Règlement Général de Protection des Données personnelles :

Démarche et outil qualité pour la mise en conformité de l'entreprise

Master Qualité et Performance dans les Organisations
2017-2018

Tuteur entreprise : Mme Audrey BERREBI
Suiveur UTC : Mr Jean-Matthieu PROT

Mémoire d'Intelligence Méthodologique

Claire MANCET

Mémoire en ligne sur www.utc.fr/master-qualite,
puis « travaux » « Qualité-management », réf 443, juillet 2018

Résumé

Le règlement général sur la protection des données du 27 avril 2016 (communément appelé «RGPD»), dont l'entrée en vigueur est fixée au 25 mai 2018 dans tous les pays de l'Union Européenne, est venu renforcer la protection de la vie privée des citoyens européens notamment suite au constat de l'utilisation massive des données personnelles.

Le RGPD renforce ainsi la responsabilité des acteurs qui mettent en œuvre des traitements de données à caractère personnel, la protection de la vie privée et la maîtrise des citoyens sur leurs données à caractère personnel.

La démarche et les travaux ont été élaborés dans un laboratoire pharmaceutique (PME) et l'objectif du projet consiste à accompagner cette entreprise dans la mise en conformité au RGPD.

- Mots clés : RGPD, données personnelles, système de management de la qualité, cartographie des processus de traitement, outil d'autodiagnostic.

Abstract

The General Regulation on Data Protection of 27 April 2016 (commonly named "GRDP") has an application date of May 25th 2018 and was issued to reinforce the protection of European citizens' private life due to the wide use of their personal data ("Big Data").

Thus GDRP strengthens the responsibilities of entities which deal with personal data treatments, the protection of private life and the control of citizens on their personal data.

The approach and the tasks were drawn up in a pharmaceutical laboratory (SME) and the scope of the project aims at guiding this company in the process of compliance to GRDP.

- Key words: GRDP, private data, quality management system, treatment process-map, self-assessment tool.

Remerciements

Je remercie Mme Audrey BERREBI Directeur Qualité pour son accompagnement, ses conseils et sa confiance lors de mon projet en entreprise.

Je remercie Mr Jean-Matthieu PROT Co-Responsable du Master Technologie et Territoires de Santé pour ses conseils et son suivi.

Je remercie toute l'équipe du Master Qualité et Performance dans les Organisations et plus particulièrement Mr Gilbert FARGES pour la qualité de son enseignement et pour sa confiance.

Je tiens aussi à témoigner ma gratitude à mes proches pour leur encouragement et leur soutien indéfectible.

SOMMAIRE

Légende

Les chiffres entre crochets correspondent aux références bibliographiques.

Glossaire

Approche processus : Méthode de représentation visuelle et transversale des activités de l'entreprise, permettant de détecter les points faibles et les dysfonctionnements situés le plus souvent à l'interface entre les services de l'entreprise [1].

Destinataire : Personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers [2].

Donnée à caractère personnel : Toute information se rapportant à une personne physique identifiée ou identifiable (personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale [2].

Donnée sensible : Donnée relative à l'origine raciale ou ethnique, aux opinions politiques, aux convictions religieuses ou philosophiques ou à l'appartenance syndicale, et le traitement des données génétiques, biométriques aux fins d'identifier une personne physique de manière unique, données concernant la santé ou la vie sexuelle ou l'orientation sexuelle [2] (Données portant sur des catégories particulières de données à caractère personnel).

Personne concernée : Personne physique dont les données à caractère personnel font l'objet d'un traitement [2].

Processus : Ensemble d'activités corrélées ou interactives qui transforme des éléments d'entrée en éléments de sortie [1].

Responsable du traitement : Personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement [2].

Sous-traitant : 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 [2].

Tiers : Personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous-traitant, sont autorisées à traiter les données à caractère personnel [2].

Traitement de données personnelles : Toute opération, en tout ou partie automatisée, concernant des données à caractère personnel [2].

Transfert de données : Toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'Union Européenne.

Violation de données à caractère personnel : violation de la sécurité entraînant de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

Liste des abréviations

BCR : Binding Corporate Rules (Règles d'entreprise contraignantes)
CRM : Customer Relationship Management
DCP : Données à caractère personnel
DPO : Data Protection Officer
PDS : Planification dynamique stratégique
RGPD : Règlement Général sur la Protection des Données
RT : Responsable de Traitement
SME : Small and Medium Enterprise
SWOT : Matrice S (Strenghts=Forces), W (Weaknesses=Faiblesses), O (Opportunities=Opportunités), T (Threats=Menaces)

Liste des figures

Avant-propos

Ces travaux de stage du Master Qualité et performance dans les organisations ont été réalisés dans le cadre de la formation continue et au sein d'une entreprise biomédicale et pharmaceutique (laboratoire pharmaceutique et distributeur de dispositifs médicaux).

Cette période de stage permet à l'étudiant de mettre à profit les connaissances acquises lors de la période théorique et de démontrer ses compétences métier, notamment son aptitude à analyser et synthétiser un référentiel, à cerner les enjeux, à impliquer les acteurs et à mettre en place des outils de pilotage et des outils opérationnels faciles d'emploi.

Le point essentiel à retenir est le rôle transversal et de support du service Qualité dans l'entreprise qui aide les organisations à s'adapter en fonction de leur environnement concurrentiel et réglementaire pour permettre la satisfaction et la confiance du client et du patient, qui sont au cœur des préoccupations de l'entreprise.

Introduction

Le règlement général sur la protection des données du 27 avril 2016 (communément appelé « RGPD »), dont l'entrée en vigueur est fixée au 25 mai 2018 dans tous les pays de l'Union Européenne, est venu renforcer la protection de la vie privée des citoyens européens, la responsabilité des acteurs qui mettent en œuvre des traitements de données à caractère personnel et la maîtrise des citoyens sur leurs données à caractère personnel.

Toutes les entreprises ainsi que les organismes publics doivent assurer une protection optimale des données en mettant en place un processus organisationnel adapté à la taille de leur structure et de leur activité et être en mesure de démontrer la protection des données en documentant la conformité.

Ce Mémoire d'Intelligence Méthodologique décrit donc le contexte et les enjeux liés au RGPD, la démarche qualité de mise en conformité avec ce nouveau règlement et l'élaboration d'une cartographie des processus de traitement des données à caractère personnel selon le RGPD et d'un outil d'autodiagnostic destinés à aider les entreprises à évaluer et à améliorer en continu leur organisation.

I. Contexte

1. Le Règlement Général Européen de Protection des données personnelles

Le RGPD renforce le droit des personnes, la responsabilité des acteurs et de leurs sous-traitants mais également le pouvoir des autorités de contrôle avec des sanctions renforcées [2].
Le règlement comporte 137 paragraphes « Considérant », 11 chapitres et 99 articles.
Ils concernent plusieurs acteurs et les processus liés aux traitements des données à caractère personnel sont nombreux et en interaction avec les différents acteurs [3].

1.1. Quel est le champ d'application du RGPD ?

Le champ d'application concerne les traitements des données automatisés et les traitements non automatisés qui figureront potentiellement dans un fichier.
Le RGPD s'applique dès lors qu'un organisme traite des données dans un fichier structuré ou non et dans le cadre d'une activité professionnelle et dès lors que le responsable de traitement ou le sous-traitant est établi sur le territoire de l'Union Européenne ou si le traitement a lieu sur le territoire de l'UE.
Le règlement s'applique également lorsque le responsable de traitement ou le sous-traitant n'est pas établi dans l'Union Européenne et que le traitement concerne des citoyens sur le territoire de l'UE.

1.2. Qu'entend-on par données à caractère personnel ?

Le RGPD cible les traitements des données permettant d'identifier directement ou indirectement une personne physique.
L'identification de la personne concernée est possible à partir d'une donnée ou à partir du croisement d'un ensemble de données [4].

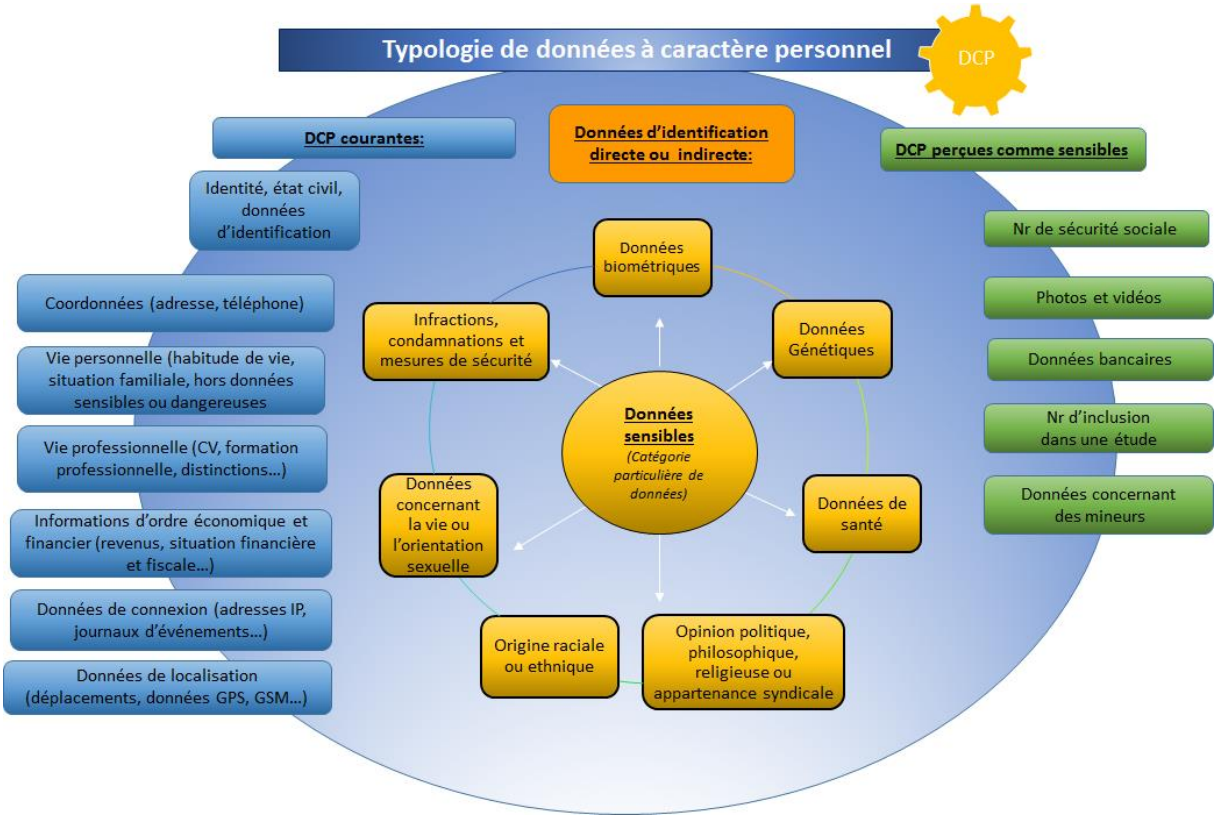


Figure 1 : Typologie de données à caractère personnel (DCP) [Source : Auteur d'après [5]]

1.3. Qu'entend-on par traitement de données à caractère personnel ?

Au sens du RGPD, il s'agit de toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction [2].

Quelques exemples de traitement [6] :
Fichiers excel, classeur papier, fichiers clients (CRM) et de gestion du personnel (RH), applications mobiles, vidéosurveillance, contrôles d'accès, biométrie, géolocalisation etc…

1.4. Qui sont les acteurs du RGPD ?

Parmi les acteurs du RGPD, on recense les personnes concernées, le destinataire, le sous-traitant, le responsable de traitement, le tiers (Voir § Glossaire) et le délégué à la protection des données ou DPO (Voir § 1.5.7).
Parmi les personnes concernées, on trouve les citoyens, les clients et les collaborateurs.
Dans une PME de santé, les personnes concernées sont les professionnels de santé, les patients et les collaborateurs.
La figure ci-dessous reprend les acteurs au sens du RGPD ainsi que les acteurs liés plus spécifiquement à l'entreprise biomédicale et pharmaceutique.

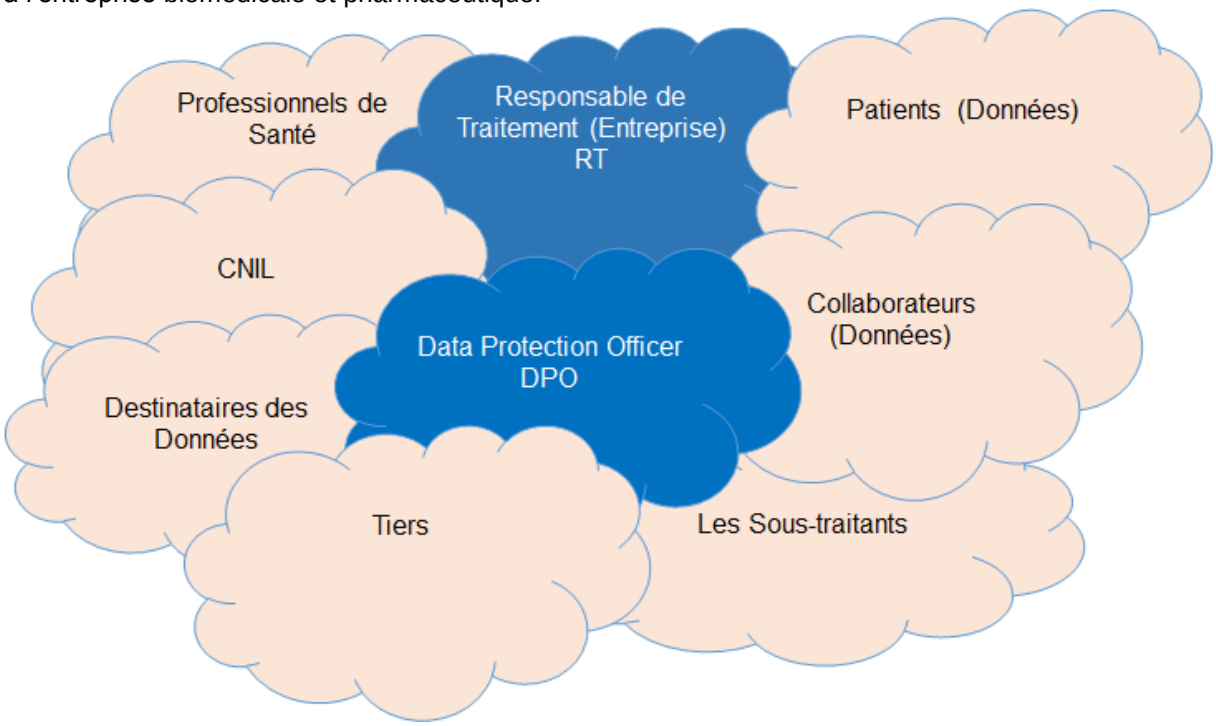


Figure 2 : Les acteurs du RGPD (entreprise de produits de santé) [Source : Auteur]

1.5. Quels sont les grands principes et changements introduits par le RGPD ?

[Sources [3] , [7], [8], [9]]

1.5.1.Licéité, loyauté, transparence du traitement des données

Le traitement n'est licite que s'il fait l'objet d'un consentement ou à défaut sa finalité est légitime ou répond à une obligation légale.
Les fondements possibles des traitements sont l'intérêt légitime, l'obligation légale, le consentement. Le Responsable de Traitement (RT) doit donc vérifier le fondement du traitement.

- Consentement de la personne concernée :

Le consentement de la personne concernée doit être obtenu spécifiquement pour chaque finalité différente du traitement.

- Traitement ultérieur :

Le RT doit suivre la réglementation nationale selon le RGPD pour vérifier si des spécificités s'appliquent, et s'assure que la portée du consentement initial permet une utilisation ultérieure des mêmes données.

1.5.2.Limitation de la finalité et de la durée de conservation des données

Le RT doit veiller à ce que les données traitées soient uniquement nécessaires aux finalités définies, précises et légitimes et qu'elles ne soient pas réutilisées pour d'autres finalités que celles prévues. Des durées de conservation des données doivent être définies.
Il existe 3 catégories d'archives dans le cycle de vie des DCP [9]:

- Les archives courantes correspondant aux données actives : leur durée de conservation doit correspondre à la finalité prévue du traitement.
- Les archives intermédiaires (archivage légal, probatoire) : leur conservation est obligatoire pour des raisons légales et les durées de conservation sont réglementées.
- Les archives définitives : elles correspondent à la suppression, à l'anonymisation ou à l'archivage à des fins archivistiques ou historiques.

1.5.3.Minimisation et exactitude des données

Le RT doit s'assurer que les données collectées sont limitées et strictement nécessaires aux finalités des traitements (Principe de proportionnalité). L'entreprise recourt alors à des procédés de destruction, d'effacement ou d'anonymisation des données en place.

1.5.4.Intégrité et confidentialité des données

Le RT s'assure que les données sont traitées de façon à garantir leur sécurité et que des mesures de protection des données et des procédures pour pérenniser la démarche sont mises en place.

1.5.5.Responsabilité des acteurs (Accountability)

Les déclarations à la CNIL ne sont plus obligatoires sauf exception, et sont remplacées par le principe de responsabilité. Les exceptions sont définies sur le site de la CNIL. Les RT doivent être en mesure de démontrer à n'importe quel moment leur conformité à la réglementation [9].

1.5.6. Formation et sensibilisation des collaborateurs

Les collaborateurs des entreprises doivent recevoir régulièrement des formations sur la réglementation portant sur le traitement de données à caractère personnel.

1.5.7. Désignation d'un délégué à la protection des données

Le Délégué à la Protection des Données (Data Protection Officer) est le chef d'orchestre de la conformité en matière de protection des données. Il est chargé d'informer et de conseiller le(s) responsable(s) de traitement, les sous-traitant(s) et les collaborateurs, de contrôler le respect du RGPD et du droit national, de conseiller l'organisme sur la réalisation d'une analyse d'impact et de coopérer avec l'autorité de contrôle dont il est l'interlocuteur.

1.5.8. Mise en place et tenue d'un registre des activités de traitement

Le RT s'assure de la tenue d'un registre du traitement où figurent a minima les informations suivantes : les finalités du traitement, les catégories de personnes concernées et les catégories de données, les catégories de destinataires, les transferts de données hors de l'UE, la durée de conservation des données et les mesures de sécurité.

Ce registre est tenu à disposition de l'Autorité de Contrôle [9] .

1.5.9. Réalisation d'audits internes pour les données sensibles

Des contrôles, des audits internes et des audits des sous-traitants doivent être planifiés.

1.5.10. Respect des principes de protection des données (privacy by design, privacy by default)

La notion de « privacy by design » est la protection de la vie privée dès la conception et la notion de « privacy by default » correspond au paramétrage des applications pour la protection des données personnelles et l'intégration de mesures de sécurité dans la technologie [9].

1.5.11. Encadrement du transfert de données vers des pays hors UE

L'entreprise doit encadrer les transferts de données vers d'autres pays [9].
Le transfert ne peut se faire que si :

- le transfert est assuré vers un pays « adéquat », ou
- une forme d'adéquation est assurée, ou
- les conditions nécessaires à la conformité sont respectées par le RT et le sous-traitant.

La Commission Européenne considère certains pays comme fiables (adéquation) car ils ont fourni la preuve de la qualité de traitement, de collecte et de protection des données personnelles.

Lorsque le pays n'est pas adéquat, il existe des dérogations dans les cas suivants:

- Le RT a obtenu le consentement explicite de la personne concernée au transfert de ses données
- Le transfert est nécessaire : pour des raisons contractuelles, pour des motifs d'intérêt public, pour l'exercice du droit ou d'une décision de justice, pour la sauvegarde d'intérêts vitaux.
- Le transfert de données est fait à partir d'un registre public
- Le transfert est effectué dans un cadre limité et légitime dûment justifié par le RT auprès des autorités.

En l'absence d'adéquation et de dérogations, d'autres outils existent :

- Accords juridiques entre Etats (Exemple : Privacy Shield qui est un accord conclu entre l'UE et les USA pour permettre des transferts de données entre l'Europe et les Etats-Unis).
- Clauses types définies par la Commission Européenne
- Règles d'entreprise contraignantes (Binding Corporate Rules-BCR) :
  Elles impliquent tous les collaborateurs de l'entreprise, définissent les responsabilités, les mécanismes de gestion des réclamations et de l'exercice des droits des personnes concernées et garantissent l'adéquation organisationnelle.

1.5.12. Obligation d'informer l'autorité de contrôle sur d'éventuelles violations de données

Les responsables de traitement sont dans l'obligation de notifier les violations (voir définition du terme « violation » au § Glossaire) de données à caractère personnel à l'autorité de contrôle, dans les meilleurs délais et si possible dans un délai n'excédant pas 72 heures après en avoir pris connaissance. Une fois ce délai dépassé, les responsables de traitement doivent motiver la raison de ce retard.

Les responsables de traitement doivent également informer les personnes concernées des violations de données personnelles les concernant si ces données sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

La CNIL a mis à disposition des entreprises un formulaire de notification des violations de données personnelle [10].

1.5.13. Etude d'impact sur la vie privée (DPIA-Data Privacy Impact Assessment)

Les responsables de traitement doivent procéder à une analyse d'impact sur la vie privée avant de mettre en place un traitement susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques et doivent consulter la CNIL au préalable lorsque l'analyse d'impact indique un risque élevé.

1.5.14. Renforcement du droit des personnes

Les personnes concernées disposent des droits suivants : droit d'accès, droit de rectification, droit à l'effacement, droit à la portabilité, droit d'opposition et droit de limitation des traitements des données à caractère personnel les concernant.

1.5.15. Pouvoir renforcé des autorités de régulation

Le RGPD désigne les Autorités de protection des données comme Autorités de contrôle.
Les autorités de contrôle, telles que la CNIL en France, deviennent des régulateurs complets ayant un rôle de conseil et pouvant prendre des mesures correctives et des sanctions.
L'autorité de contrôle est celle du lieu de l'établissement principal de l'entreprise.
Un Comité Européen de Protection des Données a été mis en place pour éventuellement régler les désaccords entre les autorités de régulation.

1.5.16. Certification et labels

Le RGPD prévoit un dispositif de certification des entreprises en matière de protection des données et un label européen de protection des données.

Tous ces changements introduits par le RGPD entraînent de nouveau enjeux pour les entreprises.

2. Enjeux

Les entreprises doivent faire face à trois grands types d'enjeux :

➢ Des enjeux d'ordre organisationnels

Les entreprises vont devoir allouer les ressources nécessaires et organiser les processus liés aux différents traitements de données notamment pour pouvoir répondre aux droits des citoyens européens (accès, rectification, droit à l'oubli, limitation, portabilité, opposition etc…).
Les entreprises doivent obligatoirement désigner un délégué à la protection des données si elles appartiennent au secteur public ou si elles réalisent un suivi régulier des personnes à grande échelle ou si leurs activités leur imposent de traiter à grande échelle des données sensibles ou concernant des infractions ou condamnations pénales.

Dans le cas particulier des laboratoires pharmaceutiques et des industriels du dispositif médical, l'obligation de désigner un Délégué à la Protection des Données s'impose car ils doivent gérer des données sensibles à grande échelle, notamment dans le cadre de leurs obligations liées aux vigilances (pharmacovigilance, matériovigilance…) et/ou aux études cliniques.

➢ Des enjeux de développement et d'image de marque

Le RGPD représente pour les entreprises et les établissements de santé une opportunité d'obtenir la confiance de leurs clients, de leurs patients et de développer leurs activités numériques selon un cadre juridique enfin établi et harmonisé et éliminant les contrastes entre les territoires. En respectant le principe de mise à jour et de rectification des données de leurs clients (fichiers de facturation et prospects par exemple), les entreprises amélioreront leur efficacité commerciale et gagneront en productivité. De même, en rationnalisant les données (principe de minimisation des données), les ressources nécessaires (moyens humains et techniques) seront également rationnalisés, l'entreprise gagnera en efficience et optimisera ses investissements [4].

D'après le MEDEF [6], **«** La protection des données personnelles est un moyen pour l'entreprise de renforcer la confiance qui la lie à ses clients, partenaires et salariés, dans un contexte de plus en plus numérique. Elle doit donc bel et bien être considérée par l'entreprise comme un atout ».

➢ Des enjeux d'ordre financiers et judiciaires

En cas de manquement aux dispositions du RGPD, les sanctions encourues sont des amendes administratives fixées par les autorités de contrôles.
Elles peuvent s'élever à 10 millions d'euros ou 2% du chiffre d'affaires du total mondial du groupe.
Pour les manquements considérés plus graves, les entreprises encourent jusqu'à 20 millions d'euros ou 4% du CA mondial.

Après l'étude du RGPD et des enjeux qui en découlent, le cadrage du projet a été établi.

3. Problématique et objectifs du projet

Afin de cerner la situation, il a été nécessaire de se poser les bonnes questions. L'outil de résolution de problème QQOQCP a été utilisé pour permettre de cadrer le projet.

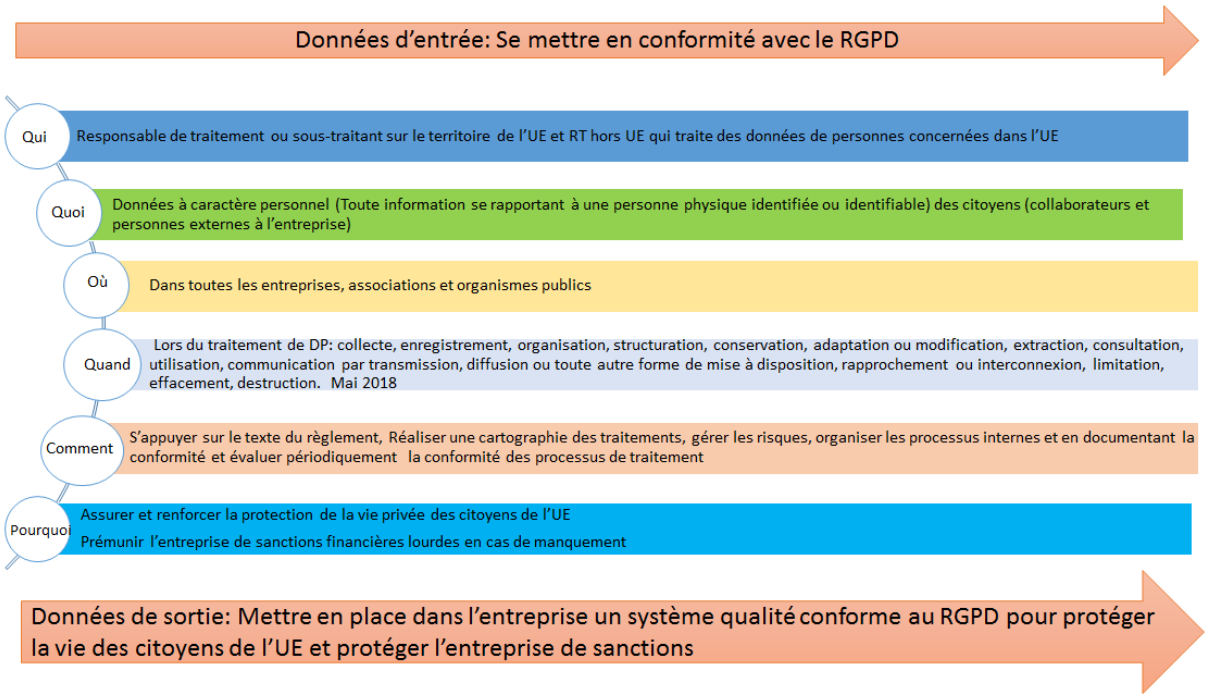


Figure 3 : Cadrage de la démarche de mise en conformité avec le RGPD [Source : Auteur]

Les enjeux et les objectifs du projet sont clarifiés et établis dans une planification dynamique stratégique qui permet de mettre en exergue le sens et l'importance de la démarche :

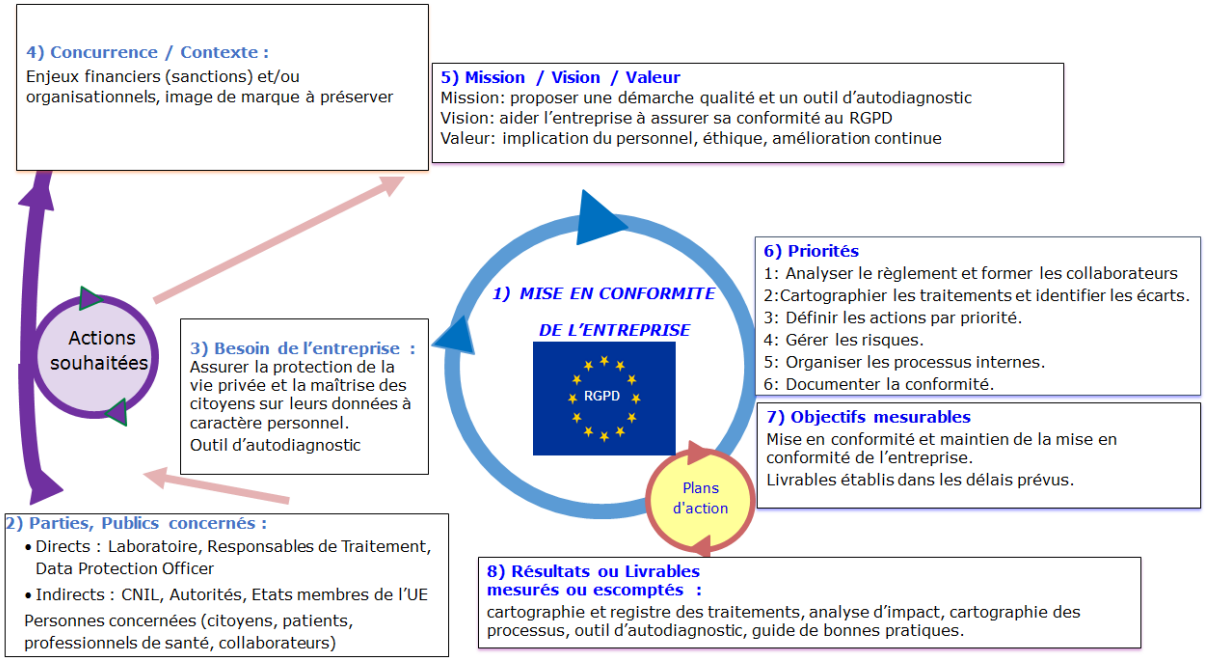


Figure 4 : Planification dynamique stratégique [Source : Auteur]

Cette planification est complétée par une analyse des risques et opportunités du projet.

Figure 5 : Matrice SWOT pour la mise en conformité des entreprises au RGPD [Source : Auteur]

Le projet consiste à mettre en place une démarche de mise en conformité au RGPD dans une petite structure (PME) pharmaceutique.

Il faudra donc adapter la démarche au fonctionnement et aux moyens disponibles dans ce type de structure.

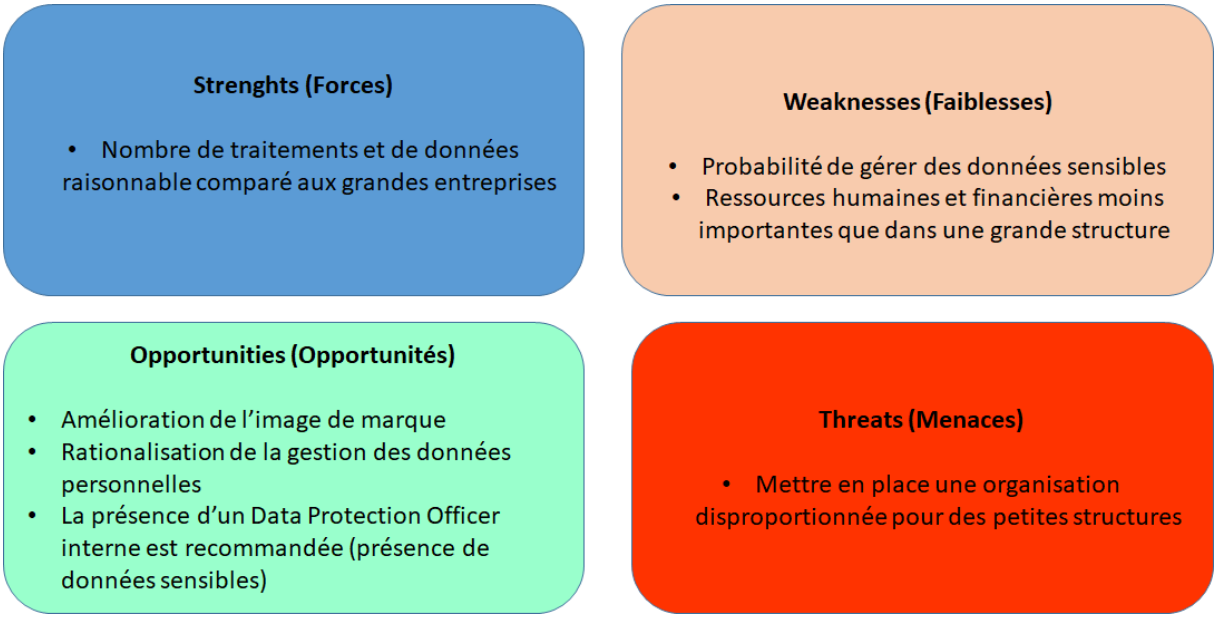


Figure 6 : Matrice SWOT du projet dans l'entreprise pharmaceutique (PME) [Source : Auteur]

II. Méthodologie de la démarche qualité

La CNIL a mis en place un guide [11] pour aider les entreprises à initier leur démarche de conformité.

Ces étapes sont décrites dans la figure ci-dessous :

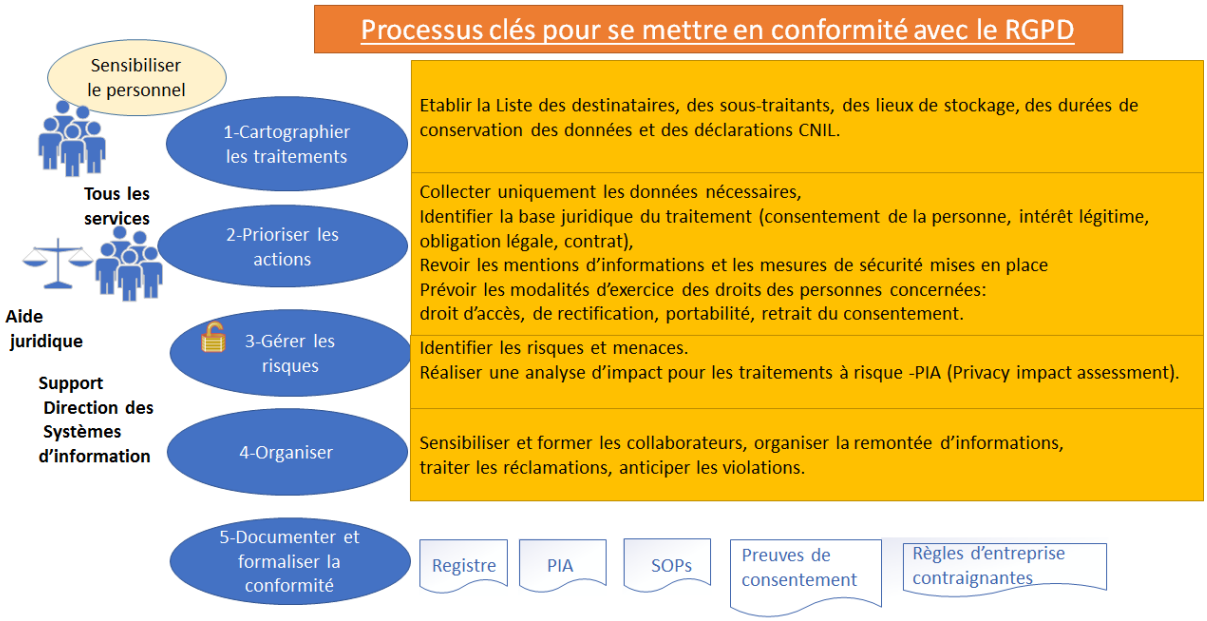


Figure 7 : Processus clés pour se mettre en conformité avec le RGPD [Auteur, d'après [11]]

Les entreprises, dont les PME, peuvent donc concevoir leur démarche qualité sur la base de ces différentes étapes.

1. Présentation de la méthodologie choisie

S'agissant d'un nouveau règlement et engendrant a fortiori de nouvelles activités, la démarche qualité de mise en conformité proposée pour la PME est basée sur les quatre phases fondamentales du cycle d'amélioration continue PDCA, dans lesquelles on retrouvera les étapes préconisées par la CNIL.

Plus précisément la démarche PDCA déployée dans le cadre du projet est la suivante :

PLAN (Prévoir ce qu'il faudra faire) *:* Cette phase consiste en une étude du contexte, une lecture approfondie et une synthèse du règlement et des guides édités par la CNIL, un diagnostic des pratiques de l'entreprise et une cartographie des traitements.
DO (Réaliser ce qui a été prévu): Durant cette phase, il s'agit d'identifier les actions à mettre en œuvre avec les Responsables de Traitements à partir du diagnostic réalisé (avec un support juridique et informatique), de leur affecter un niveau de priorité sur la base de la cartographie des traitements et selon les risques associés, de réaliser une étude d'impact pour les traitements présentant un risque élevé pour les droits des personnes concernées.
CHECK (Mesurer les résultats): Cette phase repose sur le suivi de l'avancement des actions, la mesure de leur efficacité, notamment par des audits internes (avec outil d'autodiagnostic proposé dans le cadre de ces travaux).
ACT (Améliorer et évoluer): Durant cette 4ème phase, les actions d'amélioration sont identifiées.

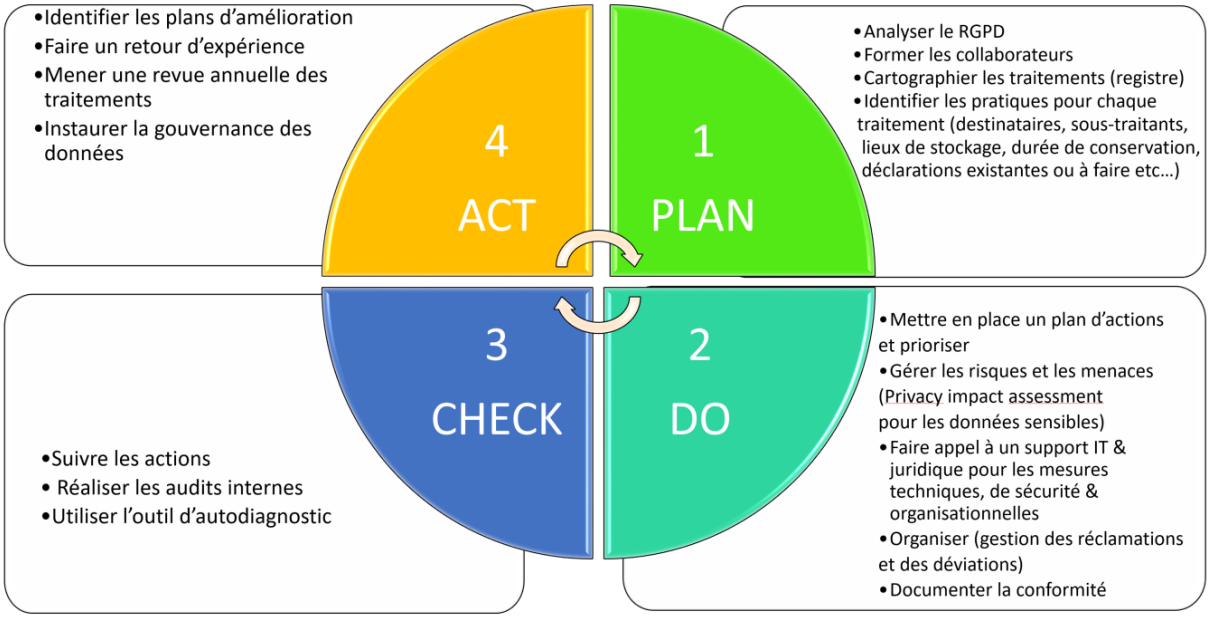


Figure 8 : Description de la méthodologie choisie pour la démarche qualité [Source : Auteur]

2. Phase PLAN

2.1. Equipe projet

Ce projet ne peut aboutir que si tous les acteurs de l'entreprise sont impliqués (principe de co-construction).L'humain est au cœur du projet pour permettre de comprendre et de bien cerner les enjeux du RGPD. Des sessions d'informations et de formation sont organisées, le but étant de mettre en place des solutions pragmatiques, réalistes et adaptées à l'entreprise.
L'équipe projet est constituée des responsables de traitements, des services Qualité et Informatique, du délégué à la protection des données ou correspondant informatique et libertés.
Le service Qualité apporte son support aux responsables de traitement pour appliquer les principes de « Privacy by Design » et « Privacy by default » et pour mettre en place des règles de bonnes pratiques et des procédures, pour aider les collaborateurs dans leurs pratiques quotidiennes.

2.2. Cartographie des traitements

Afin de pouvoir vérifier la conformité des traitements réalisés dans l'entreprise, il est nécessaire d'avoir une connaissance exhaustive des traitements [12].
Le service Qualité se rapproche donc de chaque service pour réaliser un inventaire de tous les traitements dans un registre contenant les informations suivantes pour chaque traitement:
-Finalités (s) du traitement
-Responsable de traitement
-Personnes concernées
-Type de données (sensibles ou non)
-Supports (papier, électronique)
-Lieu de stockage
-Destinataires des données
-Sous-traitant(s)
-Transfert des données hors de l'UE
-Les déclarations CNIL déjà effectuées ou à réaliser selon la liste d'exceptions
-Proportionnalité des données collectées

Lors de cette étape il est primordial d'identifier les flux de chaque traitement et d'identifier si le traitement est géré en interne ou par une personne extérieure à l'organisation.

Finalité	Données sensibles	Nature des Données	Liste des données	Document	Responsable	ARCHIVAGE		Transmission à des tiers	Déclaration CNIL	Nr déclaration Cnil	Date	Temps d'archivage	Transfert hors UE
						élect.	Papier						
gestion des accès	oui	Biométriques	Nom, prénom, empreintes digitales	Liste des accès autorisés	Responsable IT	oui	non	non	oui	ID1800XXDK	26/12/2017	Durée contrat travail	non

Figure 9: Exemple de registre de traitement [Source : Auteur]

Cet inventaire permet d'identifier les éventuels manquements (ex : durée d'archivage non définie) mais également d'identifier les données dites sensibles, pour lesquelles la mise en place d'actions sera prioritaire.

3. Phase DO

La phase « DO » consiste à travailler sur les mesures nécessaires pour garantir la protection des données et à les mettre en œuvre.

3.1. Etude d'impact (Privacy impact assessment «PIA»)

La CNIL fournit sur son site internet un ensemble de guides sur la réalisation d'une analyse d'impact ainsi qu'un logiciel téléchargeable permettant de réaliser un PIA [12].

L'étude d'impact concerne les traitements susceptibles de présenter un risque pour les droits des personnes concernées. Elle doit permettre de concevoir des traitements de données personnelles respectueux de la vie privée, d'évaluer l'impact sur la vie privée et de démontrer que les principes fondamentaux de la réglementation en matière de données à caractère personnel sont respectés ([5] [9] [13] [14]).

L'étude d'impact est basée sur la cartographie des traitements (Cf II.2.2) et réalisée prioritairement pour les traitements de données dites sensibles. Pour chaque traitement, l'analyse consiste à prévenir et réduire les risques selon trois critères de risques principaux:

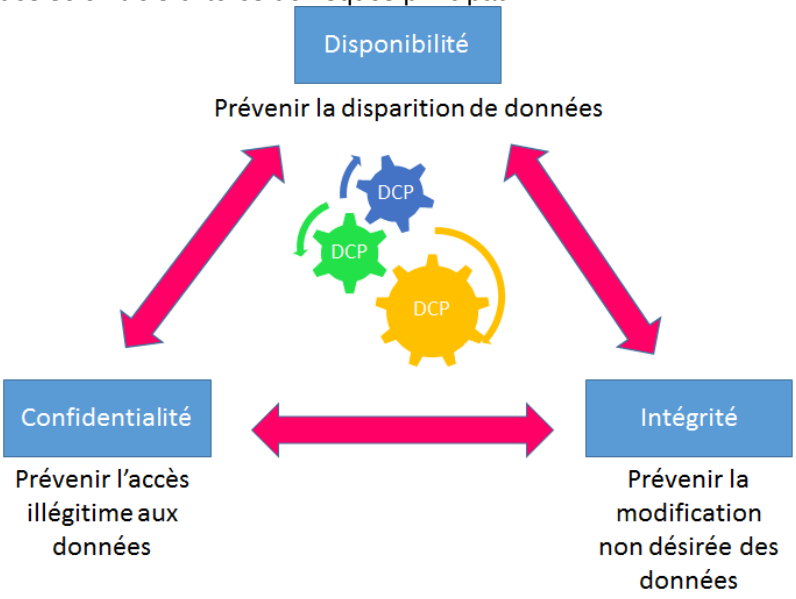


Figure 10 : Schéma des risques potentiels [15]

Pour chaque risque identifié, l'étude d'impact consiste à évaluer :

- Les supports de données (cf exemple figure 11)
- Les sources de risques : les origines possibles d'un événement redouté sont évaluées en tenant compte des sources humaines et non humaines, internes ou externes à l'entreprise (cf. figure 12);
- Les menaces réalisables : les menaces qui pourraient permettre à un événement redouté de se produire sont recensées ;
- Les mesures prises : pour chaque risque, les mesures existantes ou prévues sont décrites ;
- La gravité des risques (cf. figure 16)
- La vraisemblance des risques (cf. figure 17)

3.1.1. Supports de données

Les supports de données correspondent aux composants du système d'information sur lesquels reposent les données à caractère personnel :

Types de supports de données		Exemples
Systèmes informatiques	Matériels et supports de données électroniques	Ordinateurs, relais de communication, clés USB, disques durs
	Logiciels	Systèmes d'exploitation, messagerie, bases de données, applications métier
	Canaux informatiques	Câbles, WiFi, fibre optique
Organisations	Personnes	Utilisateurs, administrateurs informatiques, décideurs
	Supports papier	Impressions, photocopies, documents manuscrits
	Canaux de transmission papier	Envoi postal, circuit de validation.

Figure 11 : Types de supports de données [5]

3.1.2. Sources de risques

Les origines possibles d'un événement redouté sont évaluées en tenant compte des sources humaines et non humaines internes ou externes à l'entreprise.

Typologie de sources de risques	Exemples
Sources humaines internes	Salariés, administrateurs informatiques, stagiaires, dirigeants.
Sources humaines externes	Destinataires des DCP, tiers, prestataires, pirates informatiques, visiteurs, anciens employés, militants, concurrents, clients, personnel d'entretien, maintenance, délinquants, syndicats, journalistes, organisations non gouvernementales, organisations criminels, organisations sous le contrôle d'un Etat étranger, organisations terroristes, activités industrielles environnantes.
Sources non humaines	Codes malveillants d'origine inconnue (virus, vers …), eau (canalisations, cours d'eau…), matières inflammables, corrosives ou explosives, catastrophes naturelles, épidémies, animaux.

Figure 12 : Sources de risques [5]

3.1.3. Gravité et vraisemblance

La gravité et la vraisemblance des risques sont estimées selon tous les éléments précédents et selon la cotation suivante : négligeable, modérée, importante, maximale.
L'impact doit être envisagé sous 3 aspects : impact matériel, impact corporel, impact moral.

3.1.4. Détermination du niveau de gravité

La gravité représente l'ampleur du risque. Ci-dessous figurent des exemples fournis par la CNIL.
NB : Il est important de prendre compte le contexte considéré.

Niveaux	Descriptions génériques des impacts (directs et indirects)	Exemples d'impacts corporels	Exemples d'impacts matériels	Exemples d'impacts moraux
Négligeable (1)	Les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté	- Absence de prise en charge adéquate d'une personne non autonome (mineur, personne sous tutelle) - Maux de tête passagers …	- Perte de temps pour réitérer des démarches ou pour attendre de les réaliser - Réception de courriers non sollicités (ex. : spams) …	- Simple contrariété par rapport à l'information reçue ou demandée - Peur de perdre le contrôle de ses données …
Limitée (2)	Les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés	- Affection physique mineure (ex. : maladie bénigne suite au non-respect de contre-indications) - Absence de prise en charge causant un préjudice minime mais réel (ex : handicap) - Diffamation donnant lieu à des représailles physiques ou psychiques …	- Paiements non prévus (ex. : amendes attribuées de manière erronée), frais supplémentaires (ex. : agios, frais d'avocat), défauts de paiement - Refus d'accès à des services administratifs ou prestations commerciales …	- Refus de continuer à utiliser les systèmes d'information (whistleblowing, réseaux sociaux) - Affection psychologique mineure mais objective (diffamation, réputation) …
Importante (3)	Les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec des difficultés réelles et significatives	- Affection physique grave causant un préjudice à long terme (ex. : aggravation de l'état de santé suite à une mauvaise prise en charge, ou au non-respect de contre-indications) …	- Détournements d'argent non indemnisé - Difficultés financières non temporaires (ex. : obligation de contracter un prêt) …	- Affection psychologique grave (ex. : dépression, développement d'une phobie) - Sentiment d'atteinte à la vie privée et de préjudice irrémédiable …
Maximale (4)	Les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter	Affection physique de longue durée ou permanente (ex. : suite au non-respect d'une contre-indication) …	Péril financier - Dettes importantes - Impossibilité de travailler - Impossibilité de se reloger …	Affection psychologique de longue durée ou permanente - Sanction pénale …

Figure 13 : Echelles de gravité d'après [13]

3.1.5. Détermination du niveau de vraisemblance

La vraisemblance traduit la possibilité que le risque se réalise. Elle est estimée en tenant compte de la vulnérabilité des supports et de la capacité des sources de risques à exploiter ces vulnérabilités, et des mesures existantes, prévues ou complémentaires [13].

L'échelle suivante est utilisée :

1. Négligeable : en considérant les supports des données (figure 11) et les sources de risques retenues (figure 12), il semble improbable que les risques se réalisent (ex. : vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge et code d'accès).

2. Limité : en considérant les supports des données (figure 11) et les sources de risques retenues (figure 12), il semble peu probable que les risques se réalisent (ex. : vol de supports papiers stockés dans un local de l'organisme dont l'accès est contrôlé par badge).

3. Important : en considérant les supports des données (figure 11) et les sources de risques retenues (figure 12), il semble probable que les risques se réalisent (ex. : vol de supports papiers stockés dans les bureaux d'un organisme dont l'accès est contrôlé par une personne à l'accueil).

4. Maximal : en considérant les supports des données (figure 11) et les sources de risques retenues (figure 12), il semble extrêmement probable que les risques se réalisent (ex. : vol de supports papier stockés dans le hall public de l'organisme).

3.2. Exemple d'analyse d'impact

Ci-dessous figure un exemple d'analyse d'impact réalisée sur un traitement de données biométriques pour la gestion des accès physiques aux locaux d'une entreprise.

Risques	Impact sur les personnes	Principales sources de risques	Types de support/ Actions	Menaces	Mesures existantes ou prévues	Gravité	Vraisemblance
Accès illégitime aux données **Confidentialité**	Usurpation d'identité, accès illégitime aux locaux	Sources humaines internes: malveillance, inadvertance	Personnes observées, détournées	Utilisation frauduleuse du mot de passe de l'ordinateur, Divulgation involontaire du mot de passe en conversant, influence, pression.	Ordinateur protégé par un mot de passe, prévoir une liste des personnes habilitées pour l'accès à l'ordinateur et au paramétrage de la biométrie. Formation des personnes habilitées au paramétrage de la biométrie. Mettre en place un registre des accès à l'ordinateur utilisé pour la biométrie.	Importante	Limitée
Accès illégitime aux données **Confidentialité**	Usurpation d'identité, accès illégitime aux locaux	Sources humaines externes: prestataire, ancien salarié.	Personnes observées, détournées	Utilisation frauduleuse du mot de passe de l'ordinateur, Divulgation involontaire du mot de passe, débauchage d'un employé	Mettre en place une liste des personnes habilitées et une clause de confidentialité, Prévoir un renouvellement périodique du mot de passe.	Limitée	Importante

Risques	Impact sur les personnes	Principales sources de risques	Types de support/ Actions	Menaces	Mesures existantes ou prévues	Gravité	Vraisemblance
Disparition des données **Disponibilité**	Impossibilité d'accéder aux locaux	Sources humaines internes: malveillance, inadvertance	Personnes surchargées	Effacement intentionnel ou non intentionnel (erreur de manipulation menant à la suppression des données) ou vol des données). Charge de travail importante, personne insuffisamment formée	Ordinateur protégé par un mot de passe, prévoir une liste des personnes habilitées pour l'accès à l'ordinateur. Formation des personnes habilitées au paramétrage de la biométrie.	Limitée	Limitée
Disparition des données **Disponibilité**	Impossibilité d'accéder aux locaux	Sources humaines externes: prestataire, ancien salarié.	Personnes surchargées, détournées	Effacement intentionnel ou non intentionnel (erreur de manipulation menant à la suppression des données) ou vol des données). Charge de travail importante, faible loyauté vis-à-vis de l'entreprise.	Ordinateur protégé par un mot de passe, prévoir une liste des personnes habilitées pour l'accès à l'ordinateur et au paramétrage de la biométrie. Formation des personnes habilitées au paramétrage de la biométrie. Mettre en place un registre des accès à l'ordinateur utilisé pour la biométrie. Contrat et clause de confidentialité avec prestataire. Utilisation de clés permettant l'accès physique aux locaux	Limitée	Limitée

Figure 14 : Exemple d'analyse d'impact d'un système de biométrie [Source : Auteur]

Une fois l'étude d'impact effectuée, le responsable de traitement dispose d'une cartographie des risques liés au traitement des données.
Les 3 évènements redoutés (Accès illégitime à des données, disparition des données et modification non désirée des données) apparaissent dans la cartographie en fonction de leur niveau de gravité et de leur vraisemblance. Les mesures qui doivent être mise en place vont devoir permettre de réduire leur niveau de vraisemblance et si possible leur gravité.

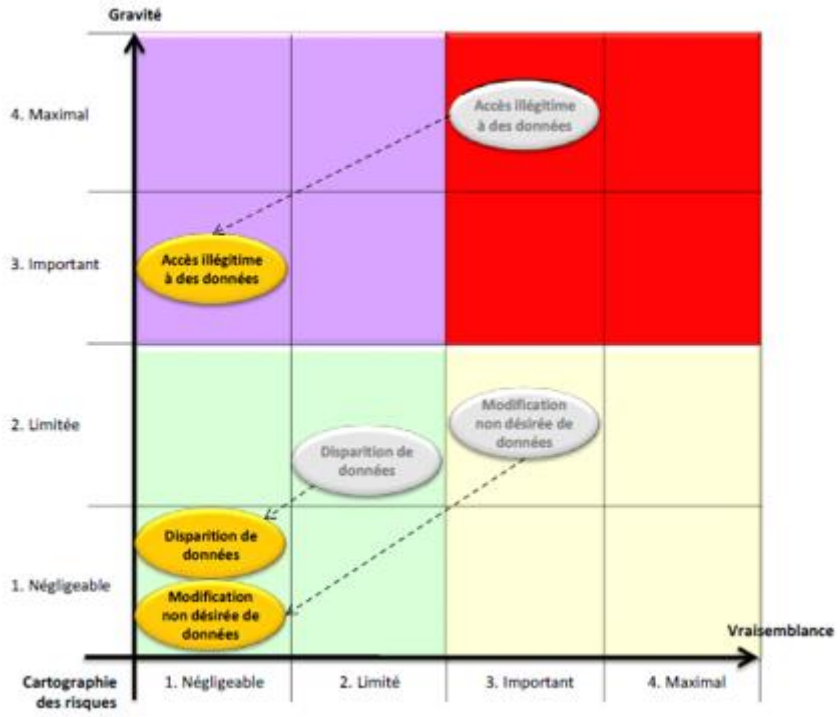


Figure 15 : Exemple de cartographie des risques liés à la sécurité des données [14]

Dans la figure 15, on retrouve en gris les niveaux de gravité et de vraisemblance de l'événement redouté selon les mesures prévues ou existantes.
En jaune, on observe le niveau de gravité et de vraisemblance de l'événement redouté, après la mise en œuvre des mesures correctives.
Il convient pour chaque entreprise de définir le score minimal à atteindre lors de l'analyse d'impacts pour la mise en place d'actions correctives.
Compte tenu de cette cartographie et des éléments de l'analyse d'impact, le responsable de traitement établit un plan d'actions avec le support de la personne en charge des aspects «informatique et libertés » (DPO par exemple).

3.3. Mesures techniques

Les responsables de traitement doivent évaluer les mesures de protection à mettre en place avec un support du service Informatique ou d'un prestataire externe.

Il peut s'agir de :

- Chiffrement : les DCP sont rendues incompréhensibles à toute personne non autorisée à y avoir accès.
- Cloisonnement des données par rapport au reste du système d'information : réduction de la possibilité de corréler les DCP et de provoquer une violation de l'ensemble des données.
- Contrôle d'accès physique : limitation du risque que des personnes non autorisées n'accèdent physiquement aux DCP.
- Contrôle d'intégrité : alerte en cas de modification non désirée ou de disparition de DCP.
- Contrôle des accès logiques : limitation du risque que les personnes non autorisées accèdent aux DCP par voie électronique.
- Durées de conservation limitées : réduction de la gravité des risques en s'assurant que les DCP ne sont pas conservées plus que nécessaires.
- Mise en place d'un système de sauvegardes
- Gestion des postes de travail

Pour mettre en place des mesures de protection et de sécurité des données, les entreprises pourront s'appuyer sur la norme ISO 27001 [16]. Cette norme décrit les exigences relatives à l'établissement, la mise en œuvre et l'amélioration continue d'un système de management de la sécurité de l'information.

3.4. Mesures organisationnelles

Une organisation est établie pour permettre la validation de chaque étape d'un nouveau traitement avec un initiateur et un circuit de visas par exemple [9].
L'entreprise doit disposer d'une personne pour piloter les traitements. Elle doit lui permettre d'avoir les connaissances nécessaires et adaptées au type d'entreprise concernée et de pouvoir bénéficier de supports informatiques.
La présence d'un Délégué à la protection des données n'est pas obligatoire mais fortement recommandée. Elle est obligatoire si l'entreprise compte plus de 250 salariés ou si elle traite des données sensibles à grande échelle.

4. Phase CHECK

Durant cette phase, la mise en place des actions est vérifiée.
Un programme d'audits internes portant sur les traitements est établi selon une analyse de risques. Les traitements présentant un niveau de risque élevé seront audités prioritairement.
Les entreprises peuvent utiliser l'outil d'autodiagnostic présenté au chapitre III.2 et se faire accompagner si besoin par des auditeurs spécialisés.

5. Phase ACT

Cette phase est indispensable au pilotage de la conformité car elle consiste pour l'entreprise à évaluer les axes d'amélioration en procédant à des revues annuelles des processus de traitement et des indicateurs et en établissant des plans d'amélioration.
La Direction, les responsables, la Qualité et le DPO sont donc impliqués. Ils revoient les résultats des audits et de la revue annuelle des traitements de données et adaptent l'organisation et les responsabilités internes en conséquence. C'est le principe de la gouvernance.

III. Bilan des travaux

Durant la période de stage, les travaux menés ont donc consisté à étudier et synthétiser un référentiel réglementaire et à initier la démarche de mise en conformité de l'entreprise avec le RGPD et de gouvernance des données, et également à réaliser une cartographie des processus liés au traitement des données selon le RGPD ainsi qu'un outil d'autodiagnostic permettant d'évaluer son niveau de conformité.

1. Cartographie des processus

L'approche processus permet de représenter les activités d'une entreprise de façon synthétique et transversale et de répondre aux attentes des parties prenantes (personnes concernées, autorités de contrôle, responsables de traitement, data protection officer, direction) en déterminant les missions dans l'entreprise.
Les différents processus du RGPD liés aux traitements des données sont imbriqués et impliquent aussi bien des acteurs dans l'entreprise que des acteurs extérieurs tels que les personnes concernées, les destinataires, les sous-traitants et les autorités de contrôle [3].
L'objectif des travaux a donc été de synthétiser les processus de traitement des données dans l'entreprise au sens du RGPD ainsi que tous les sous-processus de réalisation associés, les processus supports et de direction dans une seule et même cartographie.
Celle-ci permet de communiquer avec clarté sur les exigences du RGPD, de faciliter la compréhension des collaborateurs et d'anticiper l'amélioration continue.

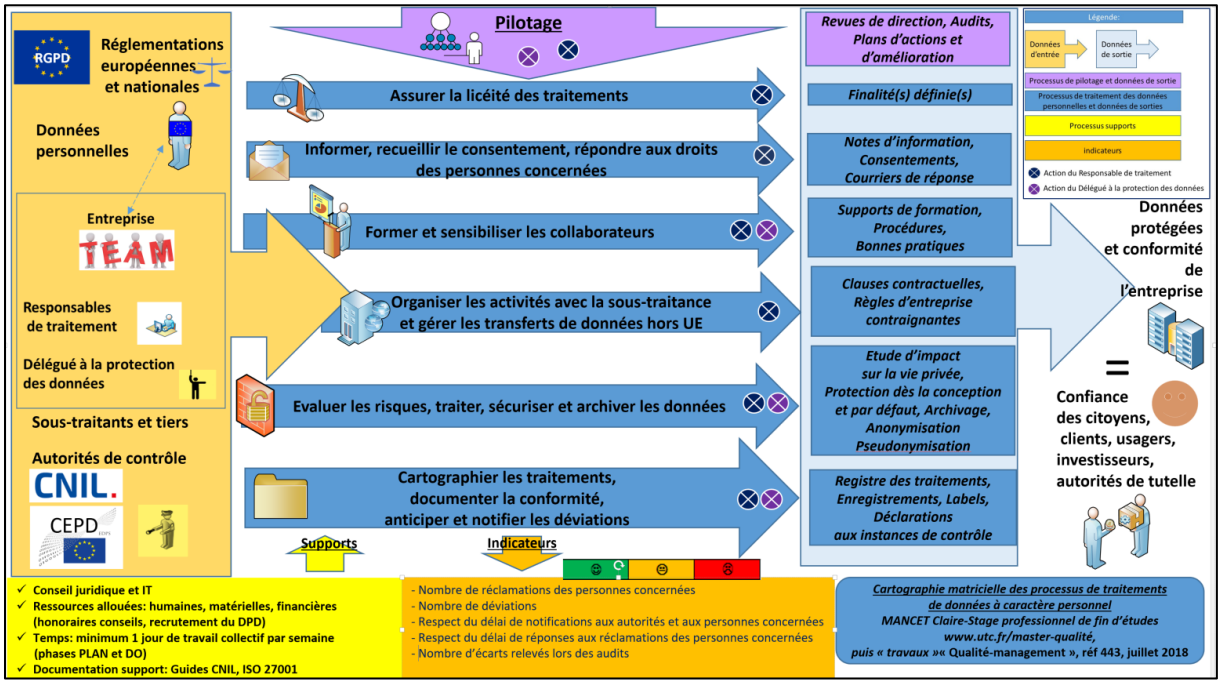


Figure 16 : Cartographie matricielle des processus de traitement

des données à caractère personnel [Source : Auteur]

Une approche processus permet de focaliser les efforts sur les processus clés et l'identification facile des actions d'amélioration et la possibilité pour l'entreprise d'assurer la confiance des parties prenantes [1].

A gauche se trouvent toutes les données d'entrée et parties prenantes dans les processus de traitement des données.

Cette cartographie met en exergue, par des flèches, les différents macroprocessus liés aux traitements des DCP et les documents et livrables attendus en sortie de processus de traitement et permettant d'aboutir à la conformité.

Elle met aussi en évidence le rôle des responsables de traitement, des collaborateurs, du Délégué à la Protection des Données ainsi que de la Direction.

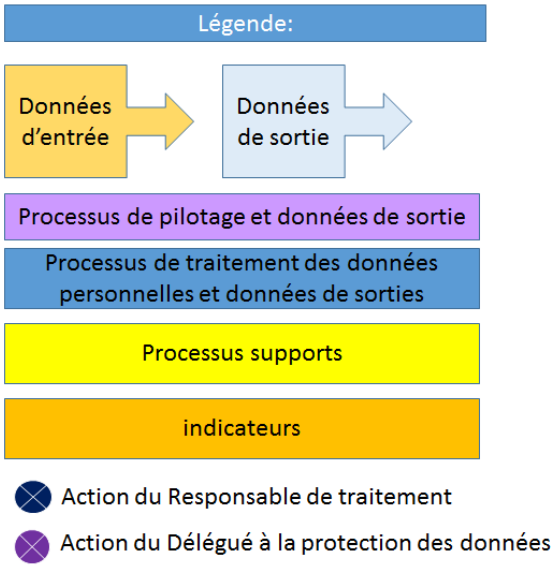


Figure 17 : Légende de la cartographie matricielle des processus de traitement [Source : Auteur]

Dans le cadre du pilotage de l'entreprise et de la gouvernance des traitements, la Direction choisit les indicateurs et revoit leurs résultats aux cours des revues annuelles et suit également les résultats des audits.

Parmi les indicateurs, on retrouve le nombre de réclamations portées par les personnes concernées, les déviations, le respect du délai de notifications des déviations aux autorités de contrôle et aux personnes concernées le cas échéant et bien entendu les écarts relevés lors des audits.

Pour faciliter les audits internes et afin d'évaluer son niveau de conformité au RGPD, un outil d'autodiagnostic a été élaboré.

2. Outil d'autodiagnostic PRIVACY DIAG

Cet outil est destiné à aider les organisations à se mettre en conformité avec le RGPD mais ne saurait se substituer à la réglementation applicable. L'application qui peut être faite de cet outil peut varier d'un organisme à l'autre. Il peut être utilisé pour mener des audits internes sur les différents traitements de données à caractère personnel de l'entreprise.

2.1. Conception de l'outil

La conception de l'outil PRIVACY DIAG a été basée sur une analyse des avantages et des inconvénients et sur une méthode inspirée des travaux d'un groupe d'étudiants datés de 2018 [17].

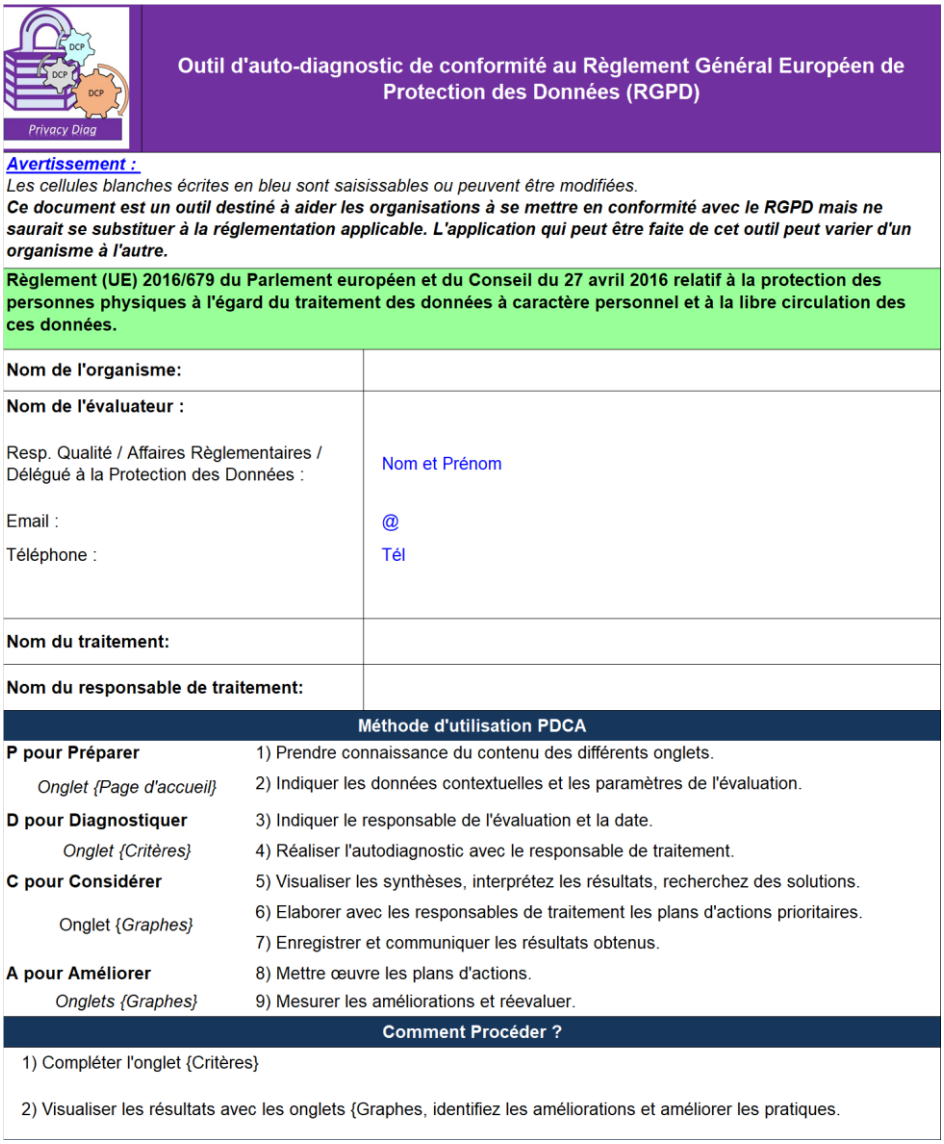
Outil	*Avantages*	*Inconvénients*
Outil d'autodiagnostic de conformité au RGPD	Précis Facile à mettre en place	Durée de réalisation relativement importante Nombre d'exigences du règlement important
Support de l'outil	***Avantages***	***Inconvénients***
Papier	Facile à mettre en place Accessible à tous les collaborateurs Distribution facilitée	Perte ou désorganisation des feuilles possible Nécessite des calculs et analyses manuels
Outil automatisé (type logiciel web)	Facile d'utilisation Calcul et analyse des résultats automatiques Possibilité de modifier les variables du programme	Limité aux systèmes d'exploitation Difficile à mettre en œuvre, nécessite des compétences en programmation. Nécessite de mises à jour progressives Coût d'exploitation pour l'entreprise.
Fichier excel avec MACRO	Simple d'utilisation Calcul automatique Analyse des résultats Accessible Possibilité de modifier facilement le programme	Limité aux systèmes d'exploitation Nécessite des compétences en programmation
Fichier excel, calcul simple	Simple d'utilisation Calcul automatique Analyse des résultats Accessible Pas de programmation	Moins ergonomique Moins attractif

Figure 18 : Avantages et inconvénients de l'outil et ses supports [Source : Auteur, d'après 17]]

L'outil d'autodiagnostic développé dans le cadre du projet correspond à un fichier Excel® contenant des formules de calcul simples et facile d'utilisation. Les chapitres des exigences sont basés les processus exigés par le RGPD.
A chaque processus est associée une liste d'actions à mettre en œuvre pour être en conformité avec le règlement. Les exigences ont été reformulées de façon simple, compréhensible et concise pour permettre une évaluation rapide.

2.2. Structure de l'outil

L'outil Excel® proposé (PRIVACY DIAG) est automatisé et autoporteur de sens. C'est une solution efficace pour mesurer la conformité des processus de traitement des données de personnel de l'organisation. Sa structure est basée sur la cartographie des processus décrite au chapitre III.1.
Il permet d'identifier les axes prioritaires d'amélioration, en une durée de 3 heures maximum (83 critères). L'évaluation peut se faire en plusieurs fois. Il est possible d'arrêter l'évaluation et de la reprendre par la suite.
L'outil est constitué de 3 onglets :
Onglet {Page d'accueil} : Il s'agit d'un onglet interactif dans lequel l'utilisateur peut trouver les instructions d'utilisation de l'outil et les échelles d'évaluation.



Outil d'auto-diagnostic de conformité au Règlement Général Européen de Protection des Données (RGPD)

Avertissement :

Les cellules blanches écrites en bleu sont saisissables ou peuvent être modifiées.

Ce document est un outil destiné à aider les organisations à se mettre en conformité avec le RGPD mais ne saurait se substituer à la réglementation applicable. L'application qui peut être faite de cet outil peut varier d'un organisme à l'autre.

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 circulation des ces données.

Nom de l'organisme:	
Nom de l'évaluateur : Resp. Qualité / Affaires Règlementaires / Délégué à la Protection des Données : Email : Téléphone :	 Nom et Prénom @ Tél
Nom du traitement:	
Nom du responsable de traitement:	

Méthode d'utilisation PDCA

P pour Préparer	1) Prendre connaissance du contenu des différents onglets.
Onglet {Page d'accueil}	2) Indiquer les données contextuelles et les paramètres de l'évaluation.
D pour Diagnostiquer	3) Indiquer le responsable de l'évaluation et la date.
Onglet {Critères}	4) Réaliser l'autodiagnostic avec le responsable de traitement.
C pour Considérer	5) Visualiser les synthèses, interprétez les résultats, recherchez des solutions.
Onglet {*Graphes}*	6) Elaborer avec les responsables de traitement les plans d'actions prioritaires.
	7) Enregistrer et communiquer les résultats obtenus.
A pour Améliorer	8) Mettre œuvre les plans d'actions.
Onglets {Graphes}	9) Mesurer les améliorations et réevaluer.

Comment Procéder ?

1) Compléter l'onglet {Critères}

2) Visualiser les résultats avec les onglets {Graphes, identifiez les améliorations et améliorer les pratiques.

Figure 19 : Page d'accueil de l'outil [15]

Dans la page d'accueil l'utilisateur remplit les données concernant l'organisme, l'évaluateur, le traitement et le responsable de traitement (rubriques présentées dans la figure ci-dessus). Chaque traitement sera évalué pour définir sa conformité aux différents processus tels que définis dans la cartographie des processus de traitement.

On retrouve également dans la page d'accueil les libellés des niveaux de conformité pour la réalisation des actions associées aux processus.

Choix de **conformité**	Taux	Commentaire concernant **l'action** une fois qu'elle sera évaluée
Non Applicable	**NA**	Non Applicable
FAUX	**0%**	L'action n'est pas réalisée selon l'avis du responsable de traitement.
Plutôt faux	**30%**	L'action est réalisée quelques fois ou de manière aléatoire.
Plutôt vrai	**70%**	L'action est réalisée et formalisée.
VRAI	**100%**	L'action est réalisée, formalisée, tracée et améliorée.

Figure 20 : Niveaux de conformité des actions associées au processus [Source : Auteur]

On trouve aussi l'échelle utilisée pour évaluer les niveaux de maturité des processus :

Taux min	Taux max	Niveaux de **maturité**	Commentaire concernant les processus après leur évaluation
0%	9%	Insuffisant	Niveau 1 : Les activités doivent être davantage formalisées.
10%	49%	Informel	Niveau 2: La bonne exécution des activités doit être pérennisée.
50%	89%	Convaincant	Niveau 3 : Les activités doivent être tracées et améliorées.
90%	100%	Conforme	Niveau 4 : Le niveau de conformité au RGPD est atteint et il faut pérenniser la démarche.

Figure 21 : Niveaux de maturité des processus de traitement [Source : Auteur]

Onglet {Critères} : L'évaluateur trouve une grille d'évaluation comportant 83 critères à évaluer. Il s'agit des actions associées à chaque processus de traitement (matérialisées en gris).
Il renseigne ses choix dans la colonne « Evaluation » à l'aide du menu déroulant. Les éléments à prendre en compte pour l'évaluation se trouvent dans la colonne « Indications ».
A la saisie du choix, le taux de conformité se calcule automatiquement. Lorsque toutes les actions associées à un processus sont évaluées, le taux correspondant au niveau de maturité du processus s'implémente dans les cellules des colonnes « Evaluation», « Taux » et « libellé de l'évaluation » matérialisées en orange dans la figure ci-dessous.

Processus et actions associées	Indications	Evaluation	Taux %	Libellé de l'évaluation
1-Assurer la licéité du traitement initial et du traitement ultérieur	Le traitement est licite s'il fait l'objet d'un consentement ou s'il correspond à un intérêt légitime ou à une obligation légale	Convaincant	68%	**Niveau 3 : Les activités doivent être tracées et améliorées.**
Les personnes concernées ont donné leur consentement au traitement de leur DCP pour une ou plusieurs finalités données OU (Voir §6.1b)		VRAI	100%	L'action est réalisée, formalisée, tracée et améliorée.
Les personnes concernées sont parties d'un contrat pour lequel le traitement des données est nécessaire.			70%	L'action est réalisée et formalisée.
Le traitement répond à une obligation légale ou réglementaire.	Ex: pharmacovigilance, transparence des liens		70%	L'action est réalisée et formalisée.
Le traitement est nécessaire à la sauvegarde des intérêts vitaux des personnes concernées ou d'une autre personne.	Ex: traitement nécessaire à des urgences sanitaires ou humanitaires	Plutôt faux	30%	L'action est réalisée quelques fois ou de manière aléatoire.
Le traitement est nécessaire à une mission d'intérêt public ou relevant de l'exercice de l'autorité publique;		Plûtot vrai	70%	L'action est réalisée et formalisée.
Le traitement est effectué à des fins légitimes	Ex: traitement à des fins de marketing direct ou de prévention des fraudes, transmission de DCP au sein d'un groupe d'entreprise	VRAI	100%	L'action est réalisée, formalisée, tracée et améliorée.

Choix de conformité
Non Applicable
FAUX
Plutôt faux
Plûtot vrai
VRAI

Figure 22 : Grille d'évaluation [Source : Auteur]

Onglet {Graphique} :

L'onglet Résultats comprend les résultats obtenus pour chaque processus de traitement.

Il comprend un histogramme présentant le nombre d'actions non évaluées, le nombre d'actions non applicables, le nombre d'actions pour lesquelles on trouvera respectivement les réponses « faux », « plutôt faux », « vrai », « plutôt vrai ».

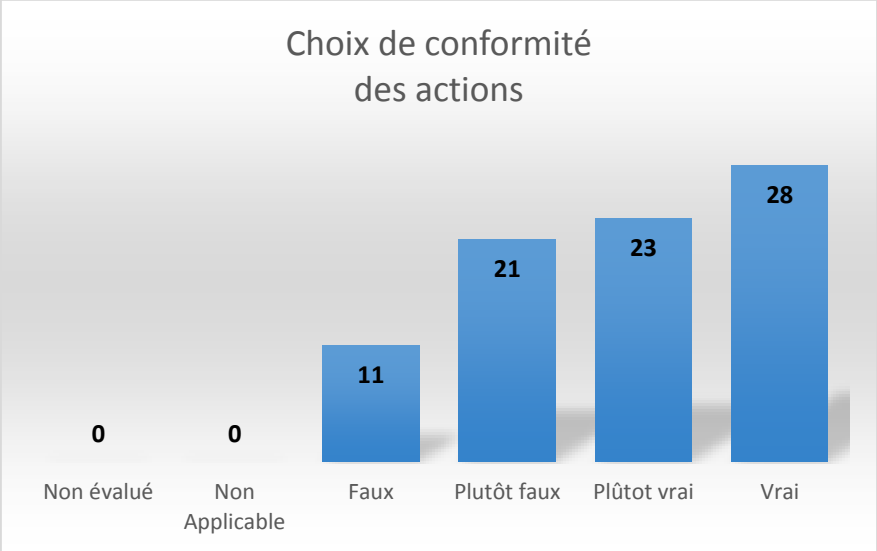


Figure 23 : Niveaux de conformité des actions évaluées [Source : Auteur]

Un autre histogramme comprend les résultats des niveaux de maturité des processus de traitement.

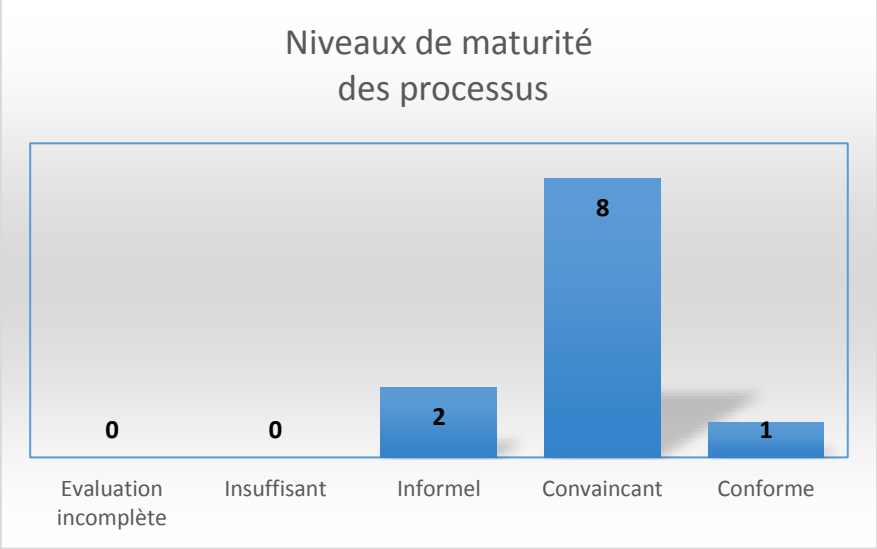


Figure 24 : Niveaux de maturité des processus de traitement [Source : Auteur]

Enfin, l'évaluateur retrouve un diagramme présentant les résultats pour les différents processus de traitement. Cette présentation visuelle lui permet de cibler les processus sur lesquels l'entreprise et le responsable de traitement vont devoir travailler en priorité pour atteindre un niveau de conformité satisfaisant.

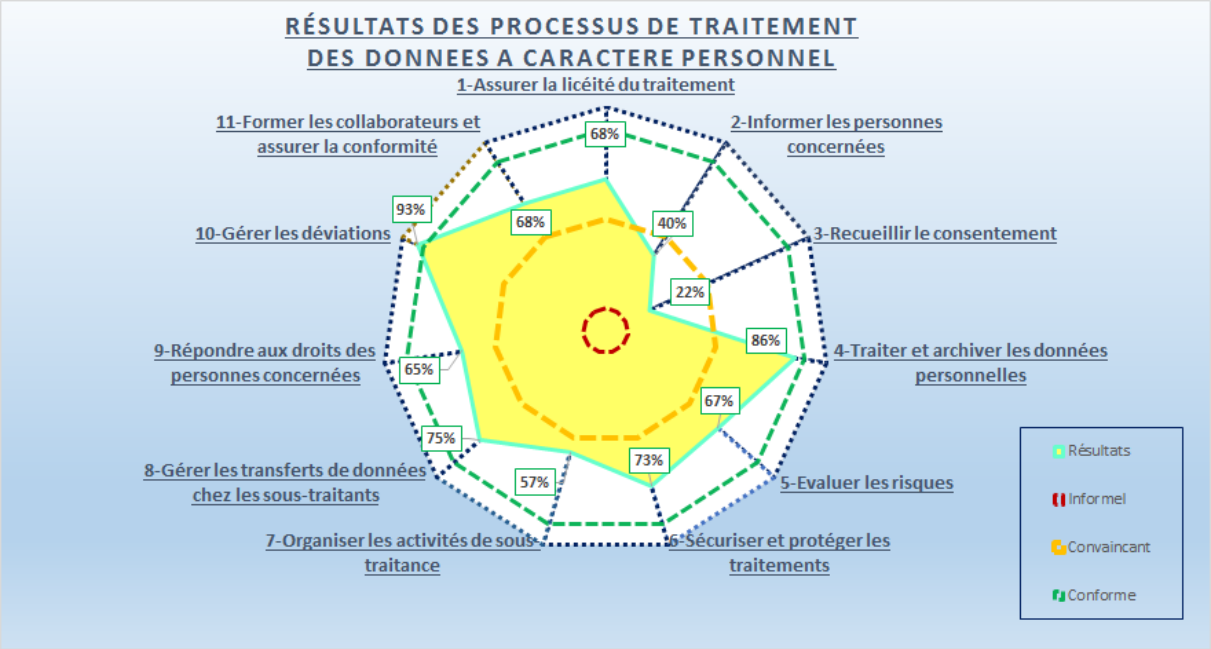


Figure 25 : Exemple de diagramme des niveaux de conformité des processus de traitement [Source : Auteur]

Après avoir revu les résultats, l'évaluateur et le responsable de traitement pourront établir les plans d'actions d'amélioration. Pour cela, un tableau est à leur disposition dans l'onglet « Résultats ».

COMMENTAIRES sur les RÉSULTATS obtenus			
Commentaires (collectifs si possible) :			
Plan d'actions de progrès envisagées :			
Action	**Pilote (qui)**	**Échéance**	**Résultats après actions**

Figure 26 : Plan d'actions d'amélioration [Source : Auteur]

L'outil «PRIVACY DIAG » permet donc une évaluation partielle ou totale de 83 critères (3h pour une évaluation totale au lieu de 6 heures environ pour 137 paragraphes « Considérant », et 99 articles du RGPD). Les résultats sont affichés sous forme de tableaux, histogrammes et diagrammes radar afin de permettre l'interprétation rapide pour identifier les plans d'actions prioritaires.
L'utilisation de cet outil permet un gain de temps pour les responsables de traitement et les auditeurs.

Conclusion

A compter du 25 mai 2018, toutes les entreprises traitant des données à caractère personnel devront se conformer au règlement européen de protection des données. Ce règlement sera également transposé dans la loi française Informatique et Libertés.

La mise en conformité avec le RGPD est une opportunité pour les entreprises d'améliorer leur image et leur compétitivité et de créer de la valeur en améliorant leurs pratiques numériques et digitales. En instaurant un cadre juridique harmonisé, il va permettre un développement du numérique.

Les travaux présentés dans ce mémoire fournissent aux entreprises un exemple de démarche qualité de mise en conformité avec un référentiel complexe, en l'occurrence le RGPD.

La démarche PDCA décrite et la cartographie des processus de traitement fournie pourront les aider à mettre en œuvre leur propre démarche et à communiquer sur les enjeux du RGPD.

Par ailleurs, les responsables de traitement et les Délégués à la Protection des Données pourront utiliser l'outil d'autodiagnostic « Privacy Diag » développé dans le cadre de ce projet pour évaluer les processus de traitement et réaliser des audits internes.

Cet outil excel simple et flexible pourra évoluer et être modifié et complété par ses utilisateurs, suivant les textes attendus pour compléter le RGPD, tels que la modification de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et le projet de règlement « e-privacy ».

Références bibliographiques :

[1] « NF EN ISO 9000 - Systèmes de management de la qualité - Principes essentiels et vocabulaire ». Afnor Editions, www.afnor.org, 15-oct-2015.
[2] JOUE, « 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 circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ». .
[3] « Infographie : Les données à caractère personnel sont entrées dans l'ère du RGPD ». CLUSIF, janv-2018.
[4] CNIL, « Guide pratique de sensibilisation au RGPD pour les PME et TPE ». www.cnil.fr.
[5] « cnil-pia-3-fr-basesdeconnaissances.pdf ». .
[6] « Guide pratique sur la protection des données personnelles ». .
[7] Pharmès, « Règlement européen sur la protection des données personnelles: tableau des dispositions commenté ». www.pharmès.fr, févr-2018.
[8] SNITEM, « Nouveau règlement européen sur la protection des données personnelles: définition, principes et nouvelles obligations (Foire aux Questions). » SNITEM, http://www.snitem.fr/, 12-déc-2017.
[9] G. DESGENS-PASANAU et CNAM, « MOOC-Protection des données personnelles : le nouveau droit », avr-2018. [En ligne]. Disponible sur: //www.fun-mooc.fr/courses/course-v1:CNAM+01032+session01/about. [Consulté le: 05-mai-2018].
[10] « CNIL_Formulaire_Notification_de_Violations.pdf ». .
[11] CNIL, « RGPD : se préparer en 6 étapes | CNIL ». .
[12] CNIL, *Outil PIA : téléchargez et installez le logiciel de la CNIL | CNIL*. www.cnil.fr.
[13] « cnil-pia-1-fr-methode.pdf ». .
[14] « cnil-pia-2-fr-modeles.pdf ». .
[15] C. Mancet, « Règlement Général de Protection des Données personnelles : Démarche et outil qualité pour la mise en conformité de l'entreprise », Université de Technologie de Compiègne, Master Qualité et Performance dans les Organisations (QPO), Mémoire d'Intelligence Méthodologique de stage professionnel de fin d'études, www.utc.fr/master-qualité, puis « Travaux » « Qualité-Management », réf. nr 443, juill. 2018.
[16] « NF ISO/CEI 27001 - Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information - Exigences ». Editions Afnor, Paris, www.afnor.org, 27-déc-2013.
[17] El Marsaoui, Lamkadem, Mancet, Meksi, « Référentiels qualité majeurs pour les entreprises biomédicales », Université de Technologie de Compiègne, Master Qualité et Performance dans les Organisations (QPO), Master Technologies et Territoires de Santé (TTS), Mémoire d'Intelligence Méthodologique du projet d'intégration, http://www.utc.fr/master-qualite, puis « Travaux » « Qualité-Management » réf n°424, janv. 2018.