuité d'Activité (PCA)	A	C/I	C	C	R	C
Former au Plan de Continuité d'Activité	A	I	I	C	R	I
Exercer et tester le Plan de Continuité d'Activité	A	C/I	C	R	R	R
Revoir et améliorer le Plan de Continuité d'Activité	A	C/I	C	C	R	C
Gérer les dispositifs de sauvegarde (backups)	A	C/I	C	C	R	C
En cas de restauration, réaliser un examen post-reprise.	A	C/I	C	C	R	C

[41] La fonction de gestionnaire de continuité d'activité est souvent combinée avec celle du RSSI.

Livrables

- Bilan d'Impact sur l'Activité
- Évaluation des risques de continuité y compris RTO et RPO
- Plan de Continuité d'Activité (PCA)
- Plan de formation du PCA
- PV du test du Plan de Continuité d'Activité
- Action d'amélioration du Plan de Continuité d'Activité
- Plan de sauvegarde (Backups)
- Compte rendu de l'examen post-reprise

C6. Gestion et notification des violations des données personnelles

Art. 33-34

Les mesures nécessaires pour assurer une gestion efficace des violations des données personnelles seront mises en place.

Bonnes pratiques et matrice des responsabilités :

Rôles / Pratiques	Responsable du traitement (RT)	[D]PO	Référent RGPD	Gestionnaire d'incidents[42]	RSSI	Dpt DCP
Déterminer et mettre en place une procédure de gestion des violations de données personnelles (depuis la détection, la signalisation, l'identification de la violation, à la prise de mesures pour limiter les conséquences et l'impact, la notification éventuelle à l'autorité de protection de données et/ou aux personnes concernées, l'analyse des causes pour tenter d'éviter toute nouvelle occurrence et l'évaluation de la gestion)	A	R/S	C	C/I	C/I	C/I
Créer et mettre en place (et mettre à jour) un registre interne des violations	A	R/S	C	R	R/C	C
Mettre en œuvre des mécanismes de détection des incidents par surveillance et déclaration des incidents [43]	A			R		
En cas de suspicion d'une violation : • Recueillir les informations pertinentes • Analyser pour vérifier l'occurrence d'une violation et la qualifier (implication de données personnelles, gravité, étendue) • Documenter l'incident • Déterminer les réponses (mesures)	A	C	C	R	C	C
En cas de violation : • Déterminer la nécessité de notifier l'APD et éventuellement les personnes concernées • Notifier l'APD si nécessaire • Notifier les personnes concernées si nécessaire	A	R C C	C	C R R	C	I (R) R
S'assurer de la communication des violations par le ST dans les délais requis pour la notification	A	R				
Tirer les leçons et les retours d'expérience des incidents et violations pour une amélioration continue	A	R/C	C	R	R	C

[42] Le rôle de gestionnaire des incidents peut être assigné au RSSI, à un expert informatique ou à une fonction dédicacée en fonction de la taille et de la structure de l'organisation.

[43] L'identification doit s'intégrer dans les processus de gestion des incidents de l'organisation.

Livrables

- Registre interne des violations
- Méthode d'évaluation du risque pour les personnes concernées en cas de violation de données personnelles
- Modèle de questionnaire pour obtenir toutes les informations nécessaires en cas de (suspicion de) survenance d'une violation de données
- Modèle de rapport de gestion de l'incident (la violation) incluant les mesures prises pour limiter les conséquences de l'incident (et de nouvelles occurrences).
- Notification à l'APD et/ou à la personne concernée

C7. Protection et sécurité des données personnelles

Art. 32

Les mesures organisationnelles et techniques appropriées seront mises en place pour protéger les données à caractère personnel des personnes concernées de manière appropriée.

Bonnes pratiques et matrice des responsabilités :

Rôles / Pratiques	Responsable du traitement (RT)	[D]PO	Référent RGPD	RSSI	IT/PMO	Dpt DCP
Intégrer les dispositifs de protection des données personnelles dans le Système de Gestion de la Sécurité de l'Information (SGSI)	A	C	C	R	C	C
Identifier, par traitement de données, les mesures organisationnelles et techniques appropriées[44]	A	C	C	R	C	C
Etablir des mesures des protection et de sécurité, y compris les mesures de prévention de pertes de données et de cyber protection	A	C	C	R	C	I
Etablir des procédures de sécurité	A	C	C	R	C	C
Communiquer et conscientiser aux mesures de protection et de sécurité	A	C/R	R	R	I	I
Mettre en œuvre la traçabilité des accès/modifications/autres traitements des DCP	A	C	C	R	R	I
Surveiller la mise en œuvre des mesures de protection et de sécurité	A	R	R	R	C	C
Revoir les mesures de protection et de sécurité	A	C/I	C	R	C	C

Livrables

- Système de Gestion de la Sécurité de l'Information (SGSI)
- Mesures organisationnelles et techniques de protection par traitement DCP, par exemple habitations, transmissions de données…
- Communication des mesures de protection et de sécurité des données personnelles
- Analyse du traçage des activités.
- PV de la revue des mesures de protection et de sécurité des données personnelles

[44] À définir en tenant compte de la nature des données, des risques pour les droits et libertés, des coûts de mise en œuvre, de l'état des connaissances, du contexte et des finalités du traitement – article 32 du RGPD.

D. Domaine de surveillance et revue

Mécanismes de surveillance, de suivi, de revue et de contrôle du dispositif déployé pour répondre aux exigences du RGPD et des lignes directrices adoptées à ce sujet.

La surveillance vise à s'assurer que le dispositif fonctionne comme prévu et elle permettra de vérifier que la gestion du risque est efficace dans la durée.

D1. Suivi et revue du dispositif (par le DPO)

Art. 39.1

Le DPO suit de manière continue le respect du RGPD au sein de l'organisation. Il organise des revues régulières, afin de garantir une conformité dans la durée.

Bonnes pratiques et matrice des responsabilités :

Rôles / Pratiques	Responsable du traitement (RT)	[D]PO	Référent RGPD	RSSI	IT/PMO/ Dpt DCP	Contrôle interne[45]	Gestionnaire des risques[46]	Gestionnaire de la conformité[47]	Audit interne
Revoir de manière régulière et planifiée l'adéquation conceptuelle[48] des pratiques de mise en conformité avec le RGPD	A	R	R	C	C	C	C	C	I
Revoir de manière régulière et planifiée l'efficacité des pratiques (*l'adéquation opérationnelle*[49]) de mise en conformité avec le RGPD (contrôles de 1er niveau - opérations)[50]	A	R	R	C	C	-	-	-	I
Revoir de manière régulière et planifiée les activités de support à la mise en œuvre du RGPD (2ième ligne de maîtrise)[51]	A	R	R	C	-	C	C	C	I
Déterminer les plans d'action et d'amélioration	A	R	C	C/I	C/I	C/I	C/I	C/I	I

[45] Voyez la définition du rôle du Contrôle interne à la section 3 – Rôles et responsabilités
[46] Voyez la définition du rôle du gestionnaire des risques (Risk Manager) à la section 3 – Rôles et responsabilités.
[47] Voyez la définition du rôle du gestionnaire de conformité (Compliance Officer) à la section 3 – Rôles et responsabilités.
[48] *L'adéquation conceptuelle* consiste à s'assurer que les pratiques ont été conçues de manière conforme aux exigences du RGPD.
[49] *L'adéquation opérationnelle* consiste à s'assurer que la mise en œuvre des pratiques se réalise de manière conforme aux exigences du RGPD, et que les mesures de contrôle fonctionnent de manière à permettre une maîtrise des risques.
[50] Voyez le schéma 1, à la section 4 - Modèle des 3 lignes de maîtrise
[51] Voyez le schéma 1, à la section 4 - Modèle des 3 lignes de maîtrise

Rôles / Pratiques	Responsable du traitement (RT)	[D]PO	Référent RGPD	RSSI	IT/PMO/ Dpt DCP	Contrôle interne[45]	Gestionnaire des risques[46]	Gestionnaire de la conformité[47]	Audit interne
Rapporter au Responsable du Traitement les conclusions des revues	A/I	R	C	I	-	I	I	I	I

Livrables

- Documents de revue : évaluation de la conception et efficacité des évaluations
- Plans d'action et d'amélioration des pratiques RGPD
- Rapport de synthèse des revues pour le Responsable du Traitement

D2. Revue du dispositif RGPD (par les acteurs des lignes de maîtrise autres que le DPO)

Art. 24

Il convient de prévoir les activités de contrôle appropriées par les différents acteurs de la seconde ligne de maîtrise pour garantir le respect du RGPD.

L'audit fournit une assurance raisonnable sur la conformité au RGPD en évaluant les activités de contrôle de la 1ère et de la 2ème ligne de maîtrise. Ce contrôle de 3ème ligne vise à atténuer les risques.

Bonnes pratiques et matrice des responsabilités :

Rôles / Pratiques	Responsable du traitement (RT)	Comité d' Audit	[D]PO Référent RGPD	RSSI	IT/PMO/ Dpt DCP	Contrôle interne	Gestionnaire des risques	Gestionnaire de la conformité	Audit interne
Revoir de manière régulière et planifiée les mesures de contrôle du RGPD (contrôles du 1er niveau – opérations)	A		C	C	C	R		I	I
Intégrer l'évaluation des risques RGPD dans la gestion des risques de l'organisation	A		C	C	C	C	R	I	I
Déterminer le plan d'amélioration des mesures de contrôle	A		C	C/I	C/I	R	I	I	I
Assurer le suivi des plans d'action (par le Contrôle Interne)	A		C/I	C/I	C/I	R	C/I	C/I	I
Développer le programme d'audit du dispositif de mise en conformité au RGPD, y compris chez les ST	C	A	C	C	C	C	C	C	R
Exécuter l'audit de conformité au RGPD	C	A	C	C	C	C	C	C	R
Déterminer le plan d'action	I	A/I	R/I	R/I	R/I	R/I	R/I	R/I	S
Assurer le suivi du plan d'action	I	A/I	C/I	C/I	C/I	C/I	C/I	C/I	R
Rédiger le rapport d'audit et présenter les conclusions	I	A/I	I	I	I	I	I	I	R
Assurer le suivi des plans d'action (à la suite de l'audit)	I	A/I	C/I	C/I	C/I	C/I	C/I	C/I	R

Livrables

- Revue de mesures de contrôle (par le Contrôle interne)
- Gestion des risques liés à la protection des données personnelles
- Plan d'amélioration des mesures de contrôle
- Rapport d'audit
- Plan d'action (à la suite de l'audit)
- Rapport de suivi de la mise en œuvre des plans d'actions

D3. Contrôle par l'Autorité de Protection des Données

Il convient de prendre les mesures appropriées pour anticiper et permettre la surveillance et les inspections par l'Autorité de Protection des Données. Cela inclut la préparation de la documentation et des preuves du respect du RGPD (gestion documentaire) conformément au principe de responsabilité (*accountability)*[52]

Bonnes pratiques et matrice des responsabilités :

Rôles / Pratiques	Responsable du traitement (RT)	[D]PO	Référent RGPD	RSSI	IT/PMO/ Dpt DCP	Contrôle interne \ Gestionnaire des risques \ Gestionnaire de la conformité	Audit Interne
Identifier les contrôles et les inspections potentielles par les autorités	A	R					
Mettre en place un répertoire/ une gestion documentaire des registres, procédures, contrats, PV, avis, et autres documents permettant de démontrer que le responsable du traitement respecte les principes et obligations du RGPD	A	R/C	C/I	R/C/I	R/C/I	C/I	I
Établir la procédure en cas de contrôle sur place par l'APD	A	R	C/I	C/I	C/I	C/I	I
Établir la procédure de réponse à une demande écrite de l'Autorité de Protection des données	A	R					
Désignation des points de contacts et des responsables des lieux	A	R	C/I	C/I	C/I	C/I	I
Définir la conduite des collaborateurs	A	R	C/I	C/I	C/I	C/I	I
Clarifier les rôles du DPO, des responsables des lieux, et des interlocuteurs privilégiés	A	R	C/I	C/I	C/I	C/I	I
Former les personnes à l'accueil et au suivi d'un contrôle par l'Autorité de Protection des Données	A	R	I	I	I	I	I

[52] Article 5.2 du RGPD

Livrables

- Liste des contrôles (les éléments que l'autorité pourrait contrôler) et inspections potentielles
- Répertoire / Gestion documentaire des documents et des registres
- Procédure de contrôle sur place
- Procédure de réponse à une demande écrite de l'Autorité de Protection des Données
- Liste des points de contact et des responsables des lieux
- Code de conduite des collaborateurs
- Rôles du DPO, responsables des lieux et interlocuteurs privilégiés
- Matériel de formation en matière de contrôle par l'Autorité de Protection des Données

Annexe 1 - Glossaire

Le tableau ci-dessous reprend les acronymes utilisés avec leur signification en français et en anglais.

Acronyme	Terme français	Terme anglais
AI	Audit Interne	Internal Audit (IA)
AIPD	Analyse d'impact relative à la protection des données	Data Protection Impact Analysis (DPIA)
APD	Autorité de Protection des Données	Data Protection Authority (DPA)
BIA	Bilan d'Impact sur l'Activité	Business Impact Analysis
CEPD	Comité Européen à la Protection des Données	European Data Protection Board (EDPB)
CI	Contrôle Interne	Internal Control (IC)
DPbD	Protection des données dès la conception	Data Protection by Design
DPbDf	Protection des données par défaut	Data Protection by default
DCP	Données à Caractère Personnel	Personal data
DPO	Délégué à la Protection des Données (DPD)	Data Protection Officer
DRH	Direction des Ressources Humaines	Human Resources department (HR)
(D)TIA	Analyse d'Impact du Transfert des Données	(Data) Transfer Impact Assessment
IT	Direction informatique	Information Technology department
EEE	Espace Économique Européen	European Economic Area (EEA)
PCA	Plan de Continuité d'Activité	Business Continuity Plan (BCP)
PMO	Bureau Projet	Project Management Office
PO	Privacy Officer	Privacy Officer
PSSI	Politique de Sécurité des Systèmes d'Information	Information Security Systems Policy (ISSP)
RACI	Matrice de responsabilités : Réalise, Approuve et assume, Consulté, Informé	Responsibility matrix: Responsible, Accountable, Consulted, Informed
RGPD	Règlement Général sur la Protection des Données	General Data Protection Regulation (GDPR)
RPO	Perte de Données Maximale Admissible (PDMA)	Recovery Point Objective

Acronyme	Terme français	Terme anglais
RSSI	Responsable de la Sécurité des Systèmes d'Information (conseiller en sécurité)	Chief Information Security Officer (CISO)
RT	Responsable du Traitement	Controller
RTO	Durée Maximale d'Interruption Acceptable (DMIA)	Recovery Time Objective
SGSI	Système de Gestion de la Sécurité de l'Information	Information Security Management System (ISMS)
SSC	Clauses contractuelles types	Standard Contractual Clauses
ST	Sous-Traitant	Processor