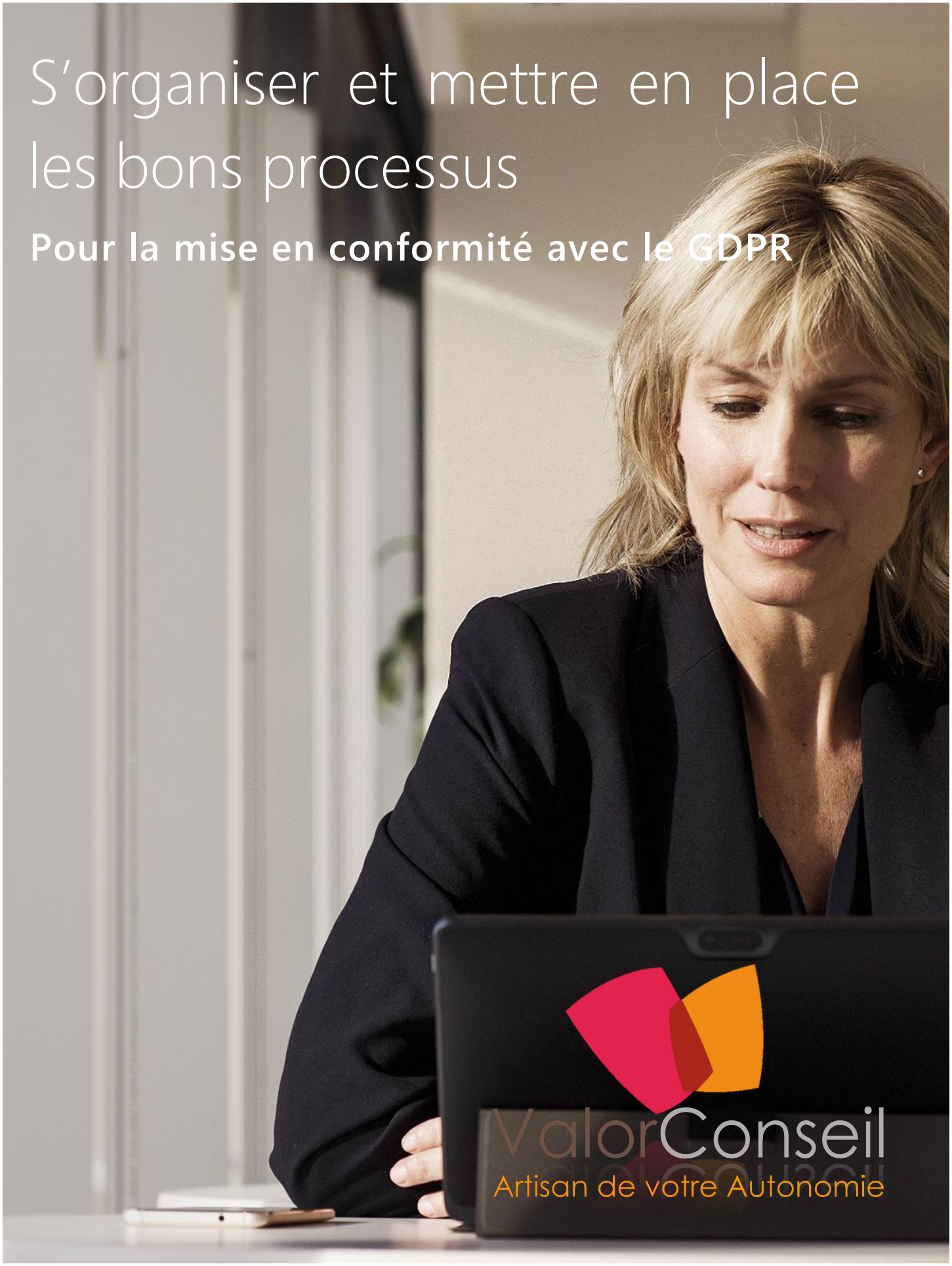
S'organiser et mettre en place les bons processus

Pour la mise en conformité avec le GDPR



ValorConseil

Artisan de votre Autonomie

Cette page est laissée intentionnellement blanche.

ValorConseil
Artisan de votre Autonomie

Table des matières

Avertissement

Ce livre blanc est un commentaire sur le Règlement Général sur la Protection des Données (RGPD, plus communément désigné par son acronyme anglais GDPR) ainsi que Microsoft l'interprète, à la date de publication. Nous avons passé beaucoup de temps à réfléchir aux objectifs du GDPR et à sa signification. Mais la mise en œuvre du GDPR ne peut que se fonder pour l'essentiel sur des faits établis ; or, certains des aspects et interprétations du GDPR ne sont pas encore bien établis.

Par conséquent, le présent document est fourni exclusivement à titre purement informatif et ne saurait être considéré comme constituant un quelconque avis juridique ou permettant de déterminer comment le GDPR pourrait s'appliquer à vous et à votre organisation. Nous vous encourageons à collaborer avec un professionnel dûment qualifié afin d'aborder le GDPR, de vérifier la manière dont ce Règlement s'appliquera spécifiquement à votre organisation et de déterminer la meilleure façon d'en assurer la conformité.

MICROSOFT EXCLUT TOUTE GARANTIE, EXPRESSE, IMPLICITE OU LÉGALE, RELATIVE AUX INFORMATIONS CONTENUES DANS CE LIVRE BLANC. Le livre blanc est fourni « EN L'ÉTAT » sans garantie d'aucune sorte et ne saurait être interprété comme un engagement de la part de Microsoft.

Microsoft ne peut pas garantir la véracité des informations présentées. Les informations de ce livre blanc, comprenant notamment et sans que la liste ne soit exhaustive, les références de site web Internet et URL, sont susceptibles de changer à tout moment, sans préavis. De plus, les avis exprimés dans ce livre blanc représentent la vision actuelle de Microsoft France sur les points cités à la date de publication du présent livre blanc et sont susceptibles de changer à tout moment sans préavis.

Publication : Novembre 2017
Version 1.0a

Résumé

À l'ère de la transformation numérique, la protection de la vie privée et l'amélioration de la sécurité sont devenues des sujets de société incontournables. Le prochain Règlement Général sur la Protection des Données (RGPD, plus communément désigné par son acronyme anglais « GDPR ») définit une nouvelle étape importante pour les droits à la vie privée, la sécurité et la conformité.

Le GDPR impose de nombreuses exigences et obligations pour les organisations à travers le monde. Le respect de cette réglementation nécessitera des investissements importants dans la gestion des données et leur protection pour un très grand nombre d'organisations et d'entreprises.

Les clients de Microsoft qui sont soumis au GDPR, qu'ils effectuent des traitements en interne, dans le cloud ou en mode hybride, devront s'assurer que les données personnelles au sein de leurs systèmes qui participent aux traitements de ces données sont correctement traitées et protégées selon les principes du GDPR. Cela signifie que de nombreux clients devront réviser ou modifier leurs procédures de traitement de données, l'implémentation de ces traitements, en particulier en ce qui concerne la sécurité de ces derniers comme stipulé dans le GDPR.

Microsoft a une expérience significative dans la gestion des principes de protection des données et de conformité à des réglementations complexes. Microsoft s'est engagé à partager cette expérience avec ses clients, afin de les aider à respecter les objectifs et les exigences de protection de la vie privée du GDPR. Dans ce contexte, ce document traite de la façon d'initier et d'organiser un programme GDPR afin de démarrer le cheminement vers la conformité avec le GDPR.

Introduction

Après plus de quatre années de négociations qui ont débuté lorsque la Commission a présenté ses propositions en janvier 2012, le Conseil de l'Europe a adopté le 14 avril 2016 le Règlement Général sur la Protection des Données[1] (RGPD), plus communément désigné par son acronyme anglais « GDPR » (et ainsi dénommé dans la suite de ce document) pour General Data Protection Regulation.

Le Règlement est entré en vigueur le 24 mai de cette même année et sera applicable directement dans tous les États membres après un délai de 2 ans, soit le 25 mai 2018 et donc dans moins d'un an à la date de publication de ce livre blanc.

A l'âge de la transformation numérique, la protection de la vie privée et l'amélioration de la sécurité sont devenues des préoccupations majeures. Depuis la Directive 95/46/CE[2] du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, plus de vingt ans se sont écoulés.

Nous sommes depuis entrés en effet dans une ère nouvelle, l'ère numérique où la donnée est désormais au centre de tout. Les masses de données de toutes sortes disponibles, la puissance de calcul à disposition – avec les évolutions des processeurs, GPU notamment, et l'avènement des environnements d'informatique en nuage (services cloud) –, et donc les usages induits sont aujourd'hui fort différents. Les données alimentent les algorithmes prédictifs entrainés et sont au cœur des prises de décision automatisées dans notre quotidien. La disruption est telle qu'on qualifie généralement cette ère numérique nouvelle de 4ième révolution industrielle.

Une révision de la Directive 95/46/CE s'imposait donc avec également l'objectif d'homogénéiser une mosaïque de réglementations imposées dans les différents états de l'Union européenne et celui de mettre à disposition une autorité de surveillance unique plutôt que 28[3].

> Grâce à ce règlement général, avoir un niveau élevé et uniforme de protection des données à travers l'UE deviendra une réalité. Il s'agit d'une victoire pour le Parlement et d'un farouche 'oui' européen à des droits très forts des consommateurs et à la concurrence à l'ère numérique. Les citoyens pourront décider eux-mêmes des informations personnelles qu'ils souhaitent partager
>
> Jan Philipp Albrecht, en charge de la législation au Parlement

[1] REGLEMENT (UE) 2016/679 DU PARLEMENT EUROPEEN ET DU CONSEIL DU 27 AVRIL 2016 RELATIF A LA PROTECTION DES PERSONNES PHYSIQUES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL ET A LA LIBRE CIRCULATION DE CES DONNEES, ET ABROGEANT LA DIRECTIVE 95/46/CE (REGLEMENT GENERAL SUR LA PROTECTION DES DONNEES) : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32016R0679

[2] DIRECTIVE 95/46/CE DU PARLEMENT EUROPEEN ET DU CONSEIL, DU 24 OCTOBRE 1995, RELATIVE A LA PROTECTION DES PERSONNES PHYSIQUES A L'EGARD DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL ET A LA LIBRE CIRCULATION DE CES DONNEES : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:31995L0046

[3] LES NOUVELLES REGLES DE L'UE SUR LA PROTECTION DES DONNEES PLACENT LES CITOYENS AUX COMMANDES : http://www.europarl.europa.eu/news/fr/news-room/20160413BKG22980/nouvelle-l%C3%A9gislation-europ%C3%A9enne-sur-la-protection-des-donn%C3%A9es

Le GDPR s'intéresse fondamentalement à la question de protéger la vie privée des personnes et de permettre l'exercice des droits en la matière. Le GDPR établit pour cela un ensemble d'exigences globales des plus strictes qui s'imposent aux organisations en termes de protection de la vie privée. Ces exigences régissent la façon dont vous devez gérer et protéger les données personnelles des citoyens européens tout en respectant leurs choix individuels, peu importe où que ces données soient traitées, stockées, ou envoyées.

Ainsi, Microsoft et ses clients sont désormais engagés dans un voyage pour atteindre les objectifs de protection de la vie privée fixés par le GDPR. Chez Microsoft, nous estimons que la vie privée est un droit fondamental, et nous pensons que ce Règlement constitue une avancée importante en termes de protection de la vie privée et des droits associés. Nous reconnaissons aussi dans le même temps que le GDPR imposera des changements significatifs aux organisations du monde entier.

Dans ce contexte, et comme le souligne Brad Smith, Président et « Chief Legal Officer » de Microsoft Corporation, « le nouveau Règlement élève la barre de façon significative quant aux droits en matière de protection de la vie privée, à la sécurité et à la conformité ».

Nombre de questions s'imposent plus que jamais, questions qui impliquent bien sûr une réponse conforme aux objectifs et exigences du GDPR, comme notamment de façon non-exhaustive :

- *Savez-vous où résident les données à caractère personnel de votre entreprise et qui a accès à ces données ?*
- *Contrôlez-vous qui a accès à vos données à caractère personnel et comment elles sont utilisées en fonction de l'évaluation du risque en temps réel ?*
- *Pouvez-vous classifier, protéger et appliquer des actions guidées par des politiques sur vos données, terminaux, entre les applications, en tout lieu, au repos et en transit ?*
- *Pouvez-vous automatiquement détecter une fuite de données ou usurpation d'identité ? Etes-vous capable de répondre adéquatement à une violation de données personnelles ?*
- *Revoyez-vous et mettez-vous à jour en permanence vos politiques et pratiques de protection de données ?*

Ces questions se posent à un grand nombre d'organisations puisque toutes celles qui manipulent des données de citoyens européens se doivent d'être en conformité avec le GDPR. Rien que pour l'Europe, cela ne concerne potentiellement pas moins de 26 millions d'entreprises.

Par ailleurs, l'impact de la mise en œuvre du GDPR sera loin d'être neutre et, ce d'autant que le niveau des amendes franchit un pas décisif puisque le montant des sanctions pourra s'élever à 20 millions d'Euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu[4].

> **Remarque** Il s'agit des amendes maximales car elles seront modulées en fonction de critères tels que la nature, la gravité et la durée de la violation, le fait que la violation ait été commise délibérément ou par négligence, le non-respect d'une injonction ou le transfert des données dans un pays tiers, etc.

[4] ARTICLE 83 - CONDITIONS GENERALES POUR IMPOSER DES AMENDES ADMINISTRATIVES : https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre8#Article83

Pour autant, force est de constater que les niveaux d'appréhension et de préparation des organisations ne sont pas forcément alignés. Le Gartner estime ainsi en mai 2017 qu'au mieux seules 50 % des entreprises seront prêtes le 25 mai 2018[5].

Ce constat est corroboré par les résultats du Global Databerg Report de Veritas, qui a sondé en 2016 – la période de référence n'est donc pas tout à fait la même – plus de 2 500 décideurs IT en Europe, au Moyen-Orient, en Afrique, aux États-Unis et en Asie Pacifique, et qui révèle que 54% d'entre eux n'ont pas encore mis en place les mesures nécessaires pour être conformes au GDPR[6]. On peut donc se demander si les organisations et les entreprises ont vraiment appréhendé tous les enjeux associés.

Qu'en est-il des entreprises françaises ? Selon l'étude de SerdaLAB/Arondor[7] datée de février 2017, on retrouve cette même situation puisque 45% des organisations et entreprises ne savent tout simplement pas que le GDPR entrera en application le 25 mai 2018 prochain, 43% n'ont pas encore réellement évalué l'impact qu'il aura sur leur fonctionnement et 38% pensent tranquillement qu'elles n'honoreront pas l'échéance !

Enfin, l'étude ORGANISATIONAL READINESS FOR THE EUROPEAN UNION GENERAL DATA PROTECTION REGULATION[8] menée fin 2016 par la société AvePoint auprès de 223 entreprises multinationales fait ressortir les trois points ayant le plus d'impact : la mise en place d'un programme de gestion des données personnelles pour respecter les exigences du GDPR, suivi de la revue des aspects contractuels avec les sous-traitants et enfin la sécurité des données et la notification.

Cela illustre, s'il en était besoin, que l'une des questions centrales pour les organisations et entreprises conscientes de leur responsabilité et obligations à venir (pour les autres, il est encore temps d'une prise de conscience bienvenue !) est la suivante :

Comment s'organiser et démarrer dans les meilleurs délais pour être prêt ?

En effet, même si la crainte des sanctions financières risque de donner une impulsion pour s'engager dans ce voyage de la mise en conformité au GDPR, il reste difficile pour les organisations et entreprises de savoir comment aborder de manière pratique ce nouveau Règlement qui s'impose à elles.

Si l'on trouve d'ores et déjà beaucoup de littérature synthétisant les principes du GDPR, force est de constater que peu s'attardent sur la description d'une approche un peu détaillée puisqu'elle constitue la valeur ajoutée même de ces sociétés de conseil ou fournisseurs de solutions.

Objectifs du livre blanc

Ce livre blanc vise donc à proposer une trame de programme permettant de tracer une trajectoire de mise en conformité au GDPR en abordant des questions importantes comme **la relation avec les sous-traitants, la sécurité des données, la notification auprès de l'autorité de contrôle pour ne reprendre ici que les points clés de l'étude ci-avant.**

---

[5] GARTNER SAYS ORGANIZATIONS ARE UNPREPARED FOR THE 2018 EUROPEAN DATA PROTECTION REGULATION : http://www.gartner.com/newsroom/id/3701117

[6] PLUS DE LA MOITIE DES ENTREPRISES NE SONT PAS PRETES POUR GDPR : http://www.infodsi.com/articles/166374/plus-moitie-entreprises-sont-pas-prete-gdpr.html

[7] PROTECTION DES DONNEES : GROS RETARD POUR BEAUCOUP D'ORGANISATIONS FRANÇAISES : http://www.influencia.net/fr/actualites/media-com,etudes,protection-donnees-gros-retard-pour-beaucoup-organisations-francaises,7364.html

[8] ORGANISATIONAL READINESS FOR THE EUROPEAN UNION GENERAL DATA PROTECTION REGULATION : https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2016/11/cipl_avepoint_gdpr_readiness_survey_report_1107_final-c.pdf

Si toutes les organisations (ou entreprises) ne sont pas concernées de la même façon par le GDPR de par la nature de leurs proposition(s) de valeur et de leurs activités, il est vraisemblable que, d'une façon générale, de multiples processus métier collectent, font usage dans des opérations de traitement, et/ou stockent des données personnelles. La mise en conformité de ces traitements de données personnelles se traduira certainement par de multiples projets à conduire. C'est pourquoi nous souhaitons employer ici le qualificatif de programme, un programme étant constitué de multiples projets.

Organisation du livre blanc

De façon à répondre aux objectifs présentés précédemment, et au-delà d'un rappel des engagements de Microsoft envers le GDPR, ce document est organisé selon les sections suivantes :

- VOUS AVEZ DIT DONNEES PERSONNELLES ?
- QUELQUES RAPPELS SUR LE GDPR
- INITIER ET CONDUIRE UN PROGRAMME GDPR
- PLANIFIER LE PROGRAMME GDPR
- METTRE EN ŒUVRE LE PROGRAMME GDPR
- VERIFIER LE PROGRAMME GDPR
- AJUSTER LE PROGRAMME GDPR
- UN RAPIDE REGARD SUR LES RECOMMANDATIONS DE LA CNIL.

Nous espérons que l'organisation ainsi proposée apportera progressivité et clarté dans les différents domaines abordés.

Audience de ce livre blanc

Ce document est destiné aux Responsables de la Sécurité du Système d'Informations (RSSI), Directeurs de la gestion des risques, Directeurs de la gestion de la vie privée, Directeurs de la conformité, Directeurs des Données, Directeurs de l'information numérique, professionnels de l'informatique, spécialistes de la sécurité et aux architectes des systèmes qui s'intéressent à la compréhension des piliers du GDPR et à la manière de s'assurer que les standards et les pratiques de l'organisation en termes de sécurité et de protection de la vie privée permettent de se conformer au GDPR.

Rappels des engagements de Microsoft envers le GDPR

Nous avons souligné notre engagement envers le GDPR et la façon dont nous soutenons nos clients dans le billet de blog GET GDPR COMPLIANT WITH THE MICROSOFT CLOUD[9] par notre responsable de la protection de la vie privée Brendon Lynch[10] et le billet de blog EARNING YOUR TRUST WITH CONTRACTUAL COMMITMENTS TO THE GENERAL DATA PROTECTION REGULATION[11] de Rich Sauer[12], Vice-Président et avocat général adjoint de Microsoft.

Cet engagement figure depuis le 1er septembre dans les termes des services en ligne[13] (Online Services Terms en anglais ou OST).

Bien que votre voyage vers GDPR puisse vous sembler difficile, nous sommes là pour vous aider.

Remarque Pour des informations spécifiques sur le GDPR, nos engagements et le début de votre voyage, visitez la section GDPR[14] dédiée du Centre de confiance[15] (Trust Center) Microsoft.

Remarque Alors que l'utilisation de services de cloud se généralise, la « conformité » devient une question récurrente et un impératif pour nos clients afin de leur offrir le niveau de transparence dont ils ont besoin. Le mot revêt différentes significations, par exemple comme outil d'évaluation des services de cloud ou comme moyen de décrire les attentes quant à l'exploitation de ces services. Microsoft s'engage tout naturellement à offrir à nos clients toutes les informations de conformité dont ils ont besoin :

« Les personnes n'utiliseront pas une technologie dans laquelle elles n'ont pas confiance. Et elles ne peuvent pas faire confiance à une technologie qu'elles ne comprennent pas. »

- Brad Smith, Président de Microsoft

Comme chacun sait, la confiance ne se décrète pas, elle se mérite et s'entretient. Microsoft a ainsi créé un Centre de confiance (Trust Center) pour l'ensemble des services de cloud de Microsoft afin d'aider nos clients à comprendre les aspects relatifs à la transparence, la sécurité, la confidentialité et la conformité vis-à-vis des services de cloud proposés. Microsoft s'engage tout naturellement à offrir à nos clients toutes les informations dont ils ont besoin pour appréhender et évaluer les aspects précédents :

Ce centre référence ainsi l'ensemble des standards et normes respectés par nos codes de bonne pratique, contrôles et processus opérationnel et proposent des informations et ressources complémentaires. D'une façon générale, le centre de confiance permet d'accéder à de la documentation relative à la conformité ainsi qu'à des informations sur la façon dont Microsoft gère les données stockées pour ses services de cloud. Ces centres de confiance fournissent des liens vers des tableaux de bord pour les clients, avec des informations à jour sur le temps de disponibilité des services et l'emplacement des données.

---

[9] GET GDPR COMPLIANT WITH THE MICROSOFT CLOUD : https://blogs.microsoft.com/on-the-issues/2017/02/15/get-gdpr-compliant-with-the-microsoft-cloud/#4J5lDmd47PkIv6xL.99

[10] Blog de Brendon Lynch : https://blogs.microsoft.com/on-the-issues/author/brendonlynch/

[11] Earning your trust with contractual commitments to the General Data Protection Regulation : https://blogs.microsoft.com/on-the-issues/2017/04/17/earning-trust-contractual-commitments-general-data-protection-regulation/#6QbqoGWXCLavGM63.99

[12] Blog de Rich Sauer : https://blogs.microsoft.com/on-the-issues/author/rsauer/

[13] LICENSING TERMS AND DOCUMENTATION : http://go.microsoft.com/?linkid=9840733

[14] Section GDPR du Centre de confiance Microsoft : http://www.microsoft.com/GDPR

[15] Centre de confiance Microsoft : https://www.microsoft.com/fr-fr/trustcenter

Remarque A cet égard, nous souhaitons souligner, qu'en avril 2014, le Groupe de l'Article 29 (ou G29), nommé ainsi en référence à l'article 29 de la Directive 95/46/CE – et qui représente les 28 autorités de protection des données personnelles dans l'Union Européenne - a considéré, à la suite d'une revue exhaustive des contrats Microsoft pour ses services Microsoft Online, que ces derniers répondaient aux plus hauts standards définis par les réglementations européennes en matière de protection des données personnelles.

En conséquence, Microsoft est la première entreprise à avoir reçu une telle appréciation, ce qui a des conséquences significatives pour les organisations publiques et privées en Europe et partout dans le monde, quelle que soit leur taille, qui souhaitaient être rassurées sur la protection de leurs données et la conformité de celle-ci au cadre légal.

Vous avez dit données personnelles ?

Les données personnelles sont définies de façon très large dans le GDPR. Les données personnelles entrant dans le périmètre peuvent inclure, mais ne sont pas limitées, aux données suivantes :

- Nom,
- Numéro d'identification (ID),
- Adresse mèl,
- Identifiant utilisateur (UID),
- Messages sur les médias sociaux,
- Informations génétiques, physiologiques ou physiques,
- Informations médicales,
- Emplacement,
- Détails bancaires,
- Adresse IP,
- Cookies.

> ### Que dit GDPR ?
>
> **Article 4 - Définitions**
> «**données à caractère personnel**», **toute information se rapportant à une personne physique identifiée ou identifiable** (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une 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

Ceci englobe certes les notions connues de données personnelles identifiables mais pas uniquement !

Les « données liées » sont aussi des données personnelles. Il s'agit de données relatives à une personne dont l'identité est connue :

- Données qui identifient directement une personne comme un numéro de téléphone, un UID permanent.
- Liens directs à une information qui identifie la personne comme l'historique de navigation, l'emplacement, les données d'utilisation ou d'erreur, ou tout autre donnée stockée avec un UID permanent.

C'est la même chose pour les « données liables ». Ce sont, dans la pratique, des données qui peuvent être utilisées de manière systématique pour créer ou recréer un lien avec les informations d'identification :

- UID permanents qui sont des condensés de (nombres basés sur des) ID liés.
- Toutes données stockées avec un GUID représentant une utilisation ou un appareil unique.

Quelques rappels sur le GDPR

Fondés sur 173 considérants préliminaires – un considérant peut contenir des explications additionnelles d'un article -, 99 articles distillés sur 10 chapitres, 88 pages égrènent les quelques 160 exigences que comportent ce nouveau Règlement européen. Nous verrons à la suite de cette section les points les plus saillants du Règlement qui peuvent éclairer la proposition de programme GDPR telle qu'elle est articulée dans la suite de ce livre blanc.

Quelques définitions structurantes

L'article 4[16] introduit les différentes rôles et concepts de protection des données à caractères personnel et en particulier ceux du responsable de traitement et sous-traitant.

> **Que dit le GDPR ?**
>
> **Article 4 - Définitions**
>
> «**responsable du traitement**», la 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**; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre;
>
> «**sous-traitant**», 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;
>
> «**destinataire**», la 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. […];
>
> «**tiers**», une 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;

C'est au responsable du traitement qu'incombe l'obligation de mettre en œuvre les mesures techniques et organisationnelles appropriées pour s'assurer qu'un traitement des données personnelles est conforme aux objectifs et exigences du GDPR. Il doit, de plus, être en mesure de le démontrer à tout moment. Lorsqu'il fait appel à des sous-traitants, il doit s'assurer que ceux-ci offrent les garanties suffisantes pour lui permettre d'être conforme et qu'ils traitent les données personnelles selon ses instructions, plus particulièrement concernant les transferts en dehors de l'Union Européenne.

Le sous-traitant doit assurer un rôle de conseil vis-à-vis du responsable du traitement pour l'aider à garantir ses obligations quant à la sécurité des données – par exemple par la mise en œuvre de la pseudonymisation – où lorsqu'une consultation préalable de l'autorité de contrôle est nécessaire dans le cas de traitement à risque élevé. Pour la France, l'autorité de contrôle est la CNIL (Commission Nationale Informatique & Libertés)[17]. Le Règlement impose que les sous-traitants non établis dans l'Union Européenne doivent désigner un représentant dans l'Union.

[16] ARTICLE 4 – DEFINITIONS : https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre1#Article4

[17] CNIL : https://www.cnil.fr

Remarque Le principe de pseudonymisation, largement cité dans le Règlement, rend possible d'éliminer le caractère nominatif des données en utilisant des pseudonymes. Pour de plus amples informations sur le sujet, vous pouvez consulter la norme ISO/IEC CD 20889[18] INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- PRIVACY ENHANCING DATA DE-IDENTIFICATION TECHNIQUES (actuellement en cours d'élaboration).

Champ d'application extraterritorial

Bien qu'il s'agisse d'un Règlement européen, le GDPR s'octroie une portée mondiale dès lors qu'il s'agit de traiter des données personnelles de résidents de l'Union Européenne. En effet, le Règlement s'applique aux responsables de traitement ou sous-traitants situés dans l'Union Européenne, même si le traitement des données à caractère personnel est effectué en-dehors de l'Union Européenne, mais également lorsque ces derniers sont situés en-dehors de l'Union Européenne.

Principes relatifs au traitement des données personnelles

La responsabilité constitue le « maître mot » au sein du GDPR.

> La responsabilité, ce n'est pas simplement ce que nous faisons, mais c'est aussi ce que nous ne faisons pas, et pour lequel nous sommes responsables
>
> Molière

Les exigences se placent en effet sous l'égide d'une responsabilité accrue aussi bien de l'entreprise que de ses sous-traitants. (On parle de coresponsabilité).

L'article 5[19] exige en effet que vous soyez en **mesure de démontrer** que vous vous conformez aux six principes énoncés et précise explicitement que ceux-ci sont de VOTRE responsabilité :

1. Observer une exigence de transparence dans le traitement et l'utilisation des données personnelles ;
2. Limiter le traitement des données personnelles à des finalités légitimes et spécifiées ;
3. Limiter la collecte de données personnelles aux finalités visées ;
4. Permettre aux personnes concernées de corriger ou de demander la suppression de leurs données personnelles ;
5. Limiter le stockage de données personnelles à la durée nécessaire à la finalité visée ;
6. Assurer que les données personnelles sont protégées avec des pratiques de sécurité appropriées.

[18] ISO/IEC CD 20889 INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- PRIVACY ENHANCING DATA DE-IDENTIFICATION TECHNIQUES : https://www.iso.org/standard/69373.html

[19] ARTICLE 5 - PRINCIPES RELATIFS AU TRAITEMENT DES DONNEES PERSONNELLES : https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article5

Que dit le GDPR ?

Article 5 - Principes relatifs au traitement des données personnelles

1. Les données à caractère personnel doivent être :

a) **traitées de manière licite, loyale et transparente** au regard de la personne concernée (licéité, loyauté, transparence);

b) **collectées pour des finalités déterminées, explicites et légitimes**, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités […];

c) **adéquates, pertinentes et limitées à ce qui est nécessaire** au regard des finalités pour lesquelles elles sont traitées (minimisation des données);

d) **exactes et, si nécessaire, tenues à jour**; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);

e) **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[…];

f) **traitées de façon à garantir une sécurité appropriée** des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);

2. Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité).

Cette responsabilité suppose notamment de :

- Mettre en œuvre les mesures organisationnelles et techniques appropriées qui assurent et démontrent que vous êtes conformes au GDPR. Ceci peut comprendre la désignation d'un Délégué à la Protection des Données (DPD), la revue et l'adaptation des politiques de sécurité et de protection des données personnelles, la formation des personnels, des audits internes des traitements, etc. ;
- Maintenir une documentation appropriée sur les traitements de données personnelles ;
- Mettre en œuvre des mesures qui respectent les principes de « protection des données dès la conception » et de « protection des données par défaut ». Ceci inclut la minimisation des données, la pseudonymisation, la transparence, la mise en place et l'amélioration des fonctionnalités de sécurité de façon continue, etc.
- Conduire une analyse d'impact de la protection des données personnelles chaque fois que nécessaire.

Remarque Le responsable du traitement se doit de mettre en œuvre dès la conception d'un traitement les mesures techniques et organisationnelles adaptées pour protéger les données personnelles tout en limitant la collecte aux seules données nécessaires et en utilisant des solutions techniques telles que la minimisation ou la pseudonymisation. L'accès aux données doit être strictement contrôlé. La conformité à des normes internationales pourra servir d'éléments de preuve.

Remarque La future norme ISO/IEC CD 20889 mentionnée précédemment vise à améliorer la pratique et la transparence au sujet de la désidentification des données. Elle permet de classer les techniques de dépersonnalisation connues à l'aide d'une terminologie normalisée : caractéristiques, technologies sous-jacentes, applicabilité de chaque technique à la réduction du risque de réidentification, ou encore utilité des données dépersonnalisées résultants sont autant d'éléments abordés. Son champ d'application s'inscrit donc dans la capacité de fournir des descriptions claires et des conseils sur les objectifs et l'application de la dépersonnalisation pour améliorer la protection de la vie privée.

Transfert de données personnelles vers des pays tiers

Le transfert dans un pays tiers de données personnelles doit garantir que le niveau de protection des personnes physiques exigé par le présent Règlement ne soit pas compromis.

Le transfert est autorisé sans accord spécifique vers les pays tiers pour lesquels la Commission a constaté qu'un niveau de protection adéquat est assuré.

La liste des pays tiers autorisés ou interdits est publiée par la Commission sur son site internet. Néanmoins le transfert sera autorisé s'il est prévu des garanties comme celles prévues dans le cadre des clauses contractuelles types de protection des données approuvées par la Commission.

Certification

La certification vis-à-vis du GDPR est encouragée tout en restant un acte volontaire. Des organismes de certification seront agréés pour pouvoir procéder à l'évaluation conduisant à la délivrance de la certification en question.

> ### Que dit le GDPR ?
>
> **Article 42 - Certification**
> […]
> 3. **La certification est volontaire** et accessible via un processus transparent.
> 4. Une certification […] ne diminue par la responsabilité du responsable du traitement ou du sous-traitant quant au respect du présent règlement […].
> 5. Une certification en vertu du présent article est délivrée par les organismes de certification visés à l'article 43 ou par l'autorité de contrôle compétente sur la base des critères approuvés par cette autorité de contrôle compétente en application de l'article 58, paragraphe 3, ou par le comité en application de l'article 63. Lorsque les critères sont approuvés par le comité, cela peut donner lieu à une certification commune, le **label européen de protection des données**.

La certification est attribuée pour une durée maximale de 3 ans et peut être retirée lorsque les exigences ne sont plus satisfaites. Un label européen de protection des données pourra voir le jour sur accord du Comité Européen de la Protection des Données (CEPD), un nouvel organe européen prévu par l'article 68[20], tout en étant conscient qu'il n'y aura probablement aucune certification GDPR universellement applicable en mai 2018. A titre d'illustration, la norme à venir ISO/IEC AWI 27552[21] INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- ENHANCEMENT TO ISO/IEC 27001 FOR PRIVACY MANAGEMENT -- REQUIREMENTS n'est attendue qu'en 2019/2020.

Dès mai 2018, ce comité sera en charge d'arbitrer les différends entre les autorités et également d'élaborer une doctrine européenne. Avant cette date, le Groupe de l'article 29 se donne pour mission d'accompagner les entreprises pour les aider à se conformer au nouveau Règlement[22]. Il devra ensuite s'effacer dès la mise en application du GDPR.

[20] ARTICLE 68 - COMITE EUROPEEN DE LA PROTECTION DES DONNEES : https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre7#Article68

[21] ISO/IEC AWI 27552 INFORMATION TECHNOLOGY -- SECURITY TECHNIQUES -- ENHANCEMENT TO ISO/IEC 27001 FOR PRIVACY MANAGEMENT -- REQUIREMENTS: https://www.iso.org/standard/71670.html

[22] ADOPTION DU REGLEMENT EUROPEEN PAR LE PARLEMENT EUROPEEN : https://www.cnil.fr/fr/adoption-du-reglement-europeen-par-le-parlement-europeen-un-grand-pas-pour-la-protection-des-donnees

Remarque Le Groupe de l'article 29, se compose d'un représentant de l'autorité ou des autorités de contrôle désignées par chaque État membre, d'un représentant de l'autorité ou des autorités créées pour les institutions et organismes communautaires et d'un représentant de la Commission. Pour la France, c'est à la CNIL qu'a été dévolu ce rôle.

Le G29 constitue le regroupement des « CNIL » européennes chargé de contribuer à l'élaboration des normes européennes en adoptant des recommandations, et de conseiller la Commission Européenne sur tout projet ayant une incidence sur la protection des données et des libertés des personnes[23].

[23] LE G29, GROUPE DES "CNIL" EUROPEENNES : https://www.cnil.fr/fr/le-g29-groupe-des-cnil-europeennes

Initier et conduire un programme GDPR

La conformité avec le GDPR ne constitue pas une activité à réaliser une fois, mais impose au contraire la mise en œuvre d'un processus itératif impliquant une responsabilité permanente. En effet, la conformité avec le GDPR doit pouvoir être prouvée à tout moment : on peut donc parler ici de conformité « dynamique ». Le portefeuille des traitements de données personnelles de l'organisation ou entreprise évolue par essence en continu, transformation digitale oblige.

En ce sens, celle-ci recouvre par exemple la gestion de la qualité, des opérations, de la sécurité, etc.

Ce programme s'adresse dans un premier temps à la mise en conformité de l'ensemble des traitements de données personnelles existants au sein de l'entreprise. Mais il se doit également d'assurer la conformité des nouveaux traitements en vue de respecter les principes de « protection des données dès la conception » et de « protection des données par défaut ».

> ### Que dit le GDPR ?
>
> **Article 25 - Protection des données dès la conception et protection des données par défaut**
>
> 1. […], le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des **mesures techniques et organisationnelles appropriées**, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires […].
>
> 2. Le responsable du traitement **met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées**. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

S'appuyer sur une approche multicycle

Dans ce contexte, l'adoption d'un modèle PDCA (PLAN-DO-CHECK-ADJUST) apparait donc pertinent.

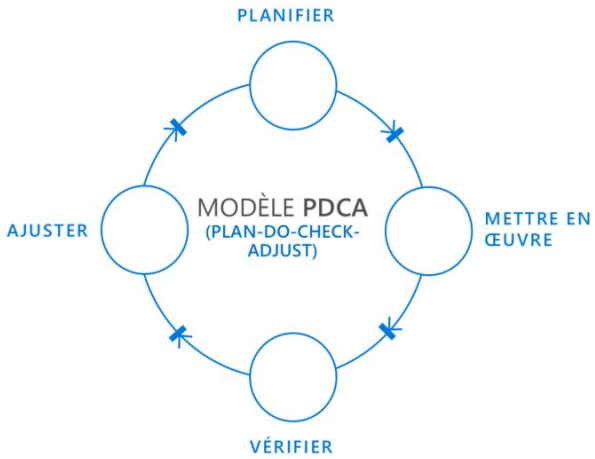


Figure 1 Cycle PDCA (PLANIFIER-METTRE EN ŒUVRE-VERIFIER-AJUSTER)

Egalement appelé « roue de Deming », il s'agit d'un modèle classique des méthodes de gestion et d'amélioration en continu de la qualité, qui a notamment été popularisé par le Microsoft Operations

Framework (MOF) 4.0, l'ITIL (Information Technology Infrastructure Library)[24], ainsi que par la norme ISO/IEC 20000-1:2011[25] INFORMATION TECHNOLOGY -- SERVICE MANAGEMENT -- PART 1: SERVICE MANAGEMENT SYSTEM REQUIREMENTS.

Remarque Microsoft Operations Framework (MOF) 4.0 est un guide concis qui aide les organisations à améliorer la qualité du service tout en permettant de réduire les coûts, de gérer les risques et de renforcer la conformité. MOF définit les principaux processus, les activités et les responsabilités nécessaires pour planifier, fournir, exploiter et gérer les services tout au long de leur cycle de vie. Le guide MOF englobe toutes les activités et les processus impliqués dans la gestion de ces services : leur conception, leur développement, leur exploitation, leur maintenance et, en fin de compte, leur retrait. Pour plus d'informations**,** consultez http://www.microsoft.com/mof.

Remarque Le cycle PDCA se retrouve également au cœur de la norme ISO/IEC 27005:2011[26] TECHNOLOGIES DE L'INFORMATION -- TECHNIQUES DE SECURITE -- GESTION DES RISQUES LIES A LA SECURITE DE L'INFORMATION.

Une approche en cycle permet de commencer l'analyse en se concentrant sur des objectifs réalisables, puis à rapidement itérer sur cette base lorsque le premier résultat s'avère concluant, au lieu de chercher à couvrir un plus grand périmètre et d'attendre des mois ou des années sans voir de réels résultats.

Cela permet de conduire, au-delà d'une mise en œuvre initiale (ou une preuve de concept), correspondante à un cycle PLAN-DO-CHECK-ADJUST, vers une implémentation opérationnelle offrant une couverture complète des systèmes informatiques, une cartographie exhaustive des données personnelles dans ces systèmes informatiques.

Ce modèle permet à la fois de :

1. Couvrir progressivement le périmètre concerné en termes de traitements et de stockage de données personnelles pour en atteindre les 100 % de couverture. Cette progression est dictée par une priorisation des traitements de données personnelles, suite à une évaluation des risques que chaque traitement fait porter sur la protection de la vie privée des personnes concernées.
2. S'inscrire justement dans un processus à conduire de façon continue.

Il offre dans ces deux situations une capacité d'amélioration en continu de la pertinence et de la qualité des mesures organisationnelles et techniques appropriées. Ceci permet d'assurer une mise au point et une prise en compte des retours d'expérience dans la mise en œuvre et l'exécution du programme.

Le modèle PDCA conduit à mener un certain nombre d'activités de façon continue.

On va d'abord procéder à un premier cycle PDCA avant d'itérer en s'appuyant sur les enseignements retenus lors de cette phase.

[24] WHAT IS ITIL BEST PRACTICE?: https://www.axelos.com/best-practice-solutions/itil/what-is-itil

[25] ISO/IEC 20000-1:2011 INFORMATION TECHNOLOGY -- SERVICE MANAGEMENT -- PART 1: SERVICE MANAGEMENT SYSTEM REQUIREMENTS: https://www.iso.org/standard/51986.html

[26] ISO/IEC 27005:2011 TECHNOLOGIES DE L'INFORMATION -- TECHNIQUES DE SECURITE -- GESTION DES RISQUES LIES A LA SECURITE DE L'INFORMATION : https://www.iso.org/fr/standard/56742.html

Comprendre les activités de chaque phase d'un modèle PDCA

Planifier

La première phase consiste à mettre en place la structure qui sera en charge du programme de mise en œuvre de la conformité avec le GDPR et de son maintien dans le temps.

De plus, comme pour chaque programme ou projet à mener, les premières étapes visent également à établir les objectifs, les références et matériaux (cadres et modèles appropriés) et les processus nécessaires à la réalisation des résultats conformément aux résultats attendus.

Ainsi, les processus de gouvernance, les outillages et modèles sont créés pendant cette phase PLANIFIER du cycle PDCA. On définira en précisant à chaque fois les parties prenantes impliquées et si nécessaire les modalités d'exécution et d'interaction : un Registre des traitements (associé à un modèle de fiche descriptive des activités de traitement, un modèle de cycle de vie des données, etc.) ; une classification des données personnelles ; un Framework de décision afin d'effectuer ou non une analyse d'impact relative à la protection des données pour les traitements à risque (DPIA) ; un modèle de processus de notification à l'autorité de contrôle, de gestion des audits de conformité, etc. De même, les outils sur lesquels s'appuient ces processus et ces livrables sont choisis : par exemple, un outil collaboratif et de gestion de contenu afin de tenir le Registre des traitements, un outil graphique préconisé pour la création des diagrammes de flux de données, un outil de gestion de workflow pour automatiser les étapes des différents processus, etc.

De plus, des outils et méthodes adaptés au développement (agile) des nouveaux traitements doivent être intégrés dans les processus de développement pour respecter les principes de « protection des données dès la conception » et de « protection des données par défaut » qui sont définis dans l'article 25 du Règlement.

Au-delà de cette initialisation, cette première phase **PLANIFIER** inclut une série d'activités caractéristiques de l'étape **DECOUVRIR** : Identifier les données personnelles dont vous disposez et où celles-ci résident.

Ceci vise à établir une cartographie exhaustive – au niveau de l'entreprise – des traitements de données personnelles déjà existants ainsi que les données personnelles stockées, avec une compréhension de la gestion du cycle de vie sous-jacent, de la gouvernance des données et de tous les contrôles de sécurité et de confidentialité pertinents mis en place et appliqués.

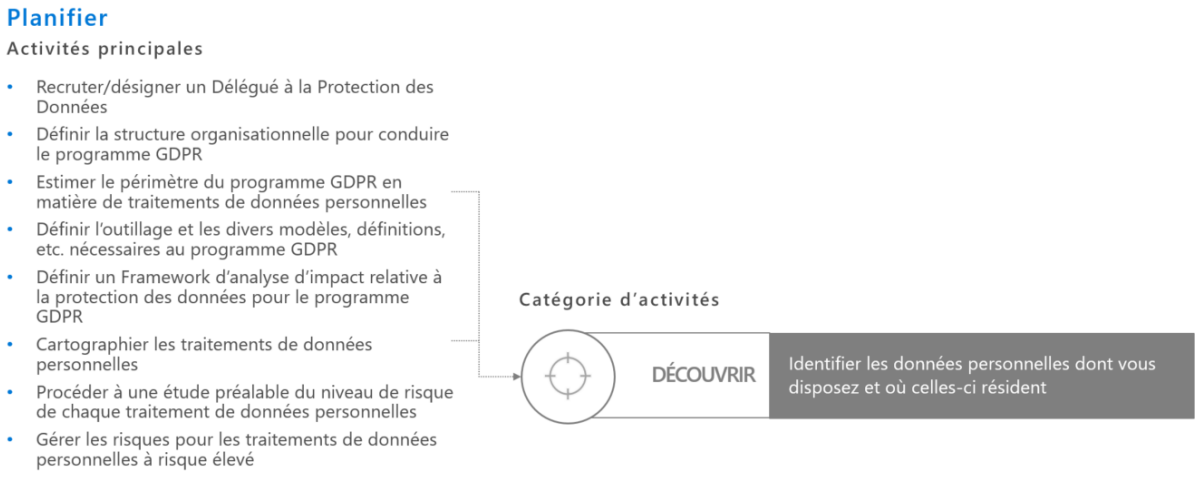


Figure 2 Activités principales de la phase PLANIFIER du cycle PDCA

Cette phase se conclut pour chaque traitement de données personnelles par une étude préalable de façon à statuer si une analyse d'impact relative à la protection des données personnelles (telle que décrit à l'article 35 du Règlement) doit être conduite pour gérer les risques inhérents à ce traitement. Une analyse d'impact sera ou non conduite en fonction des conclusions de cette étude.

Ce jalon formel permet de cibler et de planifier les activités de la phase **METTRE EN ŒUVRE** pour ce traitement.

Mettre en œuvre

Une fois le périmètre du cycle bien établi, les différents cadres et modèles à utiliser déterminés, la taxonomie de classification pour les données personnelles définies, etc., cette deuxième étape **METTRE EN OEUVRE** traite de la mise en œuvre du plan, de l'exécution du processus défini.

Cette deuxième étape **METTRE EN OEUVRE** consiste à mener une série de trois catégories typiques d'activités :

1. **GERER**. Gouverner comment les données personnelles sont accédées et utilisées : gestion du consentement et des droits des personnes concernées, conservation des données personnelles, encadrement du transfert de données, etc. ;
2. **PROTEGER**. Prévenir, détecter et répondre aux vulnérabilités et aux violations de données personnelles : protection des données personnelles, détection des violations et réponse appropriées ;
3. **RAPPORTER**. Maintenir la documentation requise, et gérer les demandes relatives aux données personnelles et les notifications de violation.

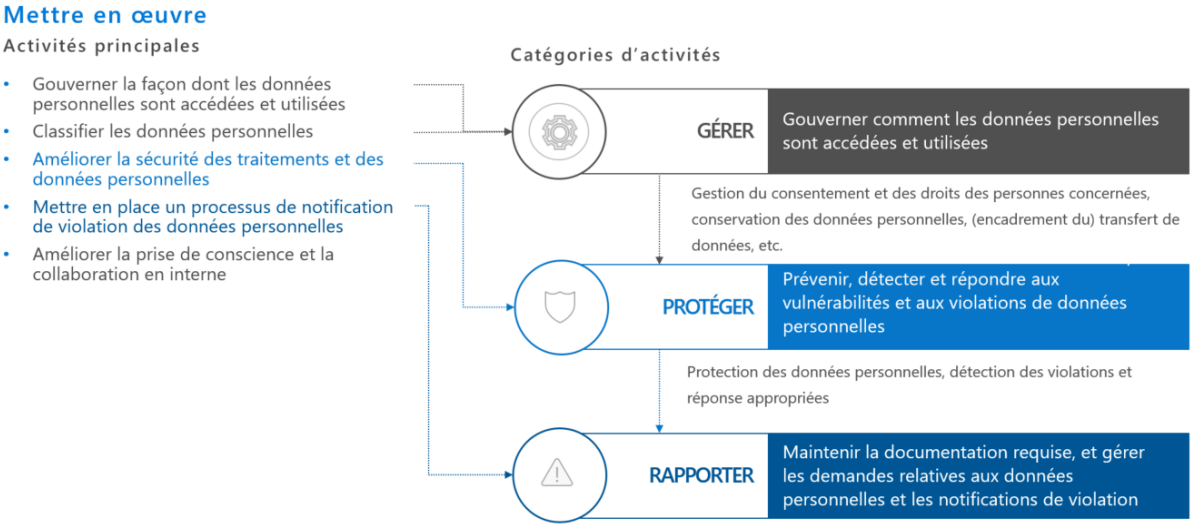


Figure 3 Activités principales de la phase METTRE EN ŒUVRE du cycle PDCA

Vérifier

La troisième étape **VERIFIER** consiste principalement à étudier les résultats réels des activités de l'étape précédente **METTRE EN ŒUVRE**, et à comparer avec les résultats attendus – cibles ou objectifs de l'étape **PLANIFIER** – pour déterminer les différences.

Ceci suppose de réviser, d'évaluer et de valider les différents indicateurs et rapports de données pour s'assurer que :

1. Les outils et les méthodes de gouvernance des données personnelles en place traitent efficacement des exigences en matière de transparence, de tenue de dossiers et de rapports ;
2. Les politiques et profils de protection des données fournissent un contrôle approprié aux personnes concernées et assurent un traitement conforme à la légalité ;
3. Les contrôles de sécurité qui ont été mis en œuvre sont effectivement appliqués pour contrôler l'endroit où les données personnelles sont stockées et comment elles sont utilisées.

Ce qui précède permet de mettre en évidence les points où la conformité avec le GDPR peut être à risque. Ceci implique de mener les catégories d'activités suivantes : **RAPPORTER**.

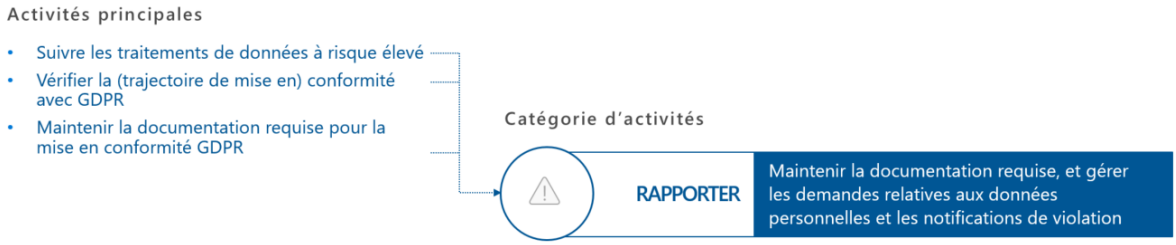


Figure 4 Activités principales de la phase VERIFIER du cycle PDCA

Un accent particulier devra être mis sur la recherche de l'écart dans la mise en œuvre du plan, la pertinence et l'exhaustivité du plan pour en permettre la meilleure exécution.

Ajuster

Cette quatrième et dernière étape **AJUSTER** est l'occasion de :

- Demander / Mettre en œuvre des mesures correctives sur les différences significatives entre les résultats réels et prévus : révision de la méthodologie sous-jacente à adopter, redéfinition, etc. ;
- Analyser les différences dans les éléments de données personnelles qui nécessitent une révision en termes de classification, de politiques de protection / de divergences de profils, etc. pour déterminer leurs causes profondes ;
- Déterminez où appliquer les modifications qui incluront les améliorations de l'ensemble du processus.

Cette étape permet de rationaliser l'effort de mise en conformité au GDPR et de créer une approche par étapes qui :

- Inclut une articulation claire des efforts et l'application d'une gouvernance IT sur les traitements de données personnelles considérés, l'engagement des métiers pour prioriser les risques sur les données personnelles manipulées et/ou stockées ainsi que sur les processus opérationnels relatifs à ces traitements.
- Permet d'étendre la couverture dans le temps en termes de traitements de données personnelles gérés et contrôlés par le programme GDPR, et d'adresser les nouveaux risques sur les nouveaux actifs de données personnelles qui apparaitraient ;
- Permet des améliorations continues en mettant en œuvre des garanties et des capacités supplémentaires envers ces mêmes traitements de données personnelles.

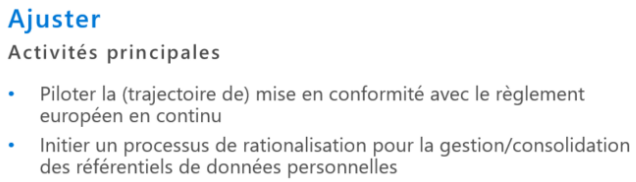


Figure 5 Activités principales de la phase AJUSTER du cycle PDCA

Vous avez dit agile ?

Comme nous venons de le voir, le modèle PDCA conduit à mener un certain nombre d'activités de façon continue.

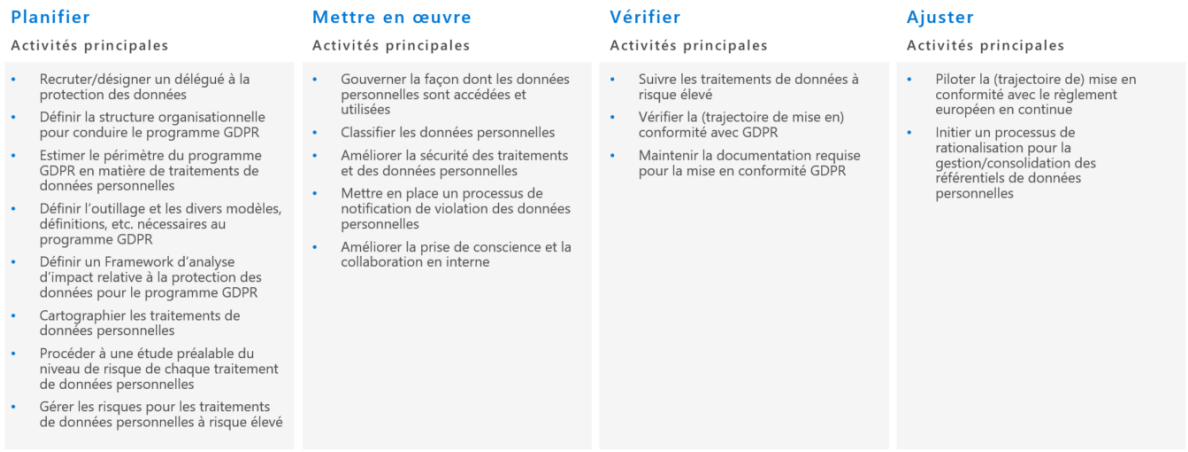


Figure 6 Activités principales à conduire lors d'un cycle PDCA

L'adoption d'un tel modèle PDCA n'empêche aucunement une démarche agile. Il s'agit pour la définition d'un « Sprint » de « puiser » dans les différents « seaux » d'activités **PLANIFIER**-**METTRE EN ŒUVRE**-**VERIFIER**-**AJUSTER**. A l'instar de la méthodologie Microsoft SDL (Security Development Lifecycle)[27] vs. « SDL for Agile[28] [29] (SDL-Agile) » dans un domaine orthogonal, méthodologie sur laquelle nous reviendrons dans la suite de ce livre blanc.

[27] MICROSOFT SDL (SECURITY DEVELOPMENT LIFECYCLE) : http://www.microsoft.com/sdl

[28] SDL FOR AGILE : https://www.microsoft.com/en-us/SDL/Discover/sdlagile.aspx

[29] SECURITY DEVELOPMENT LIFECYCLE FOR AGILE DEVELOPMENT : https://msdn.microsoft.com/en-us/library/windows/desktop/ee790621.aspx

Remarque La méthodologie Microsoft SDL (cycle de développement sécurisé) est un processus d'assurance de sécurité des logiciels, et de ses évolutions « Agile » et « Cloud » qui sont particulièrement adaptées au contexte d'évolution en continu de tels services. Ces bonnes pratiques permettent d'assurer le principe de « Sécurité dès la conception » mais également ceux de « Sécurité par défaut », « Sécurité lors du déploiement » et de communications pour l'ensemble de ces principes structurants. On parle ainsi de SD3+C pour l'ensemble de ces principes structurants.

Ces principes s'appliquent également à la protection de la vie privée (privacy), en intégrant la « Protection de la vie privée dès la conception » et la « Protection de la vie privée par défaut » en accord avec les politiques de protection de la vie privée de Microsoft[30], et l'on parle par extension de PD3+C.

Remarque L'annexe A de la norme ISO/IEC 27034-1:2011[31] comprend un cas d'étude qui illustre comment SDL se conforme aux processus et aux composants de cette norme qui fournit un modèle fondé sur les risques pour intégrer la sécurité dans le cycle de vie des logiciels. Microsoft SDL atteint ou dépasse les directives publiées dans ISO/IEC 27034-1.

Le billet de blog MICROSOFT SDL CONFORMS TO ISO/IEC 27034-1:2011[32] peut être consulté à cet effet. Avec le développement Agile que régit désormais tout et l'approche de génie logiciel d'intégration continue (Continuous Integration en anglais ou CI) / et de livraison continue (Continuous Integration en anglais ou CD) qui gouverne la mise à disposition des solutions, les équipes d'ingénierie mettent à profit la méthodologie SDL pour le développement Agile (SDL-Agile) afin d'intégrer les pratiques de sécurité critiques dans les méthodologies agiles utilisées au quotidien. Comme son nom l'indique, l'approche SDL-Agile est fidèle à la fois à SDL et à Agile. Les équipes peuvent ainsi innover et réagir rapidement aux besoins client tout en mettant à disposition des solutions qui sont (encore) plus résistantes aux attaques.

Nous détaillons chacune de ces activités dans la suite de ce document.

[30] WE SET AND ADHERE TO STRINGENT PRIVACY STANDARDS : https://www.microsoft.com/en-us/trustcenter/privacy/we-set-and-adhere-to-stringent-standards

[31] ISO/IEC 27034-1:2011 TECHNOLOGIES DE L'INFORMATION -- TECHNIQUES DE SECURITE -- SECURITE DES APPLICATIONS -- PARTIE 1: APERÇU GENERAL ET CONCEPTS : https://www.iso.org/fr/standard/44378.html

[32] MICROSOFT SDL CONFORMS TO ISO/IEC 27034-1:2011: https://blogs.microsoft.com/microsoftsecure/2013/05/14/microsoft-sdl-conforms-to-isoiec-27034-12011/

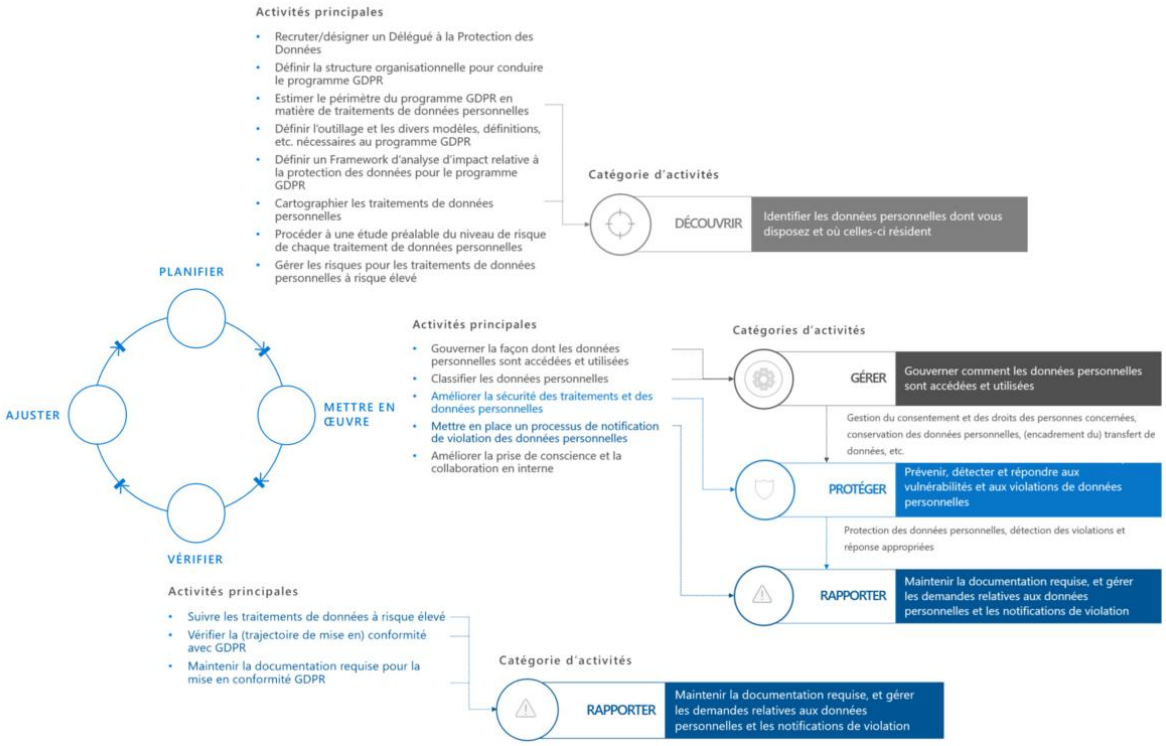


Figure 7 Vue consolidées des activités principales à conduire lors d'un cycle PDCA et regroupement par grandes catégories

Planifier le programme GDPR

La phase **PLANIFIER** du cycle PDCA est constituée d'un ensemble d'activités :

- Gouverner la façon dont les données personnelles sont accédées et utilisées (DPD) ;
- Définir la structure organisationnelle pour conduire le programme GDPR ;
- Estimer le périmètre du programme GDPR en matière de traitements de données personnelles ;
- Définir l'outillage et les divers modèles, définitions, etc. ;
- Définir un Framework d'analyse d'impact relative à la protection des données ;

La démarche classique d'une analyse de risques couvre différentes étapes ; après avoir défini le périmètre, on identifie les actifs et les menaces. Ensuite on évalue les mesures de sécurité existantes, les vulnérabilités pour finir par évaluer les risques, la probabilité d'occurrence, les impacts. Enfin, on envisage les contre-mesures que l'on mettra en œuvre pour couvrir les risques, en acceptant les risques résiduels.

- Cartographier les traitements de données personnelles ;
- Procéder à une étude préalable du niveau de risque des traitements de données personnelles ;
- Gérer les risques pour les traitements de données personnelles à risque élevé.

Ces activités sont décrites de façon unitaire dans les sections suivantes.

Recruter/désigner un Délégué à la Protection des Données

Cette activité est à mener lors de l'itération initiale du cycle PDCA.

La désignation d'un « Délégué à la Protection des Données » ou DPD (en anglais « Data Protection Officer » ou DPO) est obligatoire en 2018 dans certaines situations.

Que dit le GDPR ?

Article 37 - Désignation du délégué à la protection des données

Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque :

a) le traitement est **effectué par une autorité publique** ou un organisme public […]

b) les activités […] consistent en des **opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle** des personnes concernées; ou

c) les activités […] consistent en un **traitement à grande échelle de catégories particulières de données** […] et de données personnelles relatives à des condamnations pénales et à des infractions […].

Article 38 - Fonction du délégué à la protection des données

Article 39 - Missions du délégué à la protection des données

Les missions du délégué à la protection des données sont au moins les suivantes:

a) **informer et conseiller** […] **sur les obligations** […] en matière de protection des données;

b) **contrôler le respect du présent règlement** […], y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant;

c) **dispenser des conseils**, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données […];

d) **coopérer avec l'autorité de contrôle** […];

e) **faire office de point de contact** pour l'autorité de contrôle […].

Dans tous les cas, la désignation a minima d'une personne chargée de s'assurer de la mise en conformité au Règlement européen est fortement recommandée.

Le rôle de Délégué à la Protection des Données tel que défini dans le Règlement est central : « le but de ce rôle est de combler le fossé entre la technologie et les services juridiques ainsi que les Ressources Humaines et les Relations Publiques »[33].

Il tient ce rôle de « courroie de transmission » en relation, d'une part avec les équipes métier en charge des traitements de données personnelles, et d'autre part avec le Directeur des Systèmes d'Information (DSI), le Responsable de la Sécurité des Systèmes d'Information (RSSI), la Direction Juridique et le Directeur des Données, si ce dernier rôle existe dans l'organisation ou l'entreprise. Le Délégué à la Protection des Données doit bénéficier d'une véritable indépendance et sera le point de contact avec l'autorité de contrôle.

Autrement dit, il tient le rôle de chef d'orchestre pour assurer la conformité avec le GDPR. Référent du programme, il assure ainsi un rôle de conseil, coordonne les différentes actions à mener et assure le contrôle du bon déroulé du programme.

> **Remarque** Conscient du fait que le Règlement possède de nombreuses zones de flou, propres à interprétation, le G29 s'est engagé à travailler sur des guides dits « lignes directrices »[34] clarifiant et illustrant par des exemples concrets la mise en œuvre et le déploiement opérationnel du GDPR. Au sein du corpus de lignes directrices d'ores et déjà disponibles – un certain nombre de lignes directrices sont encore en cours de définition à la date de publication de ce livre blanc – les lignes directrices DELEGUE A LA PROTECTION DES DONNEES (EN) permettent d'éclairer les zones d'ombre relatives à la désignation, les rôles et responsabilités du Délégué à la Protection des Données et aux compétences requises notamment quant à la définition d'une fiche de description de rôle métier.
>
> Publié initialement en décembre 2016, une révision de ce guide[35] a été mise à disposition début avril 2017 apportant des précisions intéressantes : il ne peut y avoir qu'un seul Délégué à la Protection des Données pour toute l'organisation ; il sera responsable de l'ensemble des traitements de données personnelles – on ne peut pas « saucissonner » les traitements entre plusieurs Délégués à la Protection des Données – mais qu'il pourra se faire aider par une équipe sous sa responsabilité ; il doit résider si possible dans l'Union Européenne et identifier des cas de conflit d'intérêt.

Le Délégué à la Protection des Données représente une certaine évolution du rôle de Correspondant Informatique et Libertés (CIL) en France ou du DSB (Datenschutzbeauftragter) en Allemagne.

Les livrables pour la mise en œuvre de cette activité sont les suivants :

- Fiche de description du rôle métier associé.
- Allocation de l'enveloppe financière nécessaire.

Définir la structure organisationnelle pour conduire le programme GDPR

Cette activité est à mener lors de l'itération initiale du cycle PDCA.

---

[33] IS IT TIME FOR DATA PROTECTION OFFICERS? : http://www.techradar.com/news/world-of-tech/management/is-it-time-for-data-protection-officers-1322335

[34] LIGNES DIRECTRICES : https://www.cnil.fr/fr/reglement-europeen/lignes-directrices

[35] GUIDELINES ON DATA PROTECTION OFFICERS ('DPOS'): https://www.cnil.fr/sites/default/files/atoms/files/guidelines_on_dpos_5_april_2017.pdf

La mise en place de la conformité avec le GDPR nécessite une véritable prise de conscience au plus haut niveau de l'organisation pour, non seulement débloquer les budgets nécessaires, mais être capable d'impliquer les bonnes parties prenantes et d'associer les dirigeants eux-mêmes dans la démarche. Compte tenu du montant possible des sanctions financières, le GDPR constitue de fait un sujet de Comité de Direction pour l'organisation.

Dans la pratique, cette activité vise à construire l'« équipe » au-delà du Délégué à la Protection des Données. Il s'agit pour cela de porter une attention particulière pour intégrer les différentes parties prenantes nécessaires à la gouvernance du programme GDPR et de s'assurer de la prise en compte de tous les relais internes nécessaires au sein de l'entreprise.

Il convient également de préciser le modèle de gouvernance du programme GDPR, c'est-à-dire les modalités d'interaction en fonction des différents rôles dévolus, par exemple le Délégué à la Protection des Données vis-à-vis du RSSI. L'autorité de contrôle avec laquelle l'entreprise est susceptible d'interagir dans le futur doit être clairement identifiée, par exemple la CNIL pour la France.

La définition d'un comité de pilotage du programme GDPR doit également être établi. Ce comité de pilotage dans le cadre du déroulé du programme :

- Assure le pilotage des activités et actions associées réalisées ;
- Prend les décisions et arbitrages nécessaires pour lesquels il a reçu délégation du Comité de Direction ;
- Liste, précise et synthétise les éléments d'aide de décision requis pour le comité de direction, etc.

Il est enfin nécessaire à ce stade d'évaluer le budget nécessaire à la conduite du programme GDPR.

Les livrables pour la mise en œuvre de cette activité sont les suivants :

- Document de gouvernance du programme GDPR. Ce document comprend la description des parties prenantes, de leurs interactions et de leur rôle dans chacun des processus (par exemple Délégué à la Protection des Données, responsable de traitement ou d'application, RSSI, DSI, ...) ;
- Allocation de l'enveloppe financière nécessaire.

Estimer le périmètre du programme GDPR en matière de traitements de données personnelles

Cette activité est à mener lors de l'itération initiale du cycle PDCA.

Toutes les entreprises ne sont pas concernées de la même façon par le GDPR. La réalisation d'un premier recensement des traitements de données personnelles en place s'impose à ce stade, avec la nécessité de pouvoir échanger avec l'ensemble des métiers, branches, divisions, départements, entités, etc. de l'entreprise pour dresser une première liste de leurs traitements de données personnelles en place.

Les traitements de données (services, applications et dépôts associés) dont on peut déterminer rapidement qu'ils ne traitent pas de données personnelles seront écartés. A contrario, ceux qui intègrent des données personnelles doivent entrer dans la liste des traitements cibles à traiter dans les activités suivantes. Dans la pratique, et de manière à pouvoir conduire les activités suivantes dans l'étape de planification, les informations remontées doivent permettre une analyse rapide et une priorisation de l'effort.

Pour cela doivent être en particulier précisés dans la mesure du possible :

- La ou les finalités du traitement réalisé (c'est-à-dire les objectifs), l'importance et la pertinence vis-à-vis du Métier ainsi que les éventuels transferts vers des tiers ;

- La nature des données personnelles stockées ou manipulées ;
- Les services, les applications et les dépôts de données connus pour héberger ou susceptibles d'héberger et/ou de traiter des données personnelles ;
- L'exposition au sens sécurité du traitement et de ses ramifications, etc.

Il s'agit d'un premier pas dans la documentation des traitements. Cette documentation est véritablement constituée et consolidée dans l'activité de cartographie, Cf. section § CARTOGRAPHIER LES TRAITEMENTS DE DONNEES PERSONNELLES.

Ces traitements constituent le portefeuille des traitements en termes de périmètre pour assurer la mise en conformité au GDPR.

Les services, applications et dépôts de données remontés sont naturellement à croiser avec les actifs connus et gérés de l'IT. La notion de « Shadow IT » est en effet présente dans de très nombreuses entreprises : selon une étude de Help Net Security de 2014, 10 fois plus d'applications dans le Cloud sont utilisées par rapport aux estimations réalisées par l'IT.

> **Remarque** L'organisation doit maîtriser l'ensemble des actifs concernés par le GDPR y compris la dimension « Shadow IT » et les applications « non-identifiées » dans ce contexte.
>
> Il n'y a en effet simplement aucun moyen possible d'obtenir la visibilité sur ces applications (et donc les traitements) pour lesquelles l'organisation ne dispose d'aucune capacité à s'assurer que les contrôles nécessaires sont en place. Comme le souligne l'article WHY YOU NEED A CASB FOR GDPR COMPLIANCE[36], des solutions de type CASB (Cloud Access Security Broker) permettent de faire sortir de l'ombre ces applications.
>
> De telles solutions permettent également généralement d'identifier des données personnelles en transit et au repos pour une large palette d'applications dans le Cloud. Cela comprend également les solutions de stockage dans le Cloud comme (OneDrive, Google Drive, Dropbox, etc.).
>
> Il est alors possible d'envisager i) de contrôler avec les mesures qui s'imposent les flux de données personnelles et les éventuels transferts de données que cela implique et ii) d'évaluer les risques qui pèsent en fonction des sous-traitants désormais identifiés.

Tous les éléments précédents ainsi collectés doivent permettre d'évaluer si le GDPR s'applique à l'entreprise et, dans l'affirmative, dans quelle mesure. Une analyse rapide pour mesurer le niveau de criticité pour l'organisation doit être conduite et, à l'issue de celle-ci, on pourra réaliser si l'on est ou non impacté par le GDPR et à quel degré.

Comme évoqué précédemment, la portée et l'ampleur d'un programme GDPR diffèreront d'une organisation à une autre.

> **Remarque** L'outil « GDPR Assessment »[37] permet d'effectuer une autoévaluation de votre organisation sur le niveau global de maturité au regard des principales exigences du GDPR. Cet outil sous forme de questionnaire est gratuit, disponible en ligne et fournit un benchmark selon les catégories d'activités principales abordées précédemment, c.à.d. DECOUVRIR, GERER, PROTEGER, RAPPORTER et précise, le cas échéant, les solutions Microsoft susceptibles d'aider à répondre à ces exigences.

Cette première évaluation du niveau de risque vise à considérer les traitements les plus à risque en priorité dans les cycles PDCA du programme GDPR. Compte tenu du délai très court du 25 mai 2018 pour la mise en œuvre de la conformité avec le GDPR, il est préconisé de séquencer la prise en compte des traitements de données personnelles en traitant en priorité ceux que l'on a considérés comme étant les plus critiques même si, à terme, tous les traitements devront respecter le Règlement.

---

[36] WHY YOU NEED A CASB FOR GDPR COMPLIANCE: https://blog.cloudsecurityalliance.org/2017/04/04/need-casb-gdpr-compliance/

[37] GDPR Assessment : https://www.gdprbenchmark.com/

Force est de constater que dresser ce premier état des lieux de la façon la plus exhaustive possible – le GDPR exigeant à terme une couverture à 100% des traitements de données personnelles – peut s'avérer une activité coûteuse en temps.

> **Remarque** Selon l'étude ORGANISATIONAL READINESS FOR THE EUROPEAN UNION GENERAL DATA PROTECTION REGULATION mentionnée en introduction de ce livre blanc, l'inventaire des traitements (et leur cartographie) constitue sans surprise l'effort majeur à produire pour la plus grande partie des entreprises. Si 27% prétendent disposer d'un inventaire à jour incluant les données personnelles, 25% affirment posséder un inventaire à jour mais sans l'ensemble des données et le reste – c'est-à-dire presque la moitié – indiquent un inventaire minimal voire inexistant.

Certaines organisations peuvent avoir plusieurs milliers de traitements réalisés au travers de services et d'applications les plus divers et il convient d'identifier pour chacun d'eux si des données personnelles sont en jeu ou non. De plus, certains traitements réalisés via d'anciennes applications (legacy) toujours utilisées, souvent développées en externe, pourront ne plus avoir de propriétaire désigné : il est fort probable que l'organisation en ait perdu la maitrise, ce qui rendra d'autant plus difficile cette première analyse et la cartographie plus complète qui devra s'ensuivre (Cf. section § CARTOGRAPHIER LES TRAITEMENTS DE DONNEES PERSONNELLES).

Les livrables pour la mise en œuvre de cette activité sont les suivants :

- Première liste consolidée et priorisée (criticité) des traitements concernés, si possible par finalité principale. Chaque traitement doit être assorti des types de données personnelles traitées ainsi que des services, applications (internes vs. dans le Cloud vs. en mode hybride) et dépôts de données concernés ;
- Estimation de l'impact du GDPR et de l'effort à fournir pour atteindre la mise en conformité au GDPR.

Définir l'outillage et les divers modèles, définitions, etc.

Cette activité est à mener lors de l'itération initiale du cycle PDCA.

Cette activité comporte un ensemble de sous-activités :

- Définir une/revoir la taxonomie de classification pour les données personnelles ;
- Définir les politiques pour la gestion et l'utilisation des données personnelles ;
- Définir un Registre des traitements ;
- Définir/revoir/mettre à jour les différents modèles vis-à-vis du consentement et des nouveaux droits des personnes concernées ;
-
- Définir un modèle de processus de notification de violation de données personnelles.

Celles-ci sont décrites dans les sections suivantes.

Définir une/revoir la taxonomie de classification pour les données personnelles

Le GDPR exige des organisations de sécuriser les données personnelles en accord avec leur sensibilité. Comme abordé à la section § VOUS AVEZ DIT DONNEES PERSONNELLES ?, les données personnelles sont de différents types : données concernant les mineurs, données de santé, données biométriques, etc.

Ces mêmes données revêtent des sensibilités particulières comme le décrit l'article 9[38].

> Que dit le GDPR ?
>
> **Article 9 - Traitement portant sur des catégories particulières de données à caractère personnel**
> 1. Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits.
> 2. Le paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie :
> [Cf. (10) conditions énoncées…]

Remarque La conduite de cette activité peut s'inspirer des considérations décrites dans les livres blancs PROTECT AND CONTROL YOUR KEY INFORMATION ASSETS THROUGH INFORMATION CLASSIFICATION - CLASSIFY, LABEL, PROTECT, AND AUDIT (CLPA) YOUR KEY INFORMATION ASSETS[39] et DATA CLASSIFICATION FOR CLOUD READINESS[40].

Remarque Nous conseillons également de considérer pour la définition d'une taxonomie appropriée l'annexe B.1 de la future norme ISO/IEC FDIS 19944[41] INFORMATION TECHNOLOGY -- CLOUD COMPUTING -- CLOUD SERVICES AND DEVICES: DATA FLOW, DATA CATEGORIES AND DATA USE.

Le livrable en sortie de cette activité est un document de classification des données personnelles au regard du GDPR. Dans une approche plus holistique des choses, cela consiste à rédiger ou mettre à jour un document de classification pour l'ensemble des actifs de l'entreprise.

Définir les politiques pour la gestion et l'utilisation des données personnelles

Comme son titre le suggère, cette activité consiste à établir les bases d'un plan de gouvernance des données. Il s'agit de développer (les bases) des standards de sécurité qui décrivent au sein de l'entreprise la gestion, l'accès, le transfert et la suppression des données personnelles.

Cela couvre les données personnelles dans les trois états suivants :

- **Au repos**. Les données enregistrées sur tout support de stockage, y compris les données d'archivage et de rétention ;
- **En traitement**. Toutes les données qui ne sont pas dans un état de repos, c'est-à-dire sur un seul nœud particulier dans un réseau, par exemple, en mémoire, dans le cache du processeur ou cache du disque, etc. ;
- **En transit**. Toutes les données transférées entre au moins deux nœuds.

Ainsi que les opérations suivantes : Stocker vs. Recouvrer vs. Conserver vs. Archiver vs. Retirer.

---

[38] ARTICLE 9 - TRAITEMENT PORTANT SUR DES CATEGORIES PARTICULIERES DE DONNEES A CARACTERE PERSONNEL : https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article9

[39] PROTECT AND CONTROL YOUR KEY INFORMATION ASSETS THROUGH INFORMATION CLASSIFICATION - CLASSIFY, LABEL, PROTECT, AND AUDIT (CLPA) YOUR KEY INFORMATION ASSETS : https://aka.ms/classify

[40] DATA CLASSIFICATION FOR CLOUD READINESS : https:// aka.ms/data-classification-cloud

[41] ISO/IEC FDIS 19944 INFORMATION TECHNOLOGY -- CLOUD COMPUTING -- CLOUD SERVICES AND DEVICES: DATA FLOW, DATA CATEGORIES AND DATA USE : https://www.iso.org/standard/66674.html

Il convient de développer également des standards de sécurité qui régissent la conservation des données typiquement fonction de leurs types et sensibilités.

Les livrables en sortie de cette activité sont les suivants :

- Plan de gouvernance des données personnelles ;
- Politique de sécurité de l'information (ou révision) ;
- Politique de protection des données personnelles (et le cas échéant profils associés).

Définir un Registre des traitements

Le GDPR exige de recenser et de cartographier précisément les traitements de données personnelles :

Qui est responsable ? Quelles données (catégorie/sensibilité) ? Pour quelles finalités ? Où (services, applications, dépôts de données, stockage vs. Transfert) ? Jusqu'à quand (conservation) ? Comment (mesure de sécurité) ?

Toutes ces informations nécessitent la tenue d'un Registre des traitements pour les activités associées. Le Registre doit être maintenu à jour avec le déroulé du programme GDPR et fourni sur demande à l'autorité de contrôle (la CNIL pour la France). Il sert en effet de référence en cas d'audit.

Que dit le GDPR ?

Article 30 - Registre des activités de traitement

Chaque responsable du traitement et, le cas échéant, le représentant du responsable du traitement tiennent un registre des activités de traitement effectuées sous leur responsabilité. Ce registre comporte toutes les informations suivantes:

a) **le nom et les coordonnées du responsable du traitement** et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données;
b) **les finalités du traitement**;
c) **une description des catégories de personnes concernées et des catégories de données personnelles**;
d) **les catégories de destinataires** auxquels les données personnelles ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales;
e) le cas échéant, **les transferts de données personnelles** vers un pays tiers ou à une organisation internationale […];
f) dans la mesure du possible, **les délais prévus pour l'effacement** des différentes catégories de données;
g) dans la mesure du possible, **une description générale des mesures de sécurité techniques et organisationnelles** […].

Cela suppose de définir, pour le Registre, un outillage adapté à l'entreprise et ses pratiques, qui peut aller d'un simple fichier Excel, comme le modèle de registre Règlement Européen[42] proposé par la CNIL à un outil collaboratif comme par exemple une bibliothèque SharePoint.

[42] Modèle de registre Règlement Européen : https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-publie.xlsx

Remarque Un projet « GDPR Activity Hub »[43] est mis à disposition en Open source par Microsoft sur la forge communautaire GitHub afin d'aider les organisations à avancer dans leur cheminement vers la conformité avec le GDPR. L'objectif de ce projet est de donner aux organisations une base leur permettant de conserver une trace de l'ensemble des activités principales, des tâches associées, des événements essentiels, des demandes reçues, etc. pour le respect des exigences GDPR. Fondé sur les technologies SharePoint, ce projet peut constituer une fondation pour le Registre.

Cet outillage pourra également passer par l'instanciation d'un catalogue de données, par exemple avec Azure Data Catalog[44], afin d'obtenir davantage de valeur et rationaliser les actifs de données de l'entreprise dans ce chemin vers la conformité avec le GDPR.

Au-delà de l'outillage, il convient de :

- Définir un modèle de fiche de traitement des données personnelles ;
- Définir un modèle complémentaire de cycle de vie des données personnelles ;
- Définir les modalités d'utilisation du Registre.

Ces sous-activités sont précisées dans les sections suivantes.

Définir un modèle de fiche de traitement des données personnelles

Au-delà de ces modalités de mise en œuvre d'un Registre des traitements, il est nécessaire de définir également un modèle de fiche de traitement pour sa description conformément à l'article 30[45]. Ce modèle est destiné aux entrées du Registre. Les fiches de traitements sont complétées lors de la cartographie des traitements de données personnelles (Cf. section § CARTOGRAPHIER LES TRAITEMENTS DE DONNEES PERSONNELLES) et utilisées lors de l'étude préalable pour identifier et prioriser les actions à mener pour se conformer au GDPR (Cf. section § PROCEDER A UNE ETUDE PREALABLE DU NIVEAU DE RISQUE DES TRAITEMENTS DE DONNEES PERSONNELLES).

Définir un modèle complémentaire de cycle de vie des données personnelles

Par ailleurs, il convient également de définir, en tant qu'annexe de la fiche descriptive précédente, un modèle complémentaire de description du cycle de vie des données personnelles. Ce modèle sera fonction de la nature et des possibilités du Registre.

La description du cycle de vie des données personnelles s'avère notamment nécessaire pour la planification et la mise en œuvre de la capacité d'exercice des droits de la personne concernée sur ses données – le droit d'accès, de rectification, de suppression, etc.

Ce modèle complémentaire de cycle de vie des données personnelles est destiné à décrire les étapes du traitement, les services, applications et dépôts de données, à visualiser les flux de données du traitement associé ainsi que les éventuels transferts.

---

[43] GDPR Activity Hub : https://github.com/SharePoint/sp-dev-gdpr-activity-hub

[44] Azure Data Catalog : https://azure.microsoft.com/fr-fr/services/data-catalog/

[45] ARTICLE 30 - REGISTRE DES ACTIVITES DE TRAITEMENT : https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article30

Remarque La plupart des approches de modélisation sont orientées processus métier ou assez généralistes comme UML[46] (Unified Modeling Language). D'autres, plus axés sur les SI, comme OBASHI[47], permettent de décrire une architecture d'applicative de la couche matérielle jusqu'à la couche application mais restent peu adaptées - la description est trop précise et nécessite un effort conséquent - sans finalement se concentrer sur l'essentiel c'est-à-dire le cycle de vie et les flux dans le cadre du traitement des données personnelles considérés.

La future norme ISO/IEC FDIS 19944[48] CLOUD SERVICES AND DEVICES: DATA FLOW, DATA CATEGORIES AND DATA USE constitue un cadre de référence des plus intéressants en matière de taxonomie des données.

Définir les modalités d'utilisation du Registre

Enfin, doit également être abordée dans cette activité la définition des modalités d'utilisation du Registre dans le temps, et en particulier les processus d'insertion, de mise à jour, de suppression d'un traitement de données personnelles.

Les livrables en sortie de cette activité complète sont les suivants :

- Mise en place du Registre des traitements au travers de l'outillage retenu ;
- Modèle de fiche de traitement, accompagné d'un modèle complémentaire de cycle de vie des données personnelles du traitement et de la description des flux associés.

Définir/revoir/mettre à jour les différents modèles vis-à-vis du consentement et des nouveaux droits des personnes concernées

Les données personnelles doivent être traitées de manière transparente dans le sens où la personne concernée doit être informée de la finalité du traitement – d'autres utilisations que pour le seul traitement décrit ne sont pas permises – et que seules les données nécessaires à cette finalité seront collectées. Le consentement de la personne doit être demandé de manière claire, explicite et être obtenu avant la collecte de la donnée, ce consentement pouvant être ensuite retiré à tout moment. Des conditions particulières s'appliquent par ailleurs pour les mineurs de moins de 16 ans qui nécessitent alors l'accord d'une autorité parentale.

De plus, les droits de la personne concernée sont étendus en commençant par le consentement que la personne doit accorder en toute connaissance de cause : la transparence est imposée sur la finalité du traitement, les données personnelles collectées, les éventuels transferts des données à des tiers et/ou en dehors de l'Union Européenne, la durée de conservation des données personnelles, le droit d'introduire une réclamation. La personne dispose ensuite d'une capacité d'exercice de droits d'accès, de rectification, de limitation du traitement, d'effacement, et de portabilité. En outre, la notion de profilage est introduite pour indiquer que la personne concernée doit en être informée et peut le refuser excepté lorsque ce dernier est nécessaire à l'exécution du contrat.

[46] UML : https://fr.wikipedia.org/wiki/UML_(informatique)

[47] OBASHI : https://en.wikipedia.org/wiki/OBASHI

[48] ISO/IEC FDIS 19944 CLOUD SERVICES AND DEVICES: DATA FLOW, DATA CATEGORIES AND DATA USE : https://www.iso.org/standard/66674.html

Que dit le GDPR ?

Section 1 - Transparence et modalités
Article 8 - Conditions applicables au **consentement des enfants** en ce qui concerne les services de la société de l'information
Article 12 - Transparence des informations et des communications et **modalités de l'exercice des droits** de la personne concernée

Section 2 - Information et accès aux données à caractère personnel
Article 13 - **Informations à fournir** lorsque des données à caractère personnel sont collectées auprès de la personne concernée
Article 14 - Informations à fournir lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée
Article 15 - **Droit d'accès** de la personne concernée

Section 3 - Rectification et effacement
Article 16 - **Droit de rectification**
Article 17 - **Droit à l'effacement** («droit à l'oubli»)
Article 18 - **Droit à la limitation du traitement**
Article 19 - Obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement
Article 20 - **Droit à la portabilité** des données

Section 4 - Droit d'opposition et prise de décision individuelle automatisée
Article 21 - **Droit d'opposition**
Article 22 - Décision individuelle automatisée, y compris le profilage

Cette activité concerne aussi bien les nouveaux traitements de données personnelles envisagés que la mise en conformité des traitements déjà en place et s'intéresse à la définition des processus et procédures « canevas » en termes de modalités d'exercices des droits des personnes concernées, qu'il s'agisse :

- Du retrait du consentement, du droit d'accès, du droit de rectification, du droit à l'effacement (droit à l'oubli), du droit à la portabilité, etc.

-ou-

- De la prise en compte des cas particuliers, par exemple avec l'article 8[49] pour le consentement des mineurs mentionné ci-dessus.

Il s'agit de définir également les formulaires « type » associés ainsi que les diverses mentions d'information associées.

Remarque Conscient du fait que le Règlement possède des zones de flou, propres à interprétation, le G29 s'est engagé à travailler sur des guides dits « lignes directrices » clarifiant et illustrant par des exemples concrets la mise en œuvre et le déploiement opérationnel du GDPR. Au sein du corpus de lignes directrices d'ores et déjà disponibles – un certain nombre de lignes directrices sont encore en cours de définition à la date de publication de ce livre blanc – les lignes directrices PORTABILITE (EN)[50] permettent d'éclairer les attendus relatifs au droit à la portabilité, un nouveau droit décrit à l'article 20 qui impose de pouvoir transmettre les données d'un système de traitement à un autre.

Les livrables en sortie de cette activité sont les suivants :

- Processus/procédures « canevas » ;

[49] ARTICLE 8 - CONDITIONS APPLICABLES AU CONSENTEMENT DES ENFANTS EN CE QUI CONCERNE LES SERVICES DE LA SOCIETE DE L'INFORMATION : https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre2#Article8

[50] GUIDELINES ON THE RIGHT TO DATA PORTABILITY : https://www.cnil.fr/sites/default/files/atoms/files/ld_portabilite_eng.pdf

- Formulaires « type » et mentions d'information.

Définir un modèle de processus de notification de violation de données personnelles

Cette activité est à mener lors de l'itération initiale du cycle PDCA.

Il s'agit ici de définir un modèle de processus avec l'organisation associée pour intégrer les éventuelles notifications de violation de données personnelles.

Le responsable du traitement doit en effet notifier toute violation de données personnelles à l'autorité de contrôle dans les meilleurs délais et si possible dans les 72 heures suite à la découverte de l'incident. La violation de données doit être communiquée à la ou les personnes concernées en cas de risque élevé. En outre, le sous-traitant doit notifier le responsable du traitement dans les meilleurs délais après avoir pris connaissance de la violation des données.

Que dit le GDPR ?

Article 4 - Définitions

«**violation de données à caractère personnel**», une 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;

Article 33 - Notification à l'autorité de contrôle d'une violation de données personnelles

1. En cas de violation de données à caractère personnel, le responsable du traitement en **notifie la violation en question à l'autorité de contrôle** […] **dans les meilleurs délais et, si possible, 72 heures** au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.

2. **Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais** après en avoir pris connaissance.

3. La notification […] doit, à tout le moins:

a) décrire la **nature de la violation** de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;
b) communiquer le **nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact** auprès duquel des informations supplémentaires peuvent être obtenues;
c) décrire les **conséquences probables de la violation** de données à caractère personnel;
d) décrire les **mesures prises** ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Article 34 - Communication à la personne concernée d'une violation de données personnelles

Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

Il est conseillé de reprendre, s'il existe, le même modèle de processus de gestion de crise offrant un temps de réaction très court en ligne avec les délais imposés par le GDPR.

Pour les entreprises disposant déjà d'un tel processus imposé par d'autres exigences réglementaires (Loi de Programmation Militaire (LPM)[51], Règlement « eIDAS »[52], directive européenne « NIS »[53], agrément HDS de l'ASIP Santé, etc.), une approche plus globale est vivement conseillée pour intégrer le processus de notification GDPR dans le cadre plus large établi.

> **Remarque** Selon l'étude ORGANISATIONAL READINESS FOR THE EUROPEAN UNION GENERAL DATA PROTECTION REGULATION mentionnée en introduction de ce livre blanc, 75% des entreprises interrogées affirment en avoir déjà en place une procédure de notification du fait d'autres législations.

Le modèle canonique à considérer comprend 6 principales étapes à structurer selon l'entreprise et ses pratiques.

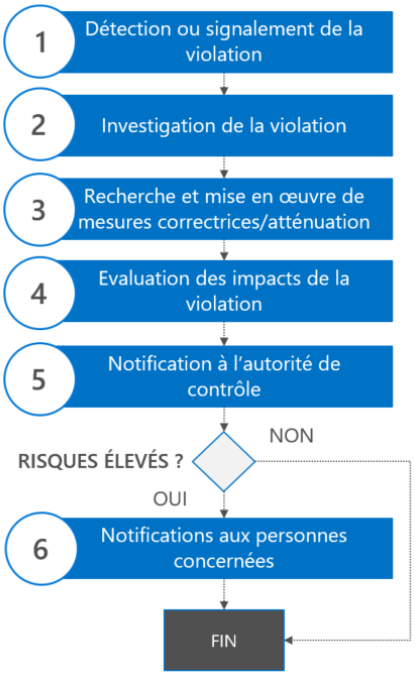


Figure 8 Illustration d'un « canevas » de processus de notification de violation de données personnelles

[51] LOI N° 2013-1168 DU 18 DECEMBRE 2013 RELATIVE A LA PROGRAMMATION MILITAIRE POUR LES ANNEES 2014 A 2019 ET PORTANT DIVERSES DISPOSITIONS CONCERNANT LA DEFENSE ET LA SECURITE NATIONALE : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825

[52] RÈGLEMENT (UE) N° 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 23 JUILLET 2014 SUR L'IDENTIFICATION ELECTRONIQUE ET LES SERVICES DE CONFIANCE POUR LES TRANSACTIONS ELECTRONIQUES AU SEIN DU MARCHE INTERIEUR ET ABROGEANT LA DIRECTIVE 1999/93/CE : http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32014R0910

[53] DIRECTIVE (UE) 2016/1148 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 6 JUILLET 2016 CONCERNANT DES MESURES DESTINEES A ASSURER UN NIVEAU ELEVE COMMUN DE SECURITE DES RESEAUX ET DES SYSTEMES D'INFORMATION DANS L'UNION : http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L1148

Remarque importante La notion de violation de données personnelles est plus large que la simple fuite d'information. Il est nécessaire de prendre en considération la destruction, la perte d'intégrité, etc. de données personnelles.

Il convient de prendre en compte et d'intégrer dans la définition de ce processus les modèles ou téléservices disponibles. La CNIL, en tant qu'autorité de contrôle, mettra à disposition sur le site cnil.fr un téléservice pour les notifications lors de l'entrée en vigueur du Règlement européen. Un formulaire PDF[54] est disponible dans l'intervalle.

Les livrables pour la mise en œuvre de cette activité sont le processus et la ou les procédures « canevas » de notification de violation de données personnelles.

Définir un Framework d'analyse d'impact relative à la protection des données

Si la précédente Directive 95/46/CE imposait une déclaration du traitement de données personnelles aux autorités de contrôle, il est considéré[55] que cette obligation n'avait pas l'efficacité attendue et que cette dernière devait être remplacée par un mécanisme ciblant spécifiquement les activités de traitement susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

La conséquence directe est que :

1. Les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques doivent être impérativement identifiés : ceci rentre typiquement dans le champ d'une étude préalable ;
2. Une analyse basée sur les risques et axée sur les données personnelles doit être conduite pour ces activités de traitement et les protections mises en place pour atténuer les risques identifiés : c'est ce que le nouveau Règlement appelle une analyse d'impact relative à la protection des données (Data Protection Impact Analysis en anglais ou DPIA).

Remarque Selon l'étude ORGANISATIONAL READINESS FOR THE EUROPEAN UNION GENERAL DATA PROTECTION REGULATION mentionnée en introduction de ce livre blanc, la moitié des entreprises interrogées disent conduire des analyses d'impact pour les traitements les plus critiques mais sans processus formel et sans outillage particulier.

Une telle analyse d'impact doit être menée uniquement dans le cas où les traitements sont susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques. Elle n'est donc pas obligatoire.

Les critères de cette analyse sont détaillés (Cf. ci-dessous) tels qu'une évaluation systématique et approfondie d'aspects personnels des personnes physiques, un traitement à grande échelle des données, la surveillance à grande échelle d'une zone accessible au public.

Les résultats de l'analyse d'impact relative à la protection des données permettent de prendre des décisions sur les mesures techniques et organisationnelles supplémentaires à mettre en place. Au cas où les risques résiduels seraient jugés trop élevés, la décision pourrait être prise, pour un nouveau traitement de ne pas autoriser sa mise en production quitte à abandonner le projet associé ou, pour un traitement existant, dans le cadre de l'étude de sa mise en conformité, de procéder à son retrait.

[54] Formulaire de notification de violation de données personnelles : https://www.cnil.fr/sites/default/files/typo/document/CNIL_Formulaire_Notification_de_Violations.pdf

[55] Considérant (89)

L'objet de cette activité réside dans les définitions des modalités qui conduisent à une telle analyse et dans celle de son exécution.

Structurer le processus d'analyse d'impact relative à la protection des données

L'article 35[56] définit les conditions et a minima les résultats attendus de l'analyse.

> ### Que dit le GDPR ?
>
> **Article 35 - Analyse d'impact relative à la protection des données**
> Lorsqu'un type de traitement, en particulier par **le recours à de nouvelles technologies**, et **compte tenu de la nature, de la portée, du contexte et des finalités du traitement**, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel.
>
> […]
>
> L'analyse contient au moins :
> a) une description systématique des **opérations de traitement envisagées** et des **finalités du traitement**, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement;
> b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités;
> c) une **évaluation des risques** pour les droits et libertés des personnes concernées […];
> d) les mesures envisagées pour faire face aux risques, y compris les **garanties, mesures et mécanismes de sécurité** visant à assurer la protection des données personnelles et à apporter la preuve du respect du présent règlement […].

Si les termes ci-dessus restent assez généraux, les critères sont définis plus précisément aux considérants (91) et (92). Les critères à prendre en compte sont les suivants :

- Les **opérations de traitement à grande échelle** qui visent à traiter une quantité très élevée de données personnelles susceptibles d'entraîner un risque élevé[57] ;
- Les activités de traitement pour prendre des décisions concernant des personnes physiques spécifiques suite à une évaluation systématique et approfondie des aspects personnels relatifs aux personnes physiques en fonction du **profilage** de ces données ;
- Le traitement de **catégories particulières de données personnelles**, de données biométriques ou de données relatives aux condamnations et infractions pénales ou aux mesures de sécurité connexes ;
- **La surveillance à grande échelle de zones accessibles au public**, où les données empêchent ces personnes d'exercer un droit ou de bénéficier d'un service ou d'un contrat ;
- Lorsque plusieurs responsables du traitement envisagent de créer **une application ou un environnement de traitement communs** à tout un secteur ou segment professionnel, ou pour une activité transversale largement utilisée[58].

Deux exceptions sont stipulées « si le traitement concerne les données personnelles des patients ou des clients par un médecin individuel, un autre professionnel de la santé ou un avocat ».

---

[56] ARTICLE 35 - ANALYSE D'IMPACT RELATIVE A LA PROTECTION DES DONNEES : https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article35

[57] Considérant (91)

[58] Considérant (92)

Conduire une étude préalable

En regard de ce qui est énoncé, nous recommandons d'intégrer une étude préalable conduisant à une décision motivée et formalisée quant à la conduite ou non d'une analyse d'impact relative à la protection des données pour le traitement considéré. L'étude préalable doit identifier i) les risques inhérents du traitement et dans la mesure du possible et de façon préliminaire ii) les actions à mener pour la mise en conformité du traitement au GDPR.

Cette étude préalable doit conduire, sur la base de cette analyse, à une décision formalisée quant à la nécessité ou non d'approfondir l'analyse du traitement et des risques sur la vie privée qu'il fait porter sur les personnes concernées. Il s'agit de définir un arbre de décision conduisant à ce statut en sortie. Les éléments à prendre en considération sont, de façon évidente, les fiches de traitement et de cycle de vie de données personnelles, les critères et éventuelles pondérations associées, la ou les phases de validation de la proposition de décision pour conduire à une décision formalisée pour la suite à donner.

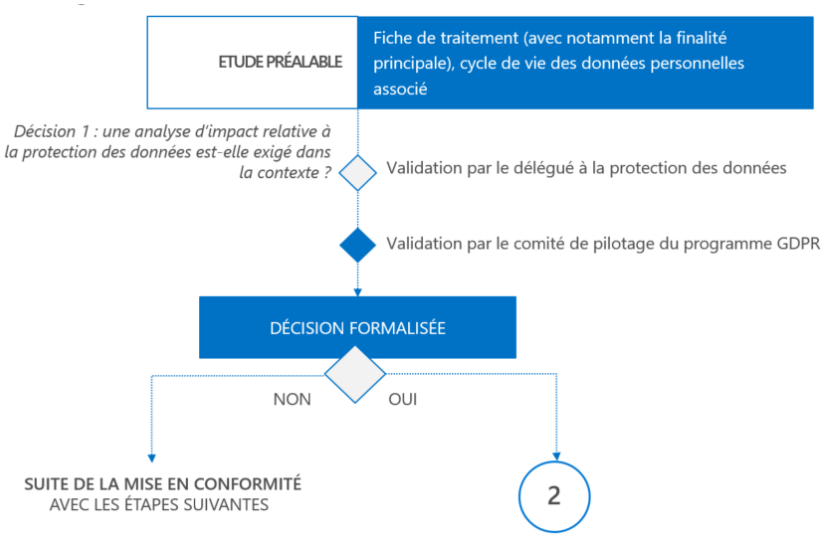


Figure 9 Exemple d'arbre de décision pour décider d'une analyse d'impact relative à la protection des données

Dans l'hypothèse où l'arbre de décision précédent conclurait à la nécessité d'une analyse d'impact, il convient alors de structurer un (« canevas » de) processus complet d'analyse d'impact répondant aux exigences exprimées du GDPR.

Conduire une analyse d'impact relative à la protection des données

L'analyse d'impact représente l'opportunité de conduire de façon approfondie i) une étude juridique à l'égard du traitement considéré et ii) une analyse des risques identifiés avec pour corollaires la définition de plan d'atténuation des risques, d'évaluation des risques résiduels, des pondérations, priorisation et itérations associés.

Au-delà des nécessaires validations et avis du Délégué à la Protection des Données, les risques résiduels doivent être identifiés, évalués et acceptés.

A l'instar de l'étude préalable, les conclusions de l'étude d'analyse d'impact doivent être consignées dans un rapport d'analyse d'impact. Ce rapport doit faire l'objet d'une validation du comité de pilotage du programme GDPR et, bien sûr, être consigné dans le Registre des traitements pour le traitement considéré à des fins de traçabilité dans le cadre de la documentation globale à maintenir pour la conformité avec le GDPR.

La figure suivante synthétise les grandes lignes ainsi brossées d'un « canevas » d'analyse d'impact relative à la protection des données.

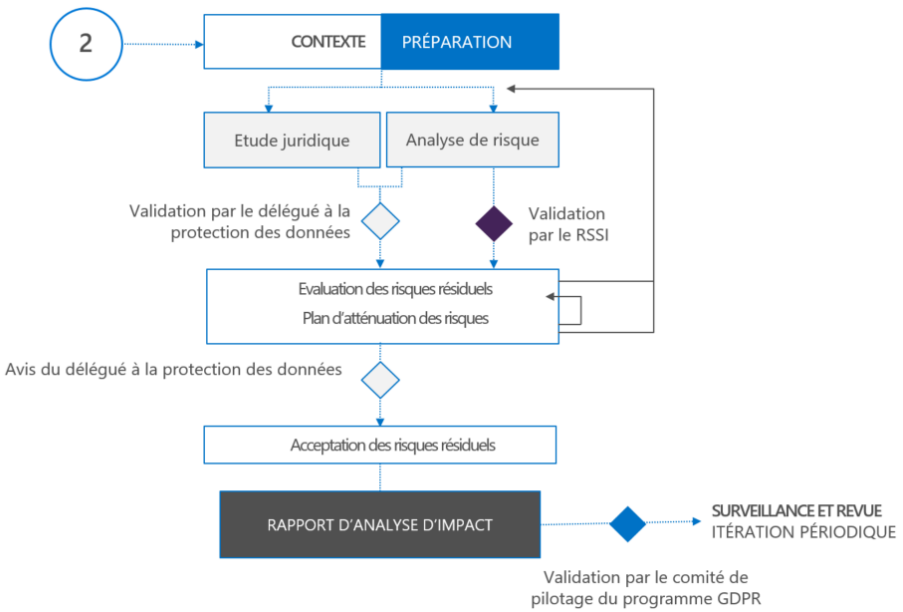


Figure 10 Exemple de « canevas » d'analyse d'impact relative à la protection des données

Les différentes boîtes de cette figure sont bien sûr à préciser en termes de méthodes, bonnes pratiques, d'outillage, etc. à intégrer dans ce Framework.

> **Remarque** Conscient du fait que le Règlement possède de nombreuses zones de flou, propres à interprétation, le G29 s'est engagé à travailler sur des guides dits « lignes directrices » clarifiant et illustrant par des exemples concrets la mise en œuvre et le déploiement opérationnel du GDPR. Au sein du corpus de lignes directrices d'ores et déjà disponibles – un certain nombre de lignes directrices sont encore en cours de définition à la date de publication de ce livre blanc – les lignes directrices ANALYSE D'IMPACT (EN)[59] permettent d'éclairer sur un jour bienvenu le Framework à établir.

> **Remarque** La CNIL propose un corpus de documents sur l'analyse d'impact : PIA-1, LA METHODE : COMMENT MENER UNE ETUDE D'IMPACT SUR LA VIE PRIVEE[60], PIA-2, L'OUTILLAGE : MODELES ET BASES DE CONNAISSANCE DE L'ETUDE D'IMPACT SUR LA VIE PRIVEE[61] et PIA-3, LES BONNES PRATIQUES : MESURE POUR TRAITER MES RISQUES SUR LES LIBERTES ET LA VIE PRIVEE[62].

L'étude juridique s'appuiera sur un questionnaire (qu'il vous faudra construire) qui synthétisera les exigences réglementaires. A titre d'exemple, le tableau ci-dessous énonce sous forme de questions les exigences des articles 5 et 7.

---

[59] GUIDELINES ON DATA PROTECTION IMPACT ASSESSMENT (DPIA) AND DETERMINING WHETHER PROCESSING IS "LIKELY TO RESULT IN A HIGH RISK" FOR THE PURPOSES OF REGULATION 2016/679 : https://www.cnil.fr/sites/default/files/atoms/files/ld_dpia_eng.pdf

[60] PIA-1, LA METHODE : COMMENT MENER UNE ETUDE D'IMPACT SUR LA VIE PRIVEE : https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methode.pdf

[61] PIA-2, L'OUTILLAGE : MODELES ET BASES DE CONNAISSANCE DE L'ETUDE D'IMPACT SUR LA VIE PRIVEE : https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Outillage.pdf

[62] PIA-3, les bonnes pratiques : Mesure pour traiter mes risques sur les libertés et la vie privée : https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-3-BonnesPratiques.pdf

Index	Question	Réponse	Statut
Traitement des données à caractère personnel (Art 5)			
1	Les données collectées sont-elles uniquement celles nécessaires au traitement ? (Art 5.1 b)	Réponse :	Accepté A revoir Refusé
2	Les données collectées sont-elles utilisées pour d'autres finalités que le traitement ? (Art 5.1 b)	Réponse :	
3	Existe-t-il un mécanisme de mise à jour des données qui puisse garantir la possibilité de rectification ou suppression des données inexactes (Art 5.1 d)	Réponse :	
4	Les données permettant l'identification des personnes concernées sont-elles détruites une fois le traitement opéré ? (Art 5.1 e)	Réponse :	
Conditions du consentement (Art 7)			
5	Est-il possible de démontrer que la personne a donné son consentement au traitement de ses données personnelles ? (Art 7.1)	Réponse :	
6	Le consentement est-il décrit de manière claire en langage compréhensible et distinguable s'il est inclus avec d'autres sujets ? (Art 7.2)	Réponse :	
7	La personne concernée peut-elle être en mesure de revenir à tout moment sur son consentement ? (Art 7.3)	Réponse :	
8	L'exécution du contrat est-il subordonné au consentement de traitement de données personnelles **non** nécessaires de ce traitement ? (Art 7.4)	Réponse :	

La deuxième partie de l'analyse d'impact relative à la protection des données consiste à mener une **analyse des risques orientée sur la protection des données personnelles**. Le Règlement n'impose ni ne préconise de méthode d'analyse des risques, mais la démarche d'évaluation des risques sécurité est une démarche classique et bien connue des responsables sécurité.

Remarque Pour la composante « analyse de risques » et ce qui s'en suit, les normes et standards en la matière sont bien évidemment applicables, qu'il s'agisse des normes ISO/IEC 27005:2011[63] GESTION DES RISQUES LIES A LA SECURITE DE L'INFORMATION, ISO 31000:2009[64] MANAGEMENT DU RISQUE -- PRINCIPES ET LIGNES DIRECTRICES et IEC 31010:2009[65] GESTION DES RISQUES -- TECHNIQUES D'EVALUATION DES RISQUES, de la méthode EBIOS[66] (Expression des Besoins et Identification des Objectifs de Sécurité) 2010 de l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) pour la composante « analyse de risques », etc.

La démarche classique d'une analyse de risques couvre différentes étapes ; après avoir défini le périmètre, on identifie les actifs et les menaces. Ensuite on évalue les mesures de sécurité existantes, les vulnérabilités pour finir par évaluer les risques, la probabilité d'occurrence, les impacts. Enfin, on envisage les contre-mesures que l'on mettra en œuvre pour couvrir les risques, en acceptant les risques résiduels.

Cartographier les traitements de données personnelles

Cette activité comporte deux sous-activités :

1. Réactualiser la liste des traitements de données personnelles ;
2. Etablir la documentation des traitements de données personnelles.

Celles-ci sont décrites dans l'ordre dans les sections suivantes.

Réactualiser la liste des traitements de données personnelles

Cette activité est à mener pour s'assurer que l'organisation dispose bien d'un **Registre des traitements à jour** où l'ensemble des traitements de données personnelles de l'organisation sont dûment identifiés et répertoriés de façon pertinente et adéquate.

En effet, le GDPR impose une « conformité dynamique ». Avec le GDPR, il est donc nécessaire de faire évoluer les éléments de description du traitement pour être en mesure de répondre à tout moment à un audit qui serait imposé par l'autorité de contrôle.

Cette activité rentre typiquement dans la dimension multicycle et l'approche itérative proposée. Elle permet notamment à chaque cycle de s'assurer que le cycle de vie des données personnelles et le diagramme des flux de données associé soient mis à jour à intervalles réguliers (c'est-à-dire a minima à chaque cycle) afin de prendre en compte les évolutions du traitement et de ses composantes : service, application, dépôt de données.

Il s'agit également d'une opportunité pour la prise en compte et l'intégration de nouveaux traitements de données personnelles.

Il convient finalement de réévaluer la priorisation de la liste des traitements figurant dans le Registre des traitements, ce qui constitue le livrable pour la mise en œuvre de cette activité.

Etablir la documentation des traitements de données personnelles

Cette activité est à mener pour chaque traitement de données personnelles identifié dans le cadre du programme. Elle est, dans la pratique, conduite sur la base de la liste des traitements classés par ordre

[63] ISO/IEC 27005:2011 TECHNOLOGIES DE L'INFORMATION -- TECHNIQUES DE SECURITE -- GESTION DES RISQUES LIES A LA SECURITE DE L'INFORMATION : https://www.iso.org/fr/standard/56742.html

[64] ISO 31000:2009 MANAGEMENT DU RISQUE -- PRINCIPES ET LIGNES DIRECTRICES : https://www.iso.org/fr/standard/43170.html

[65] IEC 31010:2009 GESTION DES RISQUES -- TECHNIQUES D'EVALUATION DES RISQUES : https://www.iso.org/fr/standard/51073.html

[66] EBIOS - EXPRESSION DES BESOINS ET IDENTIFICATION DES OBJECTIFS DE SECURITE : https://www.ssi.gouv.fr/guide/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite/

de priorité (Cf. section précédente) : par exemple, les traitements de données personnelles les plus prioritaires sont considérés pour l'itération courante du cycle PDCA.

Cette activité doit permettre de renseigner le modèle de fiche descriptive préalablement établi pour chaque traitement considéré dans le cadre de cette itération du cycle PDCA. On devra aller au-delà des premiers éléments d'information récoltés lors de l'estimation du périmètre du programme GDPR et de leur analyse critique (Cf. section § ESTIMER LE PERIMETRE DU PROGRAMME GDPR EN MATIERE DE TRAITEMENTS DE DONNEES PERSONNELLES).

Il convient ainsi d'établir de façon non-exhaustive :

- La finalité principale du traitement ;
- S'il s'agit d'un traitement relatif à des données personnelles de mineurs ;
- La façon dont est demandé, obtenu, et enregistré le consentement ;
- Le niveau de contrôle (c'est-à-dire avec recours ou non à des sous-traitants) ;
- Les mesures de sécurité techniques et organisationnelles pour protéger les données personnelles.

Cette activité est menée par le responsable du traitement – et le cas échant les personnes en charge des services, applications, dépôts identifiés dans ce contexte – en relation avec le Délégué à la Protection des Données qui apporte ici sa connaissance du Règlement. Chaque fiche de traitement est visée par ce même Délégué à la Protection des Données pour approbation, le RSSI pouvant être mis à contribution pour valider les mesures de sécurité décrites.

Il est recommandé de faire figurer en annexe, un descriptif du cycle de vie des données établi sur la base du modèle précédemment défini.

La description du cycle de vie des données personnelles est nécessaire pour la planification et la mise en œuvre de la capacité d'exercice des droits de la personne concernée sur ses données – le droit d'accès, de rectification, de suppression, etc.

De plus, cette description du cycle complet de vie des données permet d'assurer qu'il n'y a pas d'utilisation secondaire des données personnelles, ce qui constitue un prérequis pour pouvoir « prouver sa conformité ». Le transfert des données vers des tiers doit aussi être pris en compte dans la suite du déroulé du programme et des activités associées : le responsable du traitement doit spécifier vers qui les données sont transférées et pour quel(s) traitement(s). Un exemple est l'utilisation du Cloud où le fournisseur de services de cloud (Cloud Service Provider en anglais ou CSP) en tant que sous-traitant devra être inclus dans le périmètre du traitement des données et de la gestion associée.

> **Remarque importante** Il est nécessaire de ne pas s'intéresser uniquement aux données transférées et stockées sous forme numérique. GDPR s'applique en effet également aux autres formes physiques telles que photocopie, scan, courrier postal ou transporteur.

La description doit également intégrer, s'il y a lieu, le transfert des données en-dehors de l'Union Européenne (UE). En effet, autant les transferts à l'intérieur de l'UE sont autorisés entre tous les États membres, autant le transfert en-dehors de l'UE reste soumis aux conditions décrites au chapitre V du Règlement.

Les diagrammes résultant de l'application du modèle doivent indiquer les catégories de données personnelles selon leur sensibilité – l'article 9 définit un ensemble de données sensibles (race, religion, origine ethnique, ...). Ils nécessiteront ensuite un examen particulier pour s'assurer que les contrôles qu'ils décrivent sont adaptés au niveau de risque fonction des catégories de données. C'est l'objet des activités suivantes comme l'étude préalable (Cf. section suivante) ou par exemple la modélisation des menaces (Cf. section § INTEGRER UNE DEMARCHE GUIDEE).

Le livrable en sortie de cette activité correspond à la mise à jour du Registre des traitements avec la fiche de traitement et le cycle de vie des données personnelles dûment complétés pour chaque traitement de données personnelles retenu pour cette itération du cycle PDCA.

Procéder à une étude préalable du niveau de risque des traitements de données personnelles

Cette activité est à mener pour chaque traitement de données personnelles identifié dans le cadre du programme. Elle est dans la pratique conduite sur la base de la liste des traitements classés par ordre de priorité : les traitements les plus prioritaires sont considérés pour l'itération courante du cycle PDCA.

Il s'agit de conduire une étude préalable afin de prioriser les actions à mener au regard des risques pour la phase METTRE EN ŒUVRE du cycle PDCA. Cette étude reprend le déroulé et la structure établis avec le Framework d'analyse d'impact relative à la protection des données, Cf. section § DEFINIR UN FRAMEWORK D'ANALYSE D'IMPACT RELATIVE A LA PROTECTION DES DONNEES, et vise à identifier :

1. Les risques liés au traitement.
2. Les différentes actions à mener pour la mise en conformité avec les objectifs et exigences du GDPR.

Pour chaque traitement considéré, il convient de porter une attention au traitement en tant que tel et aux données personnelles qu'il recouvre, et donc de façon non-exhaustive :

- D'identifier la base juridique sur laquelle repose le traitement en termes de contrats, d'obligations légales, d'intérêt légitime, de consentement, etc. ;
- De vérifier que seules les données strictement nécessaires au traitement considéré sont collectées et utilisées, que celles-ci ne sont pas conservées plus que nécessaire ;
- De considérer la nature de données personnelles et le type de traitement qui peuvent imposer une analyse d'impact sur la base du Framework précédemment défini ;
- De considérer les éventuels transferts de données et la possible nécessité de les encadrer ;
- De vérifier les clauses contractuelles dans le cas de recours à des sous-traitants.

Il est également important de vérifier l'existence et les modalités d'exercice des droits des personnes concernées, et de façon non-exhaustive de :

- Vérifier la présence **d'un consentement préalable explicite**, son enregistrement pour de futurs audits ;
- Mesurer le niveau d'alignement pour les nouveaux droits avec les modèles de processus « canevas », les formulaires « type » et les mentions d'informations, Cf. section § DEFINIR/REVOIR/METTRE A JOUR LES DIFFERENTS MODELES VIS-A-VIS DU CONSENTEMENT ET DES NOUVEAUX DROITS DES PERSONNES CONCERNEES.

De la même façon, les mesures de sécurité techniques et organisationnelles doivent être passées en revue de façon à mesurer l'adéquation :

1. De l'ensemble des contrôles de sécurité techniques mis en place pour assurer la protection des données personnelles ;
2. Des mesures organisationnelles observées.

Sur la base des éléments précédents, on pourra enfin statuer, en fonction de la nature des risques identifiés, si une analyse d'impact de la protection des données personnelles s'avère nécessaire. Il s'agit

d'appliquer ici l'arbre de décision du Framework d'analyse d'impact de la protection des données personnelles :

- Si la décision est prise de ne PAS continuer sur une analyse d'impact relative à la protection des données, les arguments ayant servi à motiver et justifier ce choix seront consignés et archivés pour servir en cas d'audit par l'autorité de contrôle ;
- Si la décision est prise de continuer sur une analyse d'impact relative à la protection des données, le livrable de cette étude préalable et la fiche de traitement de l'étape précédente serviront de données d'entrée pour l'analyse d'impact. Cette activité est décrite à la section suivante.

Comme le suggèrent les lignes précédentes, le livrable en sortie de cette activité est une décision formalisée et motivée vis-à-vis de la nécessité ou non d'une analyse d'impact relative à la protection des données. Cette décision est validée par le Délégué à la Protection des Données personnes et le comité de pilotage du programme GDPR.

Gérer les risques pour les traitements de données personnelles à risque élevé

Cette activité est à mener pour chaque traitement de données personnelles identifié dans le cadre du programme GDPR et considéré à risque élevé pour les droits et les libertés des personnes concernées au regard des données collectées et utilisées ainsi que le type de traitement réalisé. (Les traitements de données personnelles les plus prioritaires sont potentiellement uniquement considérés pour l'itération courante du cycle PDCA).

Comme abordé lors de l'activité de définition d'un Framework ad 'hoc (Cf. section § DEFINIR UN FRAMEWORK D'ANALYSE D'IMPACT RELATIVE A LA PROTECTION DES DONNEES), une analyse d'impact relative à la protection des données doit être menée « Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques »[67].

La décision de procéder à une telle analyse d'impact se base sur la décision formalisée de l'activité précédente d'étude préalable si celle-ci a relevé un ou plusieurs risques élevés. Elle va se fonder sur l'analyse de la fiche descriptive du traitement considéré, du cycle de vie des données personnelles associé et de la cartographie des flux de données obtenues dans des activités et éventuellement cycles précédents.

Il s'agit d'appliquer le processus établi avec le Framework d'analyse d'impact relative à la protection des données. Ainsi, l'analyse d'impact relative à la protection des données se décline typiquement en deux volets :

1. Une étude poussée de la base juridique qui prend en compte les exigences au sens réglementaire déclinées dans les différents articles du Règlement.
2. Une analyse des risques sécurité orientée sur la protection des données personnelles et assortie :
    a. D'un plan d'atténuation des risques décrivant les mesures de sécurité techniques et organisationnelles pour répondre aux risques identifiés et permettant de se conformer aux objectifs et exigences du GDPR ;

[67] ARTICLE 35 - ANALYSE D'IMPACT RELATIVE A LA PROTECTION DES DONNEES, paragraphe 1 : https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article35

b. D'une évaluation des risques résiduels.

Le Règlement n'impose ni ne préconise de méthode d'analyse des risques, mais la démarche d'évaluation des risques sécurité est une démarche classique et bien connue des responsables sécurité. Nous avons indiqué lors de l'activité de définition du Framework quelques guides susceptibles d'éclairer l'organisation sur la meilleure conduite à tenir en fonction de ses pratiques.

Comme déjà discuté, le résultat final de cette analyse propose une vue concise des mesures d'atténuation à implémenter pour couvrir les risques identifiés comme les plus critiques, et des risques résiduels.

A ce stade, on dispose de trois options :

1. Soit on considère que les risques résiduels sont acceptables et on continue le traitement avec la mise en œuvre des atténuations retenues ;
2. Soit on considère que, malgré les mesures d'atténuation proposées, le risque n'est pas acceptable et on arrête le traitement ;
3. Soit on décide de consulter l'autorité de contrôle pour obtenir son avis avant toute mise en œuvre du traitement.

De fait, le considérant (84)[68] du GDPR stipule que « *lorsqu'il ressort de l'analyse d'impact relative à la protection des données que les opérations de traitement des données comportent un risque élevé que le responsable du traitement ne peut atténuer en prenant des mesures appropriées compte tenu des techniques disponibles et des coûts liés à leur mise en œuvre, il convient que l'autorité de contrôle soit consultée avant que le traitement n'ait lieu*. ».

Cette décision est du ressort du Délégué à la Protection des Données, et par extension directe du comité de pilotage qui prend les décisions et arbitrages nécessaires pour lesquels il a reçu délégation du Comité de Direction de l'organisation.

> **Remarque** Il convient éventuellement de dissocier, dans les options précédentes, la situation d'un nouveau traitement à mettre en œuvre de celle d'un traitement existant à rendre conforme.

Le livrable en sortie de cette activité est, pour chaque traitement à risque élevé considéré dans cette itération du cycle PDCA, un rapport d'analyse d'impact validé par le comité de pilotage du programme GDPR avec l'acceptation du plan d'atténuation des risques ET des risques résiduels dûment identifiés. Ceci est assorti d'une obligation d'une surveillance et d'une revue périodiques dans le cadre de la phase VERIFIER du cycle PDCA, Cf. section § SUIVRE LES TRAITEMENTS DE DONNEES A RISQUE ELEVE.

[68] Nous retrouvons la même idée dans le considérant (94) du GDPR.

Mettre en œuvre le programme GDPR

La phase **METTRE EN ŒUVRE** du cycle PDCA est constituée d'un ensemble d'activités :

- Gouverner la façon dont les données personnelles sont accédées et utilisées ;
- Classifier les données personnelles ;
- Améliorer la sécurité des traitements et des données personnelles ;
- Mettre en place un processus de notification de violation des données personnelles ;
- Améliorer la prise de conscience et la collaboration en interne.

Ces activités sont décrites de façon unitaire dans les sections suivantes.

Gouverner la façon dont les données personnelles sont accédées et utilisées

Cette activité est à mener pour chaque traitement de données personnelles identifié dans le cadre du programme. Elle est dans la pratique conduite sur la base de la liste des traitements classés par ordre de priorité : les traitements les plus prioritaires sont considérés pour l'itération courante du cycle PDCA.

Cette activité comporte un ensemble de sous-activités :

- Décliner les politiques et définir les rôles et les responsabilités pour la gestion et l'utilisation des données personnelles ;
- Identifier et gérer les sous-traitants en particulier avec l'avènement du Cloud ;
- Intégrer/revoir la prise en charge du consentement et des nouveaux droits pour les personnes concernées.

Celles-ci sont décrites dans les sections suivantes.

Décliner les politiques et définir les rôles et les responsabilités pour la gestion et l'utilisation des données personnelles

Cette activité consiste à préciser le plan de gouvernance des données, c'est-à-dire développer les standards de sécurité qui régissent comment les données personnelles sont gérées, accédées, transférées et supprimées :

- Au repos, en traitement et en transit ;
- Stocker, Recouvrer, Conserver, Archiver, Retirer.

Ainsi que ceux régissant la conservation des données (fonction de leurs types et sensibilités).

Les livrables en sortie de cette activité sont les suivants de façon non-exhaustive :

- Procédure(s) de traitement conforme aux exigences du Règlement ;
- Politique de conservation des données personnelles ;
- Calendrier de conservation des données personnelles ;
- Procédure de suppression de données personnelles du stockage.

Identifier et gérer les sous-traitants en particulier avec l'avènement du Cloud

Cette activité vise à s'assurer que les sous-traitants connaissent leurs obligations et responsabilités liées au GDPR.

Les rôles et responsabilités entre responsable du traitement et sous-traitant évoluant (Cf. section § QUELQUES DEFINITIONS STRUCTURANTES), les sous-traitants devront, d'ici la date de la mise en application du GDPR, se mettre en conformité au GDPR s'ils veulent permettre à leurs clients de l'être eux-mêmes.

Avec les services Cloud, tous les fournisseurs de services de cloud (CSP) sur lesquels s'appuient de plus en plus d'organisations ou entreprises se trouvent dans ce cas. Les services de type IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service) et/ou SaaS (Software-as-a-Service) qui sont ainsi souscrits participent au Système d'Information et potentiellement à des traitements de données personnelles.

> **Remarque** La notion de coresponsabilité au sens du GDPR trouve également un écho dans les responsabilités partagées induites selon le modèle de déploiement (IaaS vs. PaaS vs. SaaS) relatif du ou des services participants au traitement de données personnelles. Pour plus d'information, vous pouvez consulter le livre blanc SHARED RESPONSIBILITY FOR CLOUD COMPUTING[69].

Pour les plus grands acteurs de type fournisseur de services de cloud, il n'y a d'autre alternative que de s'engager à être conformes.

> **Remarque** Microsoft s'est ainsi très tôt engagé[70] [71] dans la mise en conformité au GDPR, que ce soit pour nous-même ou pour nos clients afin d'aboutir à une conformité complète en mai 2018, dans la mesure où i) un certain nombre de points doivent encore être précisés, notamment par le G29 dans l'attente de lignes directrices comme indiqué précédemment, et où ii) Microsoft finalisera dans le courant de cette année 2017 une approche rationalisée et standardisée, par défaut, pour l'ensemble de ses clients.
>
> De plus, comme indiqué dans la section GDPR[72] du Centre de confiance (Trust Center), Microsoft s'engage à faire profiter ses clients de sa propre expérience dans son voyage vers la conformité.

> **Remarque** Il convient de noter que dans les termes des services en ligne[73] (Online Services Terms en anglais ou OST), Microsoft respecte strictement la règlementation applicable. A ce propos, et comme cela a été souligné précédemment, depuis le 1er septembre, les termes des services en ligne intègrent les engagements de Microsoft envers la conformité au GDPR.

Il s'agit d'identifier et passer en revue – sur la base de la fiche de traitement – l'ensemble des contrats des sous-traitants et d'imposer que ceux-ci prennent en considération le GDPR avec les obligations et responsabilités qui incombent désormais aux sous-traitants.

---

[69] SHARED RESPONSIBILITY FOR CLOUD COMPUTING : https://aka.ms/sharedresponsibility

[70] GET GDPR COMPLIANT WITH THE MICROSOFT CLOUD : https://blogs.microsoft.com/on-the-issues/2017/02/15/get-gdpr-compliant-with-the-microsoft-cloud/#iZGet150clyXZ5CI.99

[71] EARNING YOUR TRUST WITH CONTRACTUAL COMMITMENTS TO THE GENERAL DATA PROTECTION REGULATION : https://blogs.microsoft.com/on-the-issues/2017/04/17/earning-trust-contractual-commitments-general-data-protection-regulation/#V8LbkmkbCDryjhd1.99

[72] THE GENERAL DATA PROTECTION REGULATION (GDPR) : https://www.microsoft.com/GDPR

[73] Licensing Terms and Documentation : http://go.microsoft.com/?linkid=9840733

Cela suppose de s'assurer de la présence en bonne et due forme de clauses contractuelles en matière de sécurité et de protection des données personnelles.

Remarque Microsoft a été le premier des grands acteurs de type fournisseurs de services de cloud à adopter le premier code international des bonnes pratiques de protection des données personnelles dans le Cloud, à savoir la norme ISO/IEC 27018:2014[74]. Pour de plus amples informations, vous pouvez vous reporter à l'article ISO/IEC 27018 CODE OF PRACTICE FOR PROTECTING PERSONAL DATA IN THE CLOUD[75] sur le Centre de confiance Microsoft.

Remarque Afin de permettre à nos clients de s'assurer que les services de cloud de Microsoft sont gérés correctement et de leur offrir des garanties en la matière, les services de cloud sont vérifiés au moins chaque année vis-à-vis de plusieurs normes globales de protection de données, comprenant plusieurs normes ISO/IEC, le Registre STAR de la CSA (Cloud Security Alliance), HIPAA et HITECH. Ces rapports sont accessibles à l'adresse https://servicetrust.microsoft.com/Documents/ComplianceReports.

Il convient également d'encadrer les transferts en dehors de l'Union Européenne, par exemple les clauses contractuelles types.

Remarque Au sein du corpus de lignes directrices d'ores et déjà disponibles du G29, les lignes directrices AUTORITE CHEF DE FILE (EN)[76] donnent des éclaircissements pour la détermination de l'autorité compétente en cas de traitement transfrontalier.

Au même titre que l'ensemble des traitements de données personnelles de l'organisation sont consignés dans un Registre des traitements, nous conseillons d'établir un Registre (de risques) des sous-traitants bien que cette dimension ne soit pas spécifiquement abordée par le GDPR.

C'est l'occasion de définir les modalités de gestion afférentes dans le Registre :

- Ajout, mise à jour et suppression d'un sous-traitant ;
- Ajout, mise à jour et suppression d'un contrat pour un sous-traitant donné.

Enfin, cette activité se doit d'établir un processus pour assoir le niveau de sécurité de l'ensemble des nouveaux tiers qui entrent en contact avec les données personnelles d'un traitement.

Au final, les livrables en sortie de cette activité sont les suivants :

- Procédures de gestion des contrats ;
- Registre (de risque) des sous-traitants (comprenant les contrats avec les tiers) ;
- (Encadrement des) Transferts de données personnelles hors de l'Union Européenne.

Intégrer/revoir la prise en charge du consentement et des nouveaux droits pour les personnes concernées

Cette activité consiste, en fonction des résultats de l'étude préalable, à s'assurer de la présence d'un consentement explicite lors de la collecte de données personnelles dans le cadre d'un traitement avec

[74] ISO/IEC 27018:2014 TECHNOLOGIES DE L'INFORMATION -- TECHNIQUES DE SECURITE -- CODE DE BONNES PRATIQUES POUR LA PROTECTION DES INFORMATIONS PERSONNELLES IDENTIFIABLES (PII) DANS L'INFORMATIQUE EN NUAGE PUBLIC AGISSANT COMME PROCESSEUR DE PII : https://www.iso.org/fr/standard/61498.html

[75] ISO/IEC 27018 CODE OF PRACTICE FOR PROTECTING PERSONAL DATA IN THE CLOUD : https://www.microsoft.com/en-us/TrustCenter/Compliance/ISO-IEC-27018

[76] GUIDELINES FOR IDENTIFYING A CONTROLLER OR PROCESSOR'S LEAD SUPERVISORY AUTHORITY : https://www.cnil.fr/sites/default/files/atoms/files/lead_authorityen.pdf

la ou les mention(s) d'information conforme(s) aux exigences du Règlement vis-à-vis de la finalité, de la durée de conservation, etc.

Les conditions particulières propres aux mineurs doivent par ailleurs évidemment être abordées si applicables dans le contexte.

> Que dit le GDPR ?
>
> **Article 7 - Conditions applicables au consentement**
> Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant
>
> **Article 8 - Conditions applicables au consentement des enfants en ce qui concerne les services de la société de l'information**

Elle consiste par ailleurs en l'adaptation si nécessaire des processus/procédures pour permettre aux personnes concernées l'exercice de leurs droits en matière de protection de la vie privée. Il s'agit en d'autres termes de mettre à disposition des possibilités d'accès, de correction ou encore de suppression de leurs données personnelles.

Il s'agit donc, en fonction des résultats de l'étude préalable, d'intégrer ou de revoir le support des droits suivants :

- Droits étendus quant à l'accès, à la rectification ou à la suppression des données erronées ;
- Droits à l'effacement des données (également appelé droit à l'oubli) ;
- Droits pour restreindre le traitement des données :
  - Prévention du marketing direct – enregistrement(s) des consentements,
  - Prévention des prises de décision automatisée et du profilage.
- Droit à la portabilité des données.

Remarque Conscient du fait que le Règlement possède de nombreuses zones d'interprétation, le G29 s'est engagé à travailler sur des guides dits « lignes directrices » clarifiant et illustrant par des exemples concrets la mise en œuvre et le déploiement opérationnel du GDPR. Au sein du corpus de lignes directrices d'ores et déjà disponibles – d'autres sont encore en cours de définition à la date de publication de ce livre blanc – les lignes directrices PORTABILITE (EN)[77] permettent d'éclairer les attendus relatifs au droit à la portabilité, un nouveau droit décrit à l'article 20 qui impose de pouvoir transmettre les données d'un système de traitement à un autre.

Remarque La future norme ISO/IEC FDIS 19941[78] TECHNOLOGIES DE L'INFORMATION -- INFORMATIQUE EN NUAGE -- INTEROPERABILITE ET PORTABILITE vise à assurer un examen pragmatique et une communication claire sur la portabilité des données dans un contexte d'informatique en nuage (cloud computing). Elle permet d'établir notamment une compréhension commune de la portabilité en définissant les termes et concepts associés dans le cloud, en proposant une vue d'ensemble des types de portabilité et en explorant les différences et les problèmes liés à la portabilité dans le cloud. Elle permet ainsi l'évaluation de la portabilité pour des scénarii de services de cloud spécifiques.

[77] GUIDELINES ON THE RIGHT TO DATA PORTABILITY : https://www.cnil.fr/sites/default/files/atoms/files/ld_portabilite_eng.pdf

[78] ISO/IEC FDIS 19941 TECHNOLOGIES DE L'INFORMATION -- INFORMATIQUE EN NUAGE -- INTEROPERABILITE ET PORTABILITE : https://www.iso.org/fr/standard/66639.html

Remarque importante L'exercice des droits ci-dessus s'applique non seulement aux données de production mais également aux données sauvegardées ainsi qu'aux données archivées.

La classification des données personnelles facilite dans ce contexte l'identification des données concernées (Cf. section suivante).

Les livrables en sortie de cette activité sont les suivants, pour chaque traitement considéré, de façon non-exhaustive :

- Mention(s) d'information (pour les traitements) conforme aux exigences du Règlement ;
- Procédure(s) pour un consentement explicite ou son enregistrement ;
- Procédure(s) et formulaire de demande de retrait du consentement ;
- Procédure(s) et formulaire de demande d'accès pour les personnes concernées ;
- Procédure(s) et formulaire de demande de rectification ou d'effacement des données erronées ;
- Procédure(s) et formulaire de demande d'effacement de données (sous certaines conditions) ;
- Procédure(s) et formulaire de demande de restriction du traitement des données ;
- Procédure(s) et formulaire de demande de portabilité des données.

Auxquels s'ajoutent bien évidemment l'implémentation technique si applicable au sein dudit traitement de données personnelles.

Classifier les données personnelles

Cette activité est à mener pour chaque traitement de données personnelles identifié dans le cadre du programme. Elle est dans la pratique conduite sur la base de la liste des traitements classés par ordre de priorité : les traitements les plus prioritaires sont considérés pour l'itération courante du cycle PDCA.

Il s'agit d'organiser et de labéliser les données personnelles en appliquant la taxonomie en place (Cf. section § DEFINIR UNE/REVOIR LA TAXONOMIE DE CLASSIFICATION POUR LES DONNEES PERSONNELLES) afin :

1. D'identifier plus facilement les données personnelles concernées par l'exercice des droits de la personne concernée (Cf. section précédente) ;
2. D'imposer les contrôles de sécurité nécessaires conformément à la politique et d'assurer les traitements appropriés (Cf. section suivante).

Les informations personnelles peuvent en effet être structurées, semi-structurées ou non structurées.

Les bases de données relationnelles sont un exemple typique de données structurées ; de même, les fichiers XML avec schémas XSD spécifiés, les fichiers JSON, etc. sont des exemples courants de données semi-structurées ; les courriels et les fichiers texte sont des exemples courants de données non structurées. Les documents Office et PDF peuvent entrer dans les deux dernières catégories en fonction de leur format de document.

Selon la nature des données qui constituent les éléments d'information personnelle, l'effort requis pour classer les données en tant que données personnelles n'est pas le même en termes d'ampleur. À cet égard, **classifier les données non structurées n'est pas une tâche facile** et pourrait représenter des défis.

Par ailleurs, cette activité peut être l'occasion de revoir si besoin la politique de classification de l'information et les procédures associées.

Les livrables pour la mise en œuvre de cette activité sont les suivants, pour chaque traitement considéré, de façon non-exhaustive :

- Politique de classification de l'information ou sa révision ;
- Procédure(s) de classification de l'information.

Améliorer la sécurité des traitements et des données personnelles

Cette activité est à mener pour chaque traitement de données personnelles identifié dans le cadre du programme. Elle est dans la pratique conduite sur la base de la liste des traitements classés par ordre de priorité : les traitements les plus prioritaires sont considérés pour l'itération courante du cycle PDCA.

Vous avez dit système de management de la sécurité de l'information ?

Le GDPR exige de nombreux contrôles et dispositions en matière de protection de la vie privée. Nombre d'entre eux sont également requis par les normes ISO/IEC 27001:2013[79] et ISO/IEC 27002:2013[80] et d'autres normes du corpus ISO 270xx.

Par voie de conséquence, les organisations ou entreprises qui disposent d'un système de management de la sécurité de l'information (SMSI) au sens ISO 27000 sont susceptibles d'avoir déjà en place beaucoup d'exigences du GDPR. Certains ajustements nécessaires seront cependant susceptibles d'être aménagés.

A l'occasion de la mise en conformité au GDPR des traitements de données personnelles, d'autres organisations ou entreprises peuvent faire le choix d'un SMSI dans un cadre global de façon à gérer les données personnelles comme composante d'une gestion plus large des risques.

En effet, si l'on considère la question de la conformité dans son ensemble et le calendrier associé, l'adoption d'une approche holistique semble s'imposer pour sécuriser l'environnement numérique, aider à construire la confiance et permettre la transformation digitale de l'organisation.

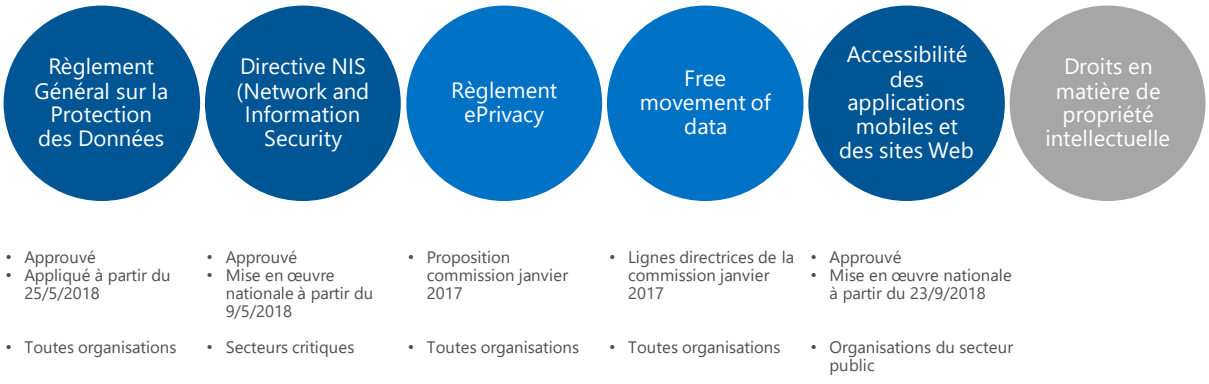


Figure 11 Quelques Règlements, Directives, etc. à prendre en considération aujourd'hui ou à courte échéance

[79] ISO/IEC 27001:2013 TECHNOLOGIES DE L'INFORMATION -- TECHNIQUES DE SECURITE -- SYSTEMES DE MANAGEMENT DE LA SECURITE DE L'INFORMATION -- EXIGENCES : https://www.iso.org/fr/standard/54534.html

[80] ISO/IEC 27002:2013 TECHNOLOGIES DE L'INFORMATION -- TECHNIQUES DE SECURITE -- CODE DE BONNE PRATIQUE POUR LE MANAGEMENT DE LA SECURITE DE L'INFORMATION : https://www.iso.org/fr/standard/54533.html

Une certaine similitude avec la posture dite « Assumer les atteintes à la sécurité »

Les exigences clés du GDPR en matière de sécurité des données personnelles s'articulent autour de deux piliers, au-delà de l'analyse et de l'évaluation des risques :

1. Prévention et protection.
2. Surveillance et détection.

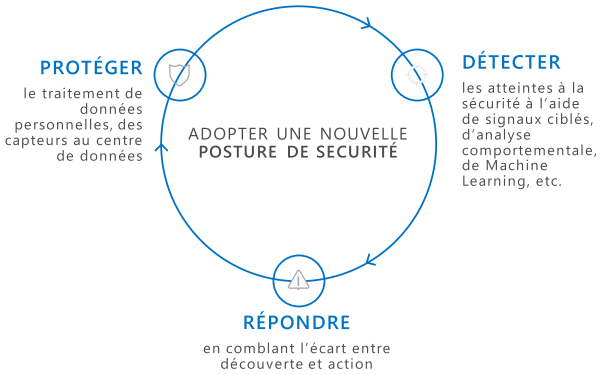


Figure 12 Triptyque de la posture « Assumer les atteintes à la sécurité »

L'adoption d'une posture « Assumer les atteintes à la sécurité » représente un changement majeur qui consiste à **s'autoriser à penser que les défenses numériques seront vulnérables à un moment donné ou à un autre pour un traitement donné**.

Accepter une telle posture ne veut pas dire se soumettre : cela signifie simplement que vous avez pris la première étape vers l'atténuation des risques.

Quel est alors le plan B ? Quel est le plan pour détecter une intrusion en termes de violation de données personnelles ? Comment réagir face à ce type d'incident ?

Cette posture implique de passer d'un simple modèle « **Protéger et Recouvrer** » à une nouvelle stratégie et une posture plus globale comprenant aujourd'hui à minima le triptyque précédent :

1. **Protéger**. Les mesures de sécurité adaptées doivent être prises pour protéger tous les points de terminaison du traitement, des capteurs au(x) centre(s) de données. Il s'agit du registre naturel d'un système de management de la sécurité de l'information (SMSI) tel qu'abordé à la section précédente ;
2. **Détecter**. Il s'agit notamment d'aller vers une approche comportementale où la détection des violations s'effectue sur le comportement (du vecteur d'attaque dans le cas d'une intrusion) en utilisant des signaux ciblés, la surveillance du comportement et l'apprentissage automatique (Machine Learning). Par exemple, la détection à temps d'une attaque en cours peut éviter l'exfiltration des données personnelles et donc une violation au sens du GDPR ;
3. **Répondre**. C'est un domaine qui suppose l'application dynamique de contrôles de sécurité en réponse à la détection pour combler l'écart entre la découverte et l'action en réaction. Cela passe par un changement radical dans la façon de réagir.

Note Le Framework piloté par les risques NIST FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY[81] comprend 5 phases : « Identifier », « Protéger », « Détecter », « Répondre », et « Recouvrer ».

Définir les mesures de sécurité conformément aux politiques

Cette activité consiste à mettre en place les mesures techniques et organisationnelles qui ont été définies comme nécessaires pour assurer la conformité avec le GDPR du traitement de données personnelles.

Les mesures de sécurité techniques et organisationnelles déjà en place sont, s'il y a lieu, renforcées sur la base des résultats de l'étude préalable. De même, les contre-mesures techniques définies lors de l'analyse d'impact relative à la protection des données pour un traitement à risque élevé sont implémentées selon le plan défini d'atténuation des risques.

Ainsi, les contrôles de sécurité en termes de mesure techniques et organisationnelles à mettre en œuvre concernent les données au repos, en cours d'utilisation et en transit, sur la base de la documentation du traitement considéré et ce selon le triptyque Confidentiality Integrity Availability ou CID pour Confidentialité, Intégrité et Disponibilité.

Que dit le GDPR ?

Article 32 - Sécurité du traitement

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les **mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque**, y compris entre autres, selon les besoins :

a) la **pseudonymisation** et le **chiffrement** des données personnelles;
b) des moyens permettant de **garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services** de traitement;
c) des **moyens permettant de rétablir la disponibilité** des données personnelles et **l'accès à celles-ci dans des délais appropriés** en cas d'incident physique ou technique;
d) une procédure visant à **tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles** pour assurer la sécurité du traitement.

Article 34 - Communication à la personne concernée d'une violation de données à caractère personnel

La communication à la personne concernée […] n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie:

a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier **les mesures qui rendent les données personnelles incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement**;

En termes de contrôles, nous avons déjà abordé la pseudonymisation ou désidentification des données. Pour mémoire, la future norme ISO/IEC CD 20889 décrit les techniques de suppression ou de masquage des éléments d'identification des données personnelles de façon à ne pas les rendre accessibles voire à ne plus être soumis aux exigences GDPR.

Il nous apparait par ailleurs important de souligner ici que certains contrôles, en particulier le chiffrement, peuvent impacter les processus à mettre en place. Ainsi, en cas de vol de données personnelles chiffrées, si la clé de chiffrement n'est pas compromise, il n'est pas nécessaire de notifier les personnes concernées.

D'autres peuvent aller « de soi » en termes de pratiques, à l'image de la minimisation des données, Cf. article 5.

[81] NIST FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY:
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

Définir les contrôles de sécurité à mettre en œuvre

Les actifs de l'organisation en termes de données personnelles sont protégés sur la base de leur classification et du plan d'atténuation issu de l'analyse d'impact relatif à la protection des données pour un traitement à « risque élevé ».

En d'autres termes, et en première approche, à moins que les données personnelles ne soient correctement classifiées, celles-ci ne peuvent pas être protégées de façon appropriée. La classification d'un actif de données personnelles impose en effet des contrôles de sécurité minimaux qui doivent être appliqués lors de la manipulation, du stockage, du traitement et/ou du transfert de l'actif considéré (Cf. section § CLASSIFIER LES DONNEES PERSONNELLES).

Dans la pratique, chaque profil de protection (du plan de protection des données) associé à un niveau/label de classification spécifique contient un ensemble de règles qui définissent les exigences minimales en termes de contrôles de sécurité pour la protection de la confidentialité, de l'intégrité et de la disponibilité (triptyque CID) des actifs des données personnelles comme déjà discuté ci-dessus.

Par exemple, en qui concerne la confidentialité, et eu égard aux trois états possibles des données (Cf. section § DEFINIR LES POLITIQUES POUR LA GESTION ET L'UTILISATION DES DONNEES PERSONNELLES) :

- **Données au repos**. Peut être considéré comme « sécurisé » si et seulement si les données sont protégées par un chiffrement fort (où « chiffrement fort » est défini comme chiffrement nécessitant un temps de calcul infaisable pour une attaque en force brute") ET la clé de chiffrement est i) non présente sur le support lui-même, ii) non présente sur le nœud associé au support ; et iii) est suffisamment longue et aléatoire pour être fonctionnellement immunisée contre une attaque au dictionnaire ;
- **Données en traitement**. Peut être considéré comme « sécurisé » si et seulement si i) l'accès à la mémoire est rigoureusement contrôlé (le processus qui a accédé aux données hors du support de stockage et a lu les données dans la mémoire est le seul processus ayant accès à la mémoire et aucun autre processus ne peut accéder aux données en mémoire ou intercepter les données pendant qu'elles traversent par des Entrées/Sorties, et ii) indépendamment de la façon dont le processus se termine (soit par arrêt normal, arrêt forcé, ou arrêt de l'ordinateur), les données ne peuvent être récupérées à partir d'un emplacement autre que l'état d'origine au repos, et en nécessitant une nouvelle autorisation ;
- **Données en transit.** Peut être considéré comme « sécurisé » si et seulement si i) les deux hôtes sont capables de protéger les données dans les deux états précédents et ii) la communication entre les deux hôtes est identifiée, authentifiée, autorisée et privée, ce qui signifie qu'aucun hôte tiers ne peut écouter la communication entre les deux hôtes.

En outre, l'emplacement de données personnelles peut imposer d'appliquer des contrôles de sécurité particuliers.

Par conséquent, pour chaque niveau/label de classification propre à des données personnelles et ensuite pour chaque emplacement permis à cet égard par la politique de sécurité et/ou la politique de protection des données, un profil de protection connexe est potentiellement à élaborer par l'organisation en fonction de ses pratiques.

Selon les profils de protection, les contrôles de sécurité s'appliquant aux actifs d'informations personnelles sont obtenus par déduction. Par exemple, si une application dans le cadre du traitement ciblée traite des données classées comme personnelles et sensibles, la politique de protection associée devrait imposer que les données soient chiffrées au repos, accessibles uniquement pour un groupe restreint de personnes, stockées en interne, et que des modèles correspondants soient inclus dans le système de prévention de fuite de données (Data Loss Prevention en anglais ou DLP) (s'il existe) pour détecter et prévenir toute fuite.

Parallèlement, des solutions techniques déjà déployées ou nouvelles doivent être choisies pour implémenter les contrôles affectés à la protection des actifs d'informations personnelles. Il convient de noter que les contrôles peuvent également correspondre ou se référer à des processus manuels ou automatisés.

Les contrôles de sécurité à considérer dans le cadre du GDPR rentrent dans les sujets suivants de manière non exhaustive :

- Chiffrement – confidentialité des données au repos ;
- Chiffrement – confidentialité des données en transit/en traitement ;
- Gestion de l'identité – authentification des utilisateurs internes ;
- Gestion de l'identité – authentification des utilisateurs externes, notamment dans le cas d'une collaboration de type B2B (Business-to-Business) ;
- Contrôle d'accès (conditionnel) – autorisation(s) et permissions d'accès (contextuelles) ;
- Sécurité des services et des applications ;
- Sécurité réseau ;
- Sécurité du stockage ;
- Protection du centre de données physique ;
- Sauvegarde, archivage, et conservation ;
- Mise au rebus de supports non-électroniques (papier par exemple) ;
- Mise au rebus de supports électroniques (disques durs, clés USB, DVD-ROM, etc.).

Remarque importante La liste ci-dessus recouvre deux notions : protection et contrôle d'accès.

Remarque Le NIST (National Institute of Standards and Technology) fournit un catalogue complet de contrôle de sécurité et de contrôles de protection de la vie privée au travers du document Special Publication 800-53 Rev. 4[82]. L'Institut SANS fournit une liste[83] des contrôles critiques. Il s'agit d'un sous-ensemble du catalogue susmentionné.

[82] NIST SPECIAL PUBLICATION 800-53 REVISION 4 SECURITY AND PRIVACY CONTROLS FOR FEDERAL INFORMATION SYSTEMS AND ORGANIZATIONS: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

[83] CRITICAL CONTROLS FOR EFFECTIVE CYBER DEFENSE: http://www.sans.org/critical-security-controls/

Intégrer une démarche guidée

La définition des mesures de sécurité appropriées conformément aux politiques en place suppose de prendre la mesure de la situation pour le traitement considéré et de discerner les menaces qui pèsent sur celui-ci, les positions de l'attaquant et du défenseur étant par essence asymétriques.

> Si vous vous connaissez bien et si vous connaissez bien votre ennemi, vous ne craindrez pas de mener 100 batailles. Si vous vous connaissez bien mais que vous ne connaissez pas bien votre ennemi, pour chaque victoire vous essuierez une défaite. Si vous ne connaissez bien ni votre ennemi ni vous-même, vous perdrez toutes les batailles.
>
> Sun Tzu, L'art de la guerre

Il est clé de comprendre les menaces qui pèsent sur le traitement de données, les flux de données, le stockage, etc. La modélisation des menaces de la méthodologie Microsoft SDL (Security Development Lifecycle)[84] permet par exemple de comprendre les menaces qui pèsent sur le cycle de vie des données personnelles d'un traitement (et des flux associés) au travers de l'approche STRIDE :

S ⇨ uSurpation d'identité

T ⇨ falsificaTion

R ⇨ Répudiation

I ⇨ divulgation d'Information

D ⇨ Déni de service

E ⇨ Elévation de privilège

Cette approche permet de transformer la modélisation des menaces d'un processus dirigé par un expert à un processus que tout architecte logiciel peut conduire avec pertinence. Afin d'atténuer les menaces, cette approche vise à déterminer les risques pour pouvoir agir sur ceux qui sont inadmissibles via des heuristiques comme critique, important, modéré, faible. Cela suppose ensuite de sélectionner selon STRIDE i) la ou les techniques d'atténuation (ou AUCUNE !) puis ii) la technologie applicable correspondante dans le contexte du traitement, de ses services, applications et/ou dépôt de données.

Il convient ensuite de déterminer les éléments non pris en compte.

> **Remarque** L'outil Microsoft Threat Modeling Tool 2016[85] téléchargeable gratuitement peut être utilisé dans ce contexte.

A l'issue de la mise en œuvre effective des contrôles de sécurité, et quelle que soit l'approche retenue au final pour juger du bienfondé et de la pertinence de la mesure, il convient alors de réévaluer

[84] Microsoft SDL (Security Development Lifecycle) : http://www.microsoft.com/sdl

[85] Microsoft Threat Modeling Tool 2016 : http://www.microsoft.com/en-us/download/details.aspx?id=49168

systématiquement quels sont les risques couverts par le plan d'atténuation ainsi articulé, et quels sont dans ces conditions les risques résiduels.

Le livrable pour la mise en œuvre de cette activité est la traduction effective des mesures techniques et organisationnelles au sein des traitements conformément à l'étude préalable et, le cas échéant au plan d'atténuation des risques issu de l'analyse d'impact relative à la protection des données.

Mettre en place un processus de notification de violation des données personnelles

Cette activité est à mener pour chaque traitement de données personnelles identifié dans le cadre du programme. Elle est dans la pratique conduite sur la base de la liste des traitements classés par ordre de priorité : les traitements les plus prioritaires sont considérés pour l'itération courante du cycle PDCA.

Il s'agit de façon concrète de mettre en œuvre les conditions d'exécution du processus défini de notification d'une violation de données personnelles, Cf. section §

DEFINIR UN MODELE DE PROCESSUS DE NOTIFICATION DE VIOLATION DE DONNEES PERSONNELLES.

Remarque La norme internationale ISO/IEC 27035-1 TECHNOLOGIES DE L'INFORMATION -- TECHNIQUES DE SECURITE -- GESTION DES INCIDENTS DE SECURITE DE L'INFORMATION -- PARTIE 1: PRINCIPES DE LA GESTION DES INCIDENTS[86] (et parties suivantes) pourra être considérée dans ce contexte.

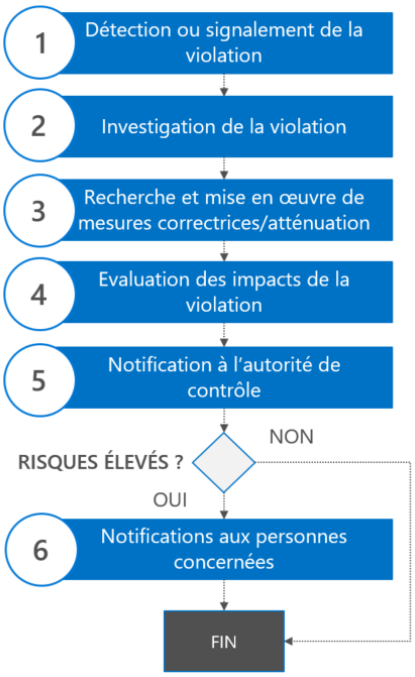


Figure 13 Rappel du « canevas » de processus de notification de violation de données personnelles proposé

La première étape de cette suggestion de « canevas » de processus de notification commence par la détection ou le signalement de la violation de données personnelles.

[86] ISO/IEC 27035-1 TECHNOLOGIES DE L'INFORMATION -- TECHNIQUES DE SECURITE -- GESTION DES INCIDENTS DE SECURITE DE L'INFORMATION -- PARTIE 1: PRINCIPES DE LA GESTION DES INCIDENTS : https://www.iso.org/fr/standard/60803.html

De façon à permettre le signalement d'une violation, le processus et les procédures associées doivent prévoir la disponibilité d'un système interne de signalement, si tel n'est pas déjà le cas, de façon à permettre son utilisation par les collaborateurs de l'organisation. Par exemple, si un collaborateur se fait dérober ou perd un appareil comportant des données personnelles de l'organisation, ce dernier doit être en mesure de pouvoir facilement et rapidement le signaler. Ceci passe également par un plan d'information approprié (Cf. section § AMELIORER LA PRISE DE CONSCIENCE ET LA COLLABORATION EN INTERNE).

La seconde étape correspond à l'investigation de la violation en tant que telle, une fois celle-ci connue. Il s'agit de déterminer sa nature, ses diverses ramifications, etc. C'est probablement l'étape la plus longue et la plus complexe pour laquelle il est nécessaire de s'appuyer sur une équipe interne de spécialistes (en fonction de la nature de la violation) ou de faire appel à un cabinet extérieur. Cette équipe doit pouvoir être activée en urgence en cas de crise. Le processus doit donc à la fois permettre d'identifier ces personnes et préciser les modalités de leur mobilisation.

Une fois le scénario ayant conduit à la violation de données clairement identifié et compris, la troisième étape s'intéresse naturellement à la recherche et à la mise en œuvre de mesures correctrices ou d'atténuation. Par exemple :

- Si un problème d'intégrité est identifié sur une base de données, la mesure corrective peut être l'application d'une sauvegarde, sachant que les toutes dernières modifications intervenues seront alors potentiellement perdues ;
- Si c'est une faille de sécurité utilisée par un attaquant pour extraire des données personnelles, les correctifs de sécurité nécessaires devront être appliqués.

La quatrième étape s'intéresse à l'évaluation des impacts de la violation vis-à-vis du type et de la sensibilité des données personnelles concernées, du nombre de personnes concernées et des effets induits.

A ce stade, les éléments nécessaires sont disponibles dans le cadre de la cinquième étape pour monter le dossier de notification et en informer l'autorité de contrôle.

Par ailleurs, en conformité avec l'article 34[87] , la gravité de l'impact de la violation de données doit être déterminée et, en fonction du résultat, cette violation doit être notifiée aux personnes directement concernées. C'est l'objet de la sixième et dernière étape.

Les livrables pour la mise en œuvre de cette activité sont les suivants de façon non-exhaustive pour chaque traitement considéré :

- Processus/Procédure de gestion des incidents de sécurité ;
- Processus de notification de violation des données personnelles ;
- Procédures de notification de violation associées.

Améliorer la prise de conscience et la collaboration en interne

Cette activité vise à développer les plans de sensibilisation et de formation en interne afin que toutes les parties prenantes dans cet effort de mise en conformité « dynamique » au GDPR puissent s'approprier à des degrés divers de leurs niveaux d'implication et de responsabilité les principes et concepts du GDPR, les processus, procédures, l'outillage et les modèles les concernant.

Au travers de la définition de ces plans, Il s'agit donc de :

[87] ARTICLE 34 - COMMUNICATION A LA PERSONNE CONCERNEE D'UNE VIOLATION DE DONNEES A CARACTERE PERSONNEL : https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article34

- Sensibiliser les collaborateurs aux enjeux de la protection de la vie privée ;
- Favoriser les remontées d'information dans l'identification et la cartographie des traitements de données personnelles ;
- Former au moins annuellement les personnels concernés sur les standards de sécurité « au jour le jour » de l'entreprise qui régissent comment les données personnelles sont gérées, accédées, transférées et supprimées.

Les livrables pour la mise en œuvre de cette activité sont les différents plans sensibilisation et de formation en interne, les contenus associés, et leur programmation et déroulé auprès des populations internes cibles de l'organisation.

Vérifier le programme GDPR

La phase **VERIFIER** du cycle PDCA est constituée d'un ensemble d'activités :

- Suivre les traitements de données à risque élevé ;
- Vérifier la (trajectoire de mise en) conformité au GDPR ;
- Maintenir la documentation requise pour la mise en conformité GDPR.

Ces activités sont décrites de façon unitaire dans les sections suivantes.

Suivre les traitements de données à risque élevé

Cette activité constitue un impératif pour tous les traitements de données ayant fait l'objet d'une analyse d'impact relative à la protection des données, Cf. section § GERER LES RISQUES POUR LES TRAITEMENTS DE DONNEES PERSONNELLES A RISQUE ELEVE.

Il s'agit d'un contrôle itératif nécessaire pour s'assurer de l'exactitude du Registre des traitements. Toute modification du traitement ou des données collectées et traitées doit provoquer un réexamen.

Pour les autres traitements, c'est-à-dire ceux n'ayant pas fait l'objet d'une analyse d'impact relative à la protection des données (Cf. section § PROCEDER A UNE ETUDE PREALABLE DU NIVEAU DE RISQUE DES TRAITEMENTS DE DONNEES PERSONNELLES), toute modification notoire du traitement ou des données collectées et traitées doit être examinée pour vérifier si une analyse d'impact est nécessaire.

Le Registre des traitements doit pouvoir être mis à disposition de l'autorité de contrôle à tout moment y compris durant une procédure d'audit.

> Que dit le GDPR ?
>
> **Article 30 - Registre des activités de traitement**
> 4. Le responsable du traitement ou le sous-traitant et, le cas échéant, leur représentant mettent **le registre à la disposition de l'autorité de contrôle sur demande**.
>
> **Article 58 - Pouvoirs**
> Chaque autorité de contrôle dispose de tous les pouvoirs d'enquête suivants:
> b) mener des **enquêtes sous la forme d'audits** sur la protection des données;

Vérifier la (trajectoire de mise en) conformité au GDPR

Cette activité est à mener pour chaque traitement de données personnelles identifié dans le cadre du programme. Elle est dans la pratique conduite sur la base de la liste des traitements classés par ordre de priorité : les traitements les plus prioritaires sont considérés pour l'itération courante du cycle PDCA.

Cette activité comporte un ensemble de sous-activités :

- Vérifier la pertinence de la cartographie des traitements ;
- Vérifier la prise en charge des nouveaux droits ;
- Vérifier l'efficacité des mesures de sécurité techniques et organisationnelles en place ;
- Vérifier le niveau opérationnel du processus de notification de violation des données personnelles.

Celles-ci sont décrites dans les sections suivantes.

Vérifier la pertinence de la cartographie des traitements

Cette activité consiste à procéder à des audits internes de données réguliers pour identifier :

- Quelles données personnelles sont effectivement détenues par l'organisation ;
- Comment ces données personnelles sont effectivement utilisées et, le cas échéant transférées ;
- L'antériorité de ces données ;
- Qui accède à ces données.

Elle est réalisée sur la base des traitements recensés et présents dans le Registre des traitements et au-delà pour les « Dark Data » (par exemple « Shadow IT »). Les éventuels « nouveaux » traitements découverts sont à intégrer dans le programme GDPR, ce qui suppose d'actualiser en conséquence le Registre des traitements.

En fonction des écarts constatés, il s'agit de convenir d'un délai pour adresser les principaux risques en matière de protection des données personnelles. Il convient pour cela de procéder à une analyse de risque sur la base des écarts constatés. L'étude préalable pourra servir de modèle, Cf. section § PROCEDER A UNE ETUDE PREALABLE DU NIVEAU DE RISQUE DES TRAITEMENTS DE DONNEES PERSONNELLES.

Les actions correctrices seront vérifiées lors d'une prochaine itération du cycle PDCA, en fonction du délai de résolution accordé.

Vérifier la prise en charge des nouveaux droits

Cette activité consiste à s'assurer que les réclamations et les demandes des personnes concernées quant à l'exercice de leurs nouveaux droits sont (bien) effectives. En d'autres termes, il convient de vérifier que les droits en question sont exerçables par les personnes concernées.

> ### Que dit le GDPR ?
>
> **Section 2 - Information et accès aux données à caractère personnel**
> Article 15 - **Droit d'accès** de la personne concernée
> Section 3 - Rectification et effacement
> Article 16 - **Droit de rectification**
> Article 17 - **Droit à l'effacement** («droit à l'oubli»)
> Article 18 - **Droit à la limitation du traitement**
> Article 19 - Obligation de notification en ce qui concerne la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement
> Article 20 - **Droit à la portabilité** des données
>
> **Section 4 - Droit d'opposition et prise de décision individuelle automatisée**
> Article 21 - **Droit d'opposition**
> Article 22 - Décision individuelle automatisée, y compris le profilage

Cela implique de vérifier que :

- Les procédures et les formulaires de demande de droits sont bien accessibles par les utilisateurs ;
- Tous les processus de demande sont opérationnels, à savoir :
  - Toutes les requêtes sont prises en compte et traitées dans des délais raisonnables ;
  - Les droits sont effectivement appliqués (rectification, effacement, etc.).

Remarque importante	Les processus peuvent être manuels ou informatisés.

Vérifier l'efficacité des mesures de sécurité techniques et organisationnelles en place

Cette activité consiste à vérifier l'efficacité des mesures de sécurité techniques et organisationnelles en place conformément à l'article 32[88] concernant la sécurité du traitement et des données personnelles.

> ### Que dit le GDPR ?
>
> **Article 32 - Sécurité du traitement**
> Le responsable du traitement et le sous-traitant mettent en œuvre les **mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque**, y compris entre autres, selon les besoins :
>
> […]
>
> d) une procédure visant à **tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles** pour assurer la sécurité du traitement.

Ces vérifications concernent aussi bien le responsable de traitement que les sous-traitants.

Vérifier le niveau opérationnel du processus de notification de violation des données personnelles

Cette activité consiste à évaluer le processus de notification en place et sa réponse.

Afin de vérifier que le processus de notification implémenté dans la phase **MISE EN ŒUVRE** est opérationnel (Cf. section § METTRE EN PLACE UN PROCESSUS DE NOTIFICATION DE VIOLATION DES DONNEES PERSONNELLES), un exercice de simulation doit être planifié pour s'assurer que toutes les parties prenantes peuvent être convoquées dans un délai court pour respecter les 72 heures et, en cas de dépassement de ce délai, d'être en mesure de le motiver.

> ### Que dit le GDPR ?
>
> **Article 33 - Notification à l'autorité de contrôle d'une violation de données personnelles**
> En cas de violation de données à caractère personnel, le responsable du traitement en **notifie la violation en question à l'autorité de contrôle** […] **dans les meilleurs délais et, si possible, 72 heures** au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard.
>
> **Article 34 - Communication à la personne concernée d'une violation de données personnelles**
> Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement **communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais**.

Comme indiqué précédemment, Le Délégué à la Protection des Données est la « pièce maîtresse » du processus et est en charge de la notification auprès de l'autorité de contrôle.

---

[88] ARTICLE 32 - SECURITE DU TRAITEMENT : https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article32

Maintenir la documentation requise pour la mise en conformité GDPR

Cette activité consiste à gérer les différents volets du « corpus documentaire » attendu afin de **démontrer la conformité** aux objectifs et exigences du GDPR.

Compte tenu des éléments développés précédemment dans ce livre blanc, ces volets sont à minima au nombre de quatre :

1. **Traitements des données personnelles**. La traduction principale de ce volet est constituée par le Registre des traitements, qui consigne, pour chaque traitement de données personnelles de l'organisation, la fiche de traitement, le cycle de vie des données personnelles et la cartographie des flux associés dûment renseignés et à jour.

   Sont précisés et consignés, le cas échéant et si applicables :

   - Le rapport d'analyse d'impact pour les analyses d'impact relatives à la protection des données qui ont été conduit ;
   - L'encadrement des transferts de données personnelles hors de l'Union Européenne, par exemple par le biais des Clauses contractuelles types.

2. **Sous-traitants**. La traduction principale de ce volet est constituée par le Registre (des risques) des sous-traitants qui consigne les contrats avec les sous-traitants.

   Doivent également être répertoriées les preuves des consentements données par les personnes concernées si la collecte a été réalisée à ce niveau.

3. **Information et droits des personnes concernées**. Ce volet est constitué des éléments suivants :

   - Les procédures/processus mises en œuvre pour l'exercice des nouveaux droits des personnes concernées comme développés précédemment ;
   - Les mentions d'information (pour les traitements) conformes aux exigences du Règlement ;
   - Les formulaires « type » (demande d'accès, correction, etc.) ;
   - Les preuves des consentements donnés par les personnes concernées.

4. **Procédures/processus internes en cas de violation de données personnelles**. Ce volet comprend la procédure et le formulaire de notification de violation (ou le téléservice correspondant et ses modalités d'invocation).

La tenue de ces volets suppose, au-delà de ce qui a été précédemment souligné en termes d'outillage, de disposer de capacités permettant de faire en sorte que tout traitement de données personnelles soit suivi et enregistré dans des documents ou journaux, que ce soit au niveau de la collecte, de l'utilisation, du transfert de données, etc.

Ceci implique notamment de mettre en œuvre des capacités de rapports :

- Journaux d'audit ;
- Notifications ;
- Consentement(s) des personnes concernées ;
- Exercice(s) des nouveaux droits pour les personnes concernées ;
- Rapport sur la gouvernance ;
- Revues de conformité.

Ajuster le programme GDPR

La phase **AJUSTER** du cycle PDCA est le « moteur » de l'amélioration en continu. Cette dernière conditionne le contexte d'exécution des itérations suivantes du cycle.

Elle comprend en particulier une activité permettant de tendre progressivement vers les principes recherchés de « protection des données dès la conception » et de « protection des données par défaut ».

Initier un processus de rationalisation pour les traitements de données personnelles

Cette activité vise à valider une trajectoire pour faciliter la prise en compte des nouveaux droits donnés à la personne concernée (sujet des données).

L'une des traductions passe par la gestion et la consolidation des dépôts de données personnels. Par exemple, une architecture centralisant les données personnelles est de nature à faciliter l'implémentation de la collecte des données, la demande et l'enregistrement d'un consentement explicite et la mise en œuvre des droits des personnes concernées.

Une telle démarche se traduit par la recherche d'une disparition programmée et progressive des différents dépôts de données personnelles existants au profit – chaque fois que possible - de ce référentiel unique.

Cela induit de fait une migration pour les applications des traitements concernés vers l'utilisation de ce dépôt référentiel. Cet effort s'inscrit dans une suppression des différents silos applicatifs historiques (legacy) de l'organisation au profit d'une plus grande agilité.

Un rapide regard sur les recommandations de la CNIL

La CNIL a mis à disposition un petit guide en 6 étapes qui décrit succinctement quelques principes de mise en œuvre[89] [90].

Figure 14 Etapes du processus de mise en conformité proposé par la CNIL

La tentative d'approche structurée multicycle que nous avons essayée de proposer et d'articuler dans les pages précédentes de ce livre blanc trouve au travers des diverses phases du cycle PDCA et activités associées une correspondance assez naturelle avec ces 6 étapes du processus précédent, comme en témoigne les figures suivantes.

[89] SE PREPARER AU REGLEMENT EUROPEEN : http://www.cnil.fr/se-preparer-au-reglement-europeen

[90] REGLEMENT EUROPEEN : SE PREPARER EN 6 ETAPES : https://www.cnil.fr/sites/default/files/atoms/files/pdf_6_etapes_interactifv2.pdf

Figure 15 Correspondance des phases et activités du programme avec les étapes 1 à 3 du processus de mise en conformité proposé par la CNIL

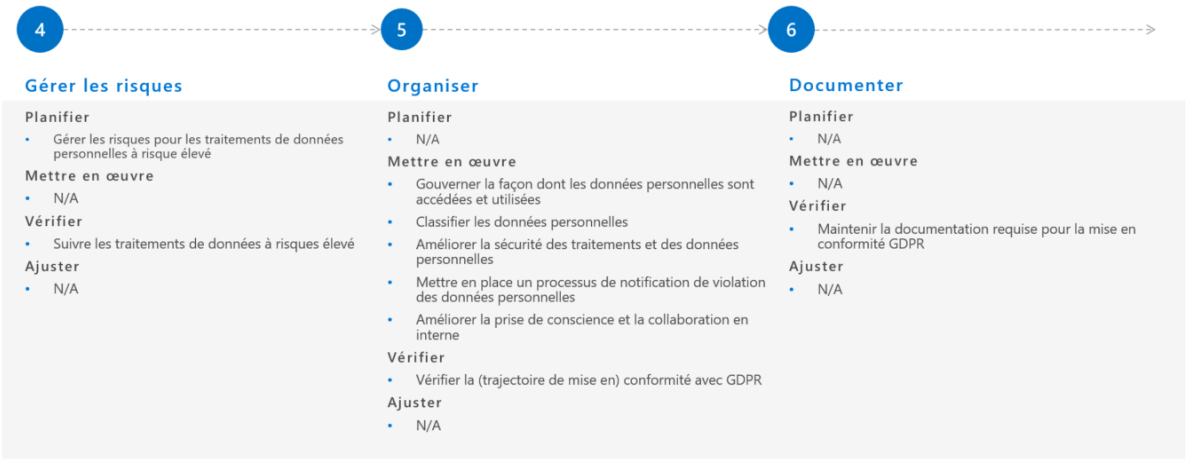


Figure 16 Correspondance des phases et activités du programme avec les étapes 4 à 6 du processus de mise en conformité proposé par la CNIL

Quelques recommandations pour conclure

Pour conclure, nous souhaitons citer le poète Bertolt Brecht :

> C'est parce que les choses sont ce qu'elles sont que les choses ne resteront pas ce qu'elles sont
>
> Berthold Brecht

Bertolt Brecht nous propose un bel aphorisme sur l'évolution, et son moteur.

A un moment où le Cloud est en train de « re-câbler » le monde et permet la redéfinition des usages et des modèles d'affaires des entreprises en pleine transformation digitale, le nouveau Règlement européen GDPR - au-delà de ses nombreuses exigences et larges implications pour les organisations qui utilisent des (traitements de) données personnelles - est aussi l'opportunité pour ces mêmes organisations de construire une nouvelle fondation – si ce virage n'a pas d'ores et déjà été pris - en matière de protection de la vie privée et de sécurité, une fondation qui soit holistique, innovante et durable.

Comme indiqué en introduction de ce livre blanc, Microsoft se tient à vos côtés pour vous aider dans votre voyage vers la conformité GDPR :

- Les services de cloud de Microsoft, tels que Microsoft Azure[91], Microsoft Dynamics 365[92] et Microsoft Office 365[93] vous permettent de faciliter les processus que vous devez implémenter pour assurer la conformité GDPR grâce à la technologie intelligente (smart), l'innovation et la collaboration.

Remarque Microsoft Azure est une collection croissante de services de cloud intégrés de type IaaS et PaaS - calcul, stockage, réseau, base de données, avancée analytique, mobile, web, API, etc - qui permettent à nos clients d'aller plus vite, de réaliser plus et de faire des économies pour la mise en œuvre de leurs (activités de) traitements. Azure sert à la fois d'environnement de développement (dans le cas de pratique DevOps notamment), de service d'hébergement et d'environnement d'exécution et de gestion de services pour héberger, mettre à l'échelle et gérer des applications et traitements sur Internet.

Remarque Microsoft Dynamics 365 est la prochaine génération d'applications d'entreprise intelligentes qui permet aux organisations de toute taille de se développer, d'évoluer et de se transformer pour répondre aux besoins de leurs clients quels qu'ils soient et de saisir de nouvelles opportunités. Il combine nos services de cloud actuels en matière de progiciel de gestion de la relation client (Customer Relationship Management en anglais ou CRM) et de planification des ressources d'entreprise (Enterprise Resources Planning en anglais ou ERP) en un seul service et comprend de nouvelles applications spécifiques pour aider à gérer les fonctions spécifiques d'une organisation (marketing, connaissances des clients, ventes, finances, services à la clientèle, opérations, automation des services projet, etc.).

[91] Microsoft Azure : https://azure.microsoft.com

[92] Microsoft Dynamics 365 : http://www.microsoft.com/fr-fr/dynamics365/

[93] Microsoft Office 365 : https://products.office.com

Remarque Microsoft Office 365 est conçu pour répondre aux besoins des organisations en termes de productivité utilisateur, de fiabilité, et de sécurité élevée. Office 365 intègre la suite bureautique familière Microsoft Office avec les versions basées sur le Cloud des services de collaboration et de communication de nouvelle génération de Microsoft - exploitant l'Internet pour aider les utilisateurs à être plus productifs de pratiquement n'importe où depuis n'importe quel appareil.

- Grâce à nos solutions en local et à nos services de cloud, Microsoft vous aide à localiser et cataloguer les données personnelles de vos traitements dans vos systèmes, à construire un environnement (hybride) plus sécurisé et à simplifier la gestion et le suivi des données personnelles.
- Pour aider les organisations à répondre à leurs exigences GDPR, Microsoft investit dans des fonctionnalités et des capacités supplémentaires.
- Enfin, nous partageons les bonnes pratiques de nos propres experts sur la protection de la vie privée.

Comme pour beaucoup de normes, de standards et de règlements, la conformité avec le GDPR n'est pas un état ponctuel, mais plutôt un processus continu. C'est par exemple une différence majeure qui peut être faite à la référence au passage à l'an 2000, référence souvent prise en termes d'analogie pour illustrer l'ampleur de la tâche.

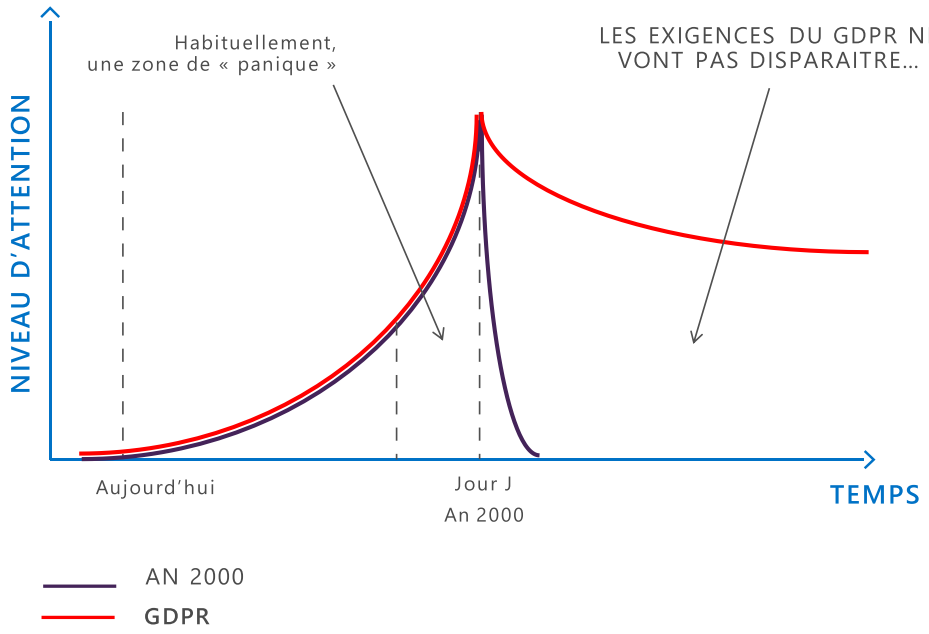


Figure 17 Jour J An 2000 vs. GDPR

GDPR et l'an 2000 sont effectivement comparables mais pas identiques.

Pour reprendre les quatre grandes catégories d'activités mises en exergue par l'approche multicycle développée dans ce livre blanc, à savoir PLANIFIER, METTRE, VERIFIER et AJOUTER, on peut voir deux phases :

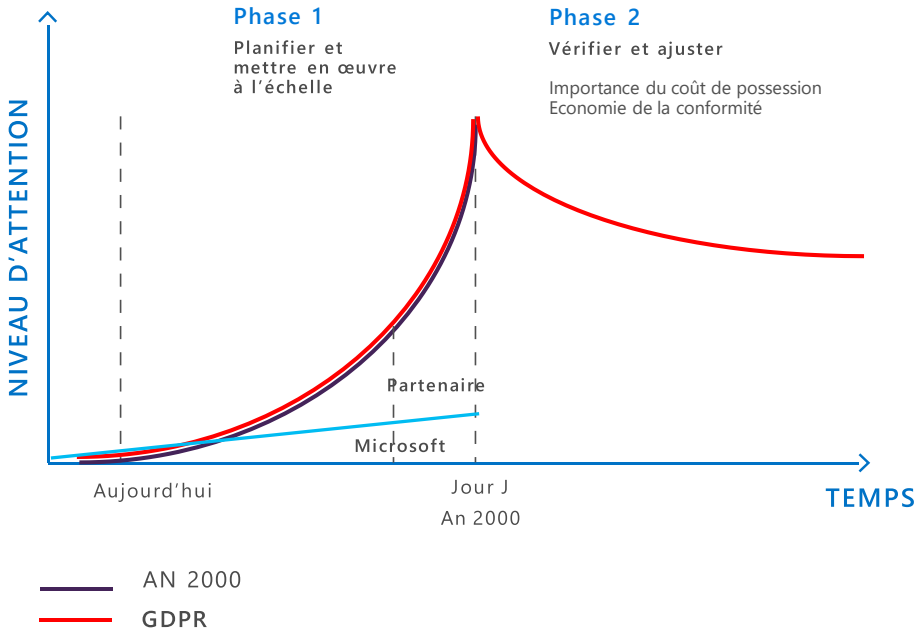


Figure 18 Phases du cycle encadrant le Jour J de GDPR

En avançant avec un fournisseur de services de cloud « hyper-scale » comme Microsoft et en utilisant des services de cloud comme Azure, Dynamics 365 et Office 365, vous pouvez bénéficier de « l'économie de la conformité ». Les services de cloud de Microsoft vous permettent de réduire les efforts de programmation et les fardeaux administratifs requis pour devenir conforme au GDPR.

Remarque Pour de plus amples informations, nous vous invitons à lire le billet de blog ACCELERATE YOUR GDPR COMPLIANCE WITH THE MICROSOFT CLOUD[94] de Julia White, notre Vice-Présidente Entreprise, Plateforme Cloud.

Dans le cadre de « l'économie de la conformité », le gestionnaire de la conformité (Compliance Manager) de Microsoft annoncé est destiné à vous aider à gérer votre posture de conformité depuis un seul et même emplacement pour tous les services de cloud de Microsoft avec les capacités suivantes :

- **Évaluation des risques en temps réel**. Un score intelligent reflète vos performances en matière de conformité vis-à-vis d'un ensemble de règlements, normes et standards sur la protection des données (par exemple, GDPR, ISO, NIST).
- **Suggestions actionnables**. Des actions recommandées sont proposées afin d'améliorer vos capacités de protection des données.
- **Conformité simplifiée**. Vous pouvez améliorer et surveiller votre posture de conformité avec la gestion des contrôles intégrés et des outils de reporting.

Compliance Manager est une solution interservices de cloud Microsoft conçue pour aider les organisations à respecter des obligations de conformité complexes telles que le GDPR. Celle-ci effectue une évaluation des risques en temps réel qui reflète votre posture de conformité vis-à-vis d'un ensemble

[94] ACCELERATE YOUR GDPR COMPLIANCE WITH THE MICROSOFT CLOUD : https://blogs.microsoft.com/blog/2017/05/24/accelerate-gdpr-compliance-microsoft-cloud/

de règlements, normes et standards sur la protection des données lors de l'utilisation des services de cloud Microsoft, ainsi que des actions recommandées et des conseils étape par étape.

Compliance Manager contient un tableau de bord qui fournit un résumé de votre posture courante quant à la conformité et la protection des données et propose des recommandations visant à améliorer la conformité et la protection des données. Il s'agit de recommandations ; c'est à vous d'évaluer leur efficacité au sein de votre environnement avant mise en œuvre.

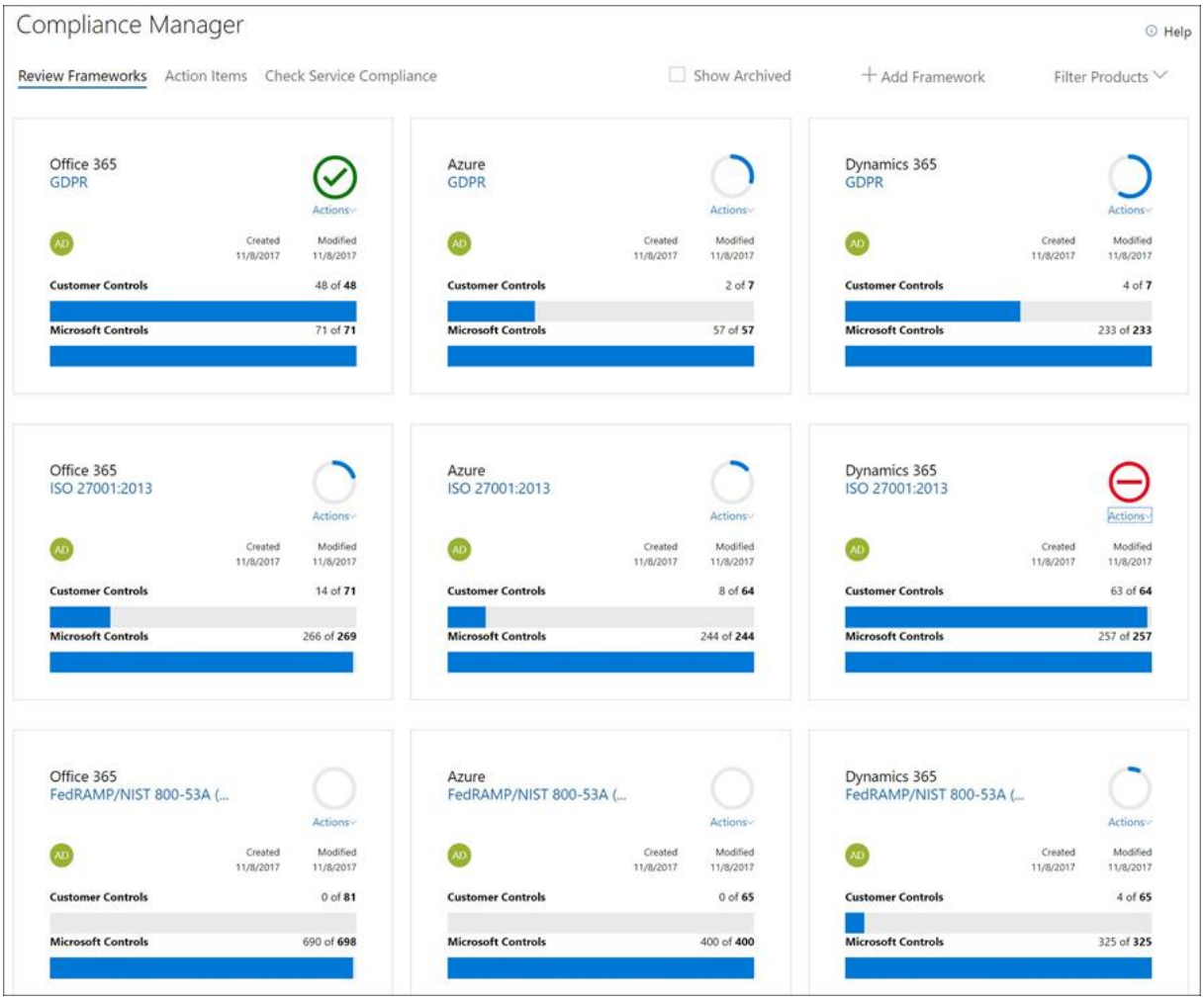


Figure 19 Exemple d'un tableau de bord de Compliance Manager

Remarque importante Les recommandations du gestionnaire de la conformité (Compliance Manager) ne doivent pas être interprétées comme un conseil juridique ou une garantie de conformité.

Remarque Pour plus d'informations, vous pouvez consulter le blog dédié[95].

[95] MANAGE YOUR COMPLIANCE FROM ONE PLACE – ANNOUNCING COMPLIANCE MANAGER PREVIEW PROGRAM: https://techcommunity.microsoft.com/t5/Security-Privacy-and-Compliance/Manage-Your-Compliance-from-One-Place-Announcing-Compliance/ba-p/106493

Remarque importante Vous pouvez vous inscrire au programme de version préliminaire qui a débuté en novembre 2017 à l'adresse https://aka.ms/compliancemanager.

Références

Liens utiles sur le Centre de confiance Microsoft

- A propos des services et produits Microsoft sur microsoft.com/GDPR :
  - Microsoft Azure,
  - Microsoft Dynamics 365,
  - Microsoft Enterprise Mobility + Security (EM+S),
  - Microsoft Office et Office 365,
  - Microsoft SQL Server et Azure SQL Database (base de données en tant que service),
  - Windows 10 et Windows Server 2016.
- Et en termes d'ebooks et de livres blancs :
  - An Overview of the General Data Protection Regulation[96],
  - Accelerate your GDPR compliance with the Microsoft Cloud[97],
  - Beginning your General Data Protection Regulation (GDPR) journey[98],
  - Discover how to start your journey toward GDPR compliance while using Microsoft Dynamics 365 applications[99],
  - How Microsoft Azure Can Help Organizations Become Compliant with the GDPR[100],
  - Supporting Your EU GDPR Compliance Journey With Enterprise Mobility + Security[101],
  - Accelerate your GDPR compliance journey with Microsoft 365[102],
  - Guide to enhancing privacy and addressing GDPR requirements with the Microsoft SQL Platform[103],
  - Accelerate GDPR with Windows 10[104].

[96] An Overview of the General Data Protection Regulation: https://aka.ms/GDPROverview

[97] Accelerate your GDPR compliance with the Microsoft Cloud: https://aka.ms/gdprebook

[98] Beginning your General Data Protection Regulation (GDPR) journey: https://aka.ms/gdprwhitepaper

[99] Discover how to start your journey toward GDPR compliance while using Microsoft Dynamics 365 applications: https://info.microsoft.com/GDPRAssessmentResponses-Registration.html

[100] An Overview of the General Data Protection Regulation: https://aka.ms/GDPROverview:

[101] Supporting your EU GDPR compliance journey with Microsoft EMS: https://aka.ms/emsgdprwhitepaper

[102] Accelerate your GDPR compliance journey with Microsoft 365: https://resources.office.com/ww-landing-M365EGDPR-accelerate-your-GDPR-compliance-whitepaper.html?LCID=EN-US

[103] Guide to enhancing privacy and addressing EU GDPR requirements with the Microsoft SQL platform: http://aka.ms/gdprsqlwhitepaper

[104] Accelerate GDPR with Windows 10: https://aka.ms/WindowsGDPRwhitepaper

Microsoft France
39 Quai du Président Roosevelt
92130 Issy-Les-Moulineaux