DONNÉES PERSONNELLES
ET SYSTÈMES D'INFORMATION

ENTREPRISES
LES CLÉS D'UNE APPLICATION RÉUSSIE DU GDPR

afai
Pour des systèmes d'information de confiance et créateurs de valeur

cigref
réussir le numérique

TECH'IN
FRANCE

LE MOT DES PRÉSIDENTS

Dans le contexte actuel de transformation numérique, l'information et son usage font l'objet de toutes les attentions, entre valorisation et protection.

Pour l'entreprise, **la donnée est devenue un nouvel actif stratégique majeur**, elle doit être exploitée et protégée, d'autant plus s'il s'agit d'une donnée sensible.

L'individu quant à lui, est grand consommateur d'information, producteur également, mais il est soucieux de protéger sa vie privée contre une utilisation abusive de ses données personnelles, et demandeur de garanties.

La confiance dans le numérique et dans l'usage de l'information est impérative, et partout dans le monde, les régulateurs veillent et encadrent à juste titre le traitement des données personnelles. Au sein de l'Union européenne, **la réglementation GDPR[1] s'appliquera dès le 25 mai 2018, et les entreprises se sont déjà largement mobilisées pour se mettre en conformité**.

En parallèle, on parle d'entreprise étendue, avec des organisations et des systèmes d'information de plus en plus globalisés et largement ouverts aux clients et partenaires, et avec des services désormais tous proposés dans le Cloud. On parle aussi d'entreprise « data-driven » (« orientée données »), avec des besoins de Big Data, corrélation et analyse des données massives captées par les objets connectés.

Le déploiement de ces solutions répond d'abord et avant tout à des besoins d'accès et de partage de l'information, à des fins d'optimisation de l'efficacité opérationnelle et de développement du business. **Toutes les entreprises sont concernées, pour leur cœur de métier comme pour les services génériques** de messagerie, de SIRH, de CRM, etc. qui tous, traitent des données personnelles.

Ces deux exigences **d'efficacité opérationnelle et de conformité avec les règles de protection de la vie privée** peuvent, de prime abord, paraître antinomiques et difficiles à concilier pour les entreprises et leurs fournisseurs partenaires… d'autant plus lorsque différentes réglementations s'imposent, pour des groupes globaux notamment.

Le système d'information porte l'activité de l'entreprise. Il est aussi l'élément central de la mise en conformité avec le GDPR et les autres réglementations. **La conformité au GDPR est un projet d'entreprise, qui engage tous les métiers**, et qui doit mesurer l'impact sur les différentes briques du SI, dont certaines sont en place depuis des années, voire même sur son architecture.

Nos trois organisations professionnelles se sont mobilisées tôt, dès l'été 2016, avec le soutien de quatre cabinets d'avocats : August Debouzy, De Gaulle Fleurance & Associés, Osborne Clarke et SAMMAN et la participation régulière de la CNIL.

---

[1] Règlement Général sur la protection des Données à caractère Personnel (ou General Data Protection Regulation)

Conscientes des enjeux, elles se sont rassemblées pour lancer une initiative conjointe en France, **« Données Personnelles et Système d'Information (DPSI) »**, avec deux objectifs :

- Sensibiliser les entreprises, utilisatrices et fournisseurs, sur l'urgence et l'ampleur de ce projet de mise en conformité avec le GDPR ;

- Produire un guide de recommandations pratiques et applicables pour se mettre en conformité avec le GDPR, et ainsi apporter une aide opérationnelle concrète à tous ceux qui ont engagé ou engagent leur projet.

Le résultat est là, et nous tenons à remercier vivement toutes les entreprises, la CNIL, les cabinets d'avocats, et l'ensemble des personnes qui ont contribué à donner à cette initiative de place toute sa force.

Pascal Antonini

Président de l'AFAI

Bernard Duverneuil

Président du CIGREF

Bertrand Diard

Président de
TECH IN France

EXECUTIVE SUMMARY

Résultat de l'initiative « Données Personnelles et Systèmes d'Information » (DPSI), ce livrable offre à toutes les entreprises les outils indispensables à une mise en conformité réussie avec le GDPR. Grâce à sa structure logique et pratique, chaque entreprise pourra entamer ou poursuivre les étapes clés du changement de manière efficace et sereine.

Rédigé dans un langage accessible à tous et illustré de nombreux exemples significatifs, le document décrypte les nouvelles obligations du Règlement, analyse leurs impacts sur les systèmes d'information, et émet des recommandations concrètes, techniques et juridiques, applicables opérationnellement par les fournisseurs de services de logiciels et par les entreprises utilisatrices.

Le document s'articule autour de trois parties distinctes et complémentaires.

Le chapitre 1, écrit sous la présidence de l'AFAI accompagnée par le cabinet d'avocats August Debouzy, fournit un guide d'auto-évaluation sous la forme d'une check-list complète pour vérifier si son entreprise est en conformité avec le GDPR. En répondant aux cinquante questions proposées, vous pourrez évaluer votre niveau de conformité et identifier les domaines dans lesquels un processus d'amélioration est à conduire.

Les questions concernent trois grandes thématiques :

- **Gouvernance** : **16 questions** sur le DPO, le périmètre d'application, les politiques et procédures, les prérequis et travaux préparatoires, les formations et informations ;
- **Métiers** : **18 questions** sur la licéité du traitement, les types de traitements mis en place, les catégories de données collectées, les droits des personnes, les obligations dans les relations entre responsable de traitement et sous-traitant, les transferts de données en dehors de l'UE, la sécurité des données personnelles, l'étude d'impact sur la vie privée ;
- **Système d'information et cybersécurité** : **16 questions** sur les catégories des données collectées, la sécurité des données personnelles, le privacy by design, la transparence, les dispositifs de détection et de notifications des failles, les clauses contractuelles obligatoires, la gestion de l'exercice des droits des personnes.

Le chapitre 2, écrit sous la présidence du CIGREF accompagné par le cabinet d'avocat De Gaulle Fleurance & Associés, liste les recommandations et les mesures à mettre en œuvre pour assurer la conformité du système d'information (SI) avec le GDPR. La démarche du sous-groupe 2 (SG2) est la suivante :

1) identification des composants du SI qui génèrent ou véhiculent des données personnelles ;
2) pour chaque composants du SI : inventaire des risques afférents selon les 3 grandes catégories suivantes :
    a. sécurité du SI : intrusion du SI par un malware, usurpation d'un compte utilisateur, défaut d'application des mises à jour de sécurité, etc.
    b. protection des données personnelles : défaut de cartographie actualisée des données personnelles et des traitements, divulgation malveillante de données personnelles, chiffrement, anonymisation/pseudonymisation, etc.

c. protection des droits des personnes : non disponibilité ; défaut d'intégrité ; perte de confidentialité ; absence de traçabilité ; usages illicites ; répudiabilité.

3) identification des mesures et recommandations potentiellement applicables en fonction de chaque typologie de risques.

Les mesures identifiées par le SG2 visent à protéger les composants et applicatifs, mais aussi tous les flux qui existent entre eux. Pour chaque risque identifié, le document donne une série de recommandations claires, pratiques et pertinentes afin de minimiser, voire de prévenir ce risque.

Ainsi, pour un risque - par exemple *« transfert non sécurisé de données personnelles »* - le chapitre 2 indique les composants du SI potentiellement exposés à ce risque (Cloud, applications, base de données, datawarehouse, Big Data, GED – Archivages, fichiers partagés, messagerie, données de sortie) ; et émet ensuite une série de recommandations à mettre en œuvre afin de gérer ce risque : intégrer les contraintes dès la phase de design (privacy by design), développer une politique sur les droits et devoirs en matière de sortie des données ; chiffrement et anonymisation ; encadrement contractuel avec le partenaire (NDA, clause de confidentialité, clause de suppression des données…) ; etc.

Enfin, ce chapitre illustre concrètement la mise en œuvre de la démarche par un cas pratique : l'activité d'un logiciel de « gestion de la relation client » ou CRM.

Le chapitre 3, écrit sous la présidence de TECH IN France accompagné par deux cabinets d'avocats SAMMAN et Osborne Clarke, fournit les outils juridiques indispensables à une application réussie du GDPR. Elaboré après échanges avec la CNIL, ce chapitre s'articule en trois grands volets :

- la gestion interne par les outils de gouvernance visant à l'autoresponsabilité des entreprises (ou « accountability ») ;
- la démonstration de cette responsabilité vis-à-vis du public et des partenaires, via des outils de confiance ;
- la gestion contractuelle des obligations et responsabilité, via la nouvelle structuration des clauses contractuelles.

Le système repose aujourd'hui sur une logique de contrôle *ex post*, imposant de nouvelles obligations de transparence auxquelles les entreprises devront se conformer par la mise en œuvre de moyens et d'instruments internalisés.

Trois principaux outils de compliance vont devoir être utilisés par les entreprises : le registre des activités, l'étude d'impact et le DPO. En répondant à des questions concrètes et simples (comment mener une étude d'impact ? quelles sont les qualités d'un bon DPO ?…) ce document guide pas à pas votre mise en conformité juridique.

Afin de démontrer son « accountability », le GDPR prévoit en outre le développement d'outils de confiance tels que les codes de conduite, les certifications et les règles d'entreprises contraignantes (ou BCR). L'intérêt et la pertinence de ces trois types d'outils sont précisément analysés dans ce chapitre.

Enfin, le GDPR bouleverse la notion de responsabilité entre les acteurs (« responsables de traitement » et « sous-traitants »), en encadrant beaucoup plus strictement les contrats conclus entre les parties. Après avoir rappelé les principes généraux de responsabilité, les rôles et obligations des différents acteurs, le document fournit des cas pratiques et détaille les modèles de clauses contractuelles dans le cadre d'un contrat entre responsable de traitement et sous-traitant et dans le cadre d'un contrat entre responsables conjoints.

SOMMAIRE

INTRODUCTION 9

La protection des données personnelles : un double enjeu sociétal et économique 9

« DPSI », une initiative de place du CIGREF, de L'AFAI et de TECH IN France, pour accompagner les entreprises dans leur mise en conformité 10

CHECK-LIST GDPR 21

Quel est l'objectif de la check-list ? 22

Démarche proposée 22

Check-list GDPR 26

RECOMMANDATIONS ET MESURES À METTRE EN PLACE POUR UN SI CONFORME 34

Identifier les mesures à mettre en place pour un SI conforme 35

Mesures potentiellement applicables sur les SI 36

Mesures applicables pour se protéger des risques identifiés 41

Illustration concrète de l'approche par le cas CRM 63

MODE D'EMPLOI ET OUTILS DE CONFORMITE AVEC LE CADRE LEGISLATIF ET REGLEMENTAIRE 75

Les outils de gouvernance 76

Les principaux outils de confiance vis-à-vis des tiers et la présomption de conformité 90

Les outils contractuels et les responsabilités 103

Cas pratiques et exemples de clauses 114

CONCLUSION 125

ANNEXES 127

SOMMAIRE DES ENCARTS

FOCUS ENTREPRISE : Michaël NGUYEN, Head of IT Management and Control, *SCOR – p.20*

FOCUS EXPERT : Jean-Sébastien MARIEZ, Avocat, *DE GAULLE FLEURANCE & ASSOCIES – p.21*

FOCUS EXPERT : Florence CHAFIOL, Avocat Associée**, Stéphanie LAPEYRE,** Avocat**,** *AUGUST DEBOUZY – p.34*

FOCUS ENTREPRISE : François CORNELY, Licensing executive, *MICROSOFT – p.39*

FOCUS ENTREPRISE : Michel BENARD, Urbaniste SI**,** *LES MOUSQUETAIRES – p.41*

FOCUS ENTREPRISE : Thierry MATHOULIN, Benjamin ALLOUL, Bernhard VON SONNLEITHNER, *WORKDAY – p.44*

FOCUS ENTREPRISE : Mylène JAROSSAY, Chief Information Security Officer *LVMH – p.63*

FOCUS ENTREPRISE : LIEN CEULEMANS, Senior Director, Legal - EMEA Privacy, **Salesforce** – p.64

ETUDE DE CAS ; Jérôme CAPIROSSI, General Manager, *UNEXX – p.65*

FOCUS EXPERT : Thaima SAMMAN, Associée-fondatrice et **Marc DREVON**, Avocat, *SAMMAN – chapitre 3*

FOCUS EXPERT : Béatrice DELMAS-LINEL, Associée-gérante et **Lise BRETEAU,** Avocat associée, *OSBORNE CLARKE – chapitre 3*

FOCUS ENTREPRISE : Elena GILOTTA, Directrice de la conformité de la zone EMEA, *BOX – p.85*

FOCUS ENTREPRISE : Stanislas DE RÉMUR, Cofondateur et CEO, *Oodrive – p.91*

FOCUS ENTREPRISE : Sylvain FOUREY, RSSI, *Groupe Cegid – p.96*

FOCUS ENTREPRISE : **Nathalie LANERET,** Responsable de la protection des données, *Capgemini – p.101*

FOCUS ENTREPRISE *:* **Christian LITAUDON,** Marketing Produits et Services**,** *SAGE – p.104*

FOCUS ENTREPRISE : Jawaher ALLALA, CEO, *Systnaps – p.115*

INTRODUCTION

La protection des données personnelles : un double enjeu sociétal et économique

Du point de vue sociétal, les États réglementent pour favoriser la confiance des consommateurs

Avec la révolution numérique, le monde est entré dans l'ère de l'information, nouvel or noir de l'économie. Grâce au développement d'internet et des nouvelles technologies, la donnée est devenue pléthorique, aisément accessible, et recèle une richesse encore très largement sous-exploitée.

La donnée ne sera cette immense source de création de valeur que si elle est dûment collectée, validée dans sa pertinence, mise en corrélation, travaillée, partagée et analysée. Sa large circulation est reconnue, par les experts autant que par les dirigeants d'entreprises et les autorités publiques, comme un facteur clé de la croissance de l'économie et de l'emploi. Les études[2] évoquent un impact d'au moins 10 points sur le PIB, potentiellement davantage dans les pays en développement ! Elle améliore également le fonctionnement interne, l'efficacité et la performance des entreprises de toute taille.

Rien n'arrêtera le « tsunami numérique » qui impacte nos vies personnelles et professionnelles, modifie les modèles d'affaire de nos entreprises, engendre de nouveaux services et métiers. Rien, sauf peut-être l'absence de confiance, véritable frein à l'adhésion des consommateurs.

La recrudescence des cyber-attaques, toujours plus sophistiquées et dans un contexte d'hyper-connectivité, entretient une méfiance légitime, aussi bien chez les individus, consommateurs et citoyens, qu'au sein des organisations. Et puisque la donnée est devenue critique, sa protection est un impératif absolu, tout au long de son cycle de vie. Le cas des données personnelles est particulièrement sensible, leur usage doit être transparent et limité. Différentes réglementations ont vu le jour ces dernières années dans de nombreux États, soucieux de protéger leurs citoyens et de favoriser la confiance sur laquelle repose le développement de l'économie numérique. Il en existe une centaine à ce jour.

Du point de vue économique, les entreprises doivent concilier protection des données personnelles et développement de leur activité

Nos entreprises, nos systèmes d'information, les solutions applicatives qui les composent, ont ainsi l'obligation de se mettre en conformité avec ces règles, le GDPR pour l'Union Européenne, et potentiellement d'autres dans le monde entier pour les sociétés dont l'activité est globale. Encore faut-il qu'elles soient raisonnables, identiques, ou pour le moins cohérentes, et qu'elles ne freinent pas le développement du business. Les obligations de localisation sur le territoire ou d'accès réservé aux ressortissants nationaux, comme dans certains pays, sont de bons exemples de contraintes difficilement compatibles avec la conduite d'une activité globale. De tels excès pourraient se traduire par l'obligation de

[2] ICC (International Chamber of Commerce), "Trade in the digital economy – A primer on global data flows for policymakers" et McKinsey Global Institute, "Digital globalization: The new era of global flows"

déployer de multiples instances des différents services, en contradiction avec les offres technologiques basées sur le cloud, et avec un fonctionnement opérationnel global.

Le défi est donc bien de développer la confiance et de protéger les personnes, tout en préservant l'activité économique de l'entreprise. Et ces deux enjeux ne sont pas antinomiques : une société réputée éthique tirera vraisemblablement bénéfice de sa réputation, et renforcera son attractivité pour les consommateurs.

« DPSI », une initiative de place du CIGREF, de L'AFAI et de TECH IN France, pour accompagner les entreprises dans leur mise en conformité

Présentation de l'initiative « Données Personnelles et Systèmes d'Information » (DPSI)

Les organisations professionnelles représentant les grandes entreprises (CIGREF), les auditeurs conseils en systèmes d'information (AFAI) et les éditeurs de logiciels (TECH IN France), rejoints par quatre cabinets d'avocats (August Debouzy, De Gaulle Fleurance & Associés, Osborne Clarke et SAMMAN), ont réuni leurs forces et travaillé conjointement depuis l'été 2016 pour produire un document de référence sur l'application concrète des règles de protection des données personnelles dans les entreprises et leur système d'information.

Cette initiative de place qui rassemble toutes les parties prenantes a fait suite à l'adoption du GDPR, applicable dès le 25 mai 2018, et a pour objectif d'accompagner les entreprises dans leur mise en conformité avec cette réglementation européenne.

L'initiative « DPSI », matérialisée par ce rapport, a cherché à mettre à la disposition des entreprises, clients et fournisseurs, un guide pratique avec un ensemble de mesures concrètes directement applicables. Il convient de préciser néanmoins que l'entreprise reste maîtresse des mesures qu'elle décidera de mettre en place, sur la base d'une appréciation de son contexte et d'une analyse de risque.

L'initiative « DPSI » est transverse à toutes les industries, et se positionne en amont et complément d'éventuels « Codes de conduite » professionnels. Ces « CoC » élaborés conjointement par les acteurs d'une même branche d'activité, et certifiés par une autorité agréée, sont prévus par le GDPR et encouragés par la CNIL.

Les travaux ont particulièrement ciblé le système d'information des organisations, qui porte leur activité, et dont l'architecture relève d'un choix d'entreprise répondant à des impératifs opérationnels (métier, marchés, flux de données, offre technologique comme le Cloud par exemple). Ce choix ne doit pas être remis en cause du seul fait des contraintes réglementaires sur les données personnelles. La conformité est un objectif incontournable, qui doit pouvoir être atteint quelles que soient les options techniques retenues.

Le groupe de travail conjoint AFAI, CIGREF, TECH IN France s'est donné deux objectifs principaux :

1. Sensibiliser les entreprises, utilisatrices et fournisseurs, sur l'urgence et l'ampleur de ce projet de mise en conformité avec le GDPR ;

2. Émettre des recommandations concrètes, applicables opérationnellement par les fournisseurs de services logiciels (on-premise ou SaaS), et par les entreprises utilisatrices, quels que soient leurs choix d'architecture et d'organisation.

Gouvernance de l'initiative « DPSI »

Les cabinets d'avocats experts se sont attachés à décrypter et à fournir une « lecture explicite et appliquée » du GDPR :

- Présentation des articles du GDPR ;
- Evolutions par rapport au droit existant ;
- Interrogations soulevées par les nouvelles dispositions ;
- Actions à envisager pour les entreprises.

Pour mémoire, **le GDPR comprend 99 articles précédés de plus de 170 considérants**, avec pour ambition :

- Une harmonisation des réglementations au sein de l'Europe ;
- Un renforcement du droit des personnes dont les données sont traitées (avec des droits nouveaux ou renforcés dont la minimisation, la portabilité, l'effacement…) ; le GDPR place délibérément l'individu au centre des préoccupations ;
- Un changement d'approche où les déclarations préalables sont remplacées par une capacité à s'autoréguler et à prouver la conformité des traitements.

Ce travail des avocats était précieux pour une compréhension commune et partagée du GDPR, et d'abord et avant tout de son périmètre d'application : définition d'une donnée personnelle, critères d'application du règlement européen (critère d'application territorial et matériel), etc.

Il a constitué le socle des travaux de trois chantiers menés en parallèle par trois sous-groupes, animés par une des trois associations et un ou deux cabinets d'avocats spécialisés. Les membres des trois associations étaient naturellement invités à participer à quelque chantier que ce soit.

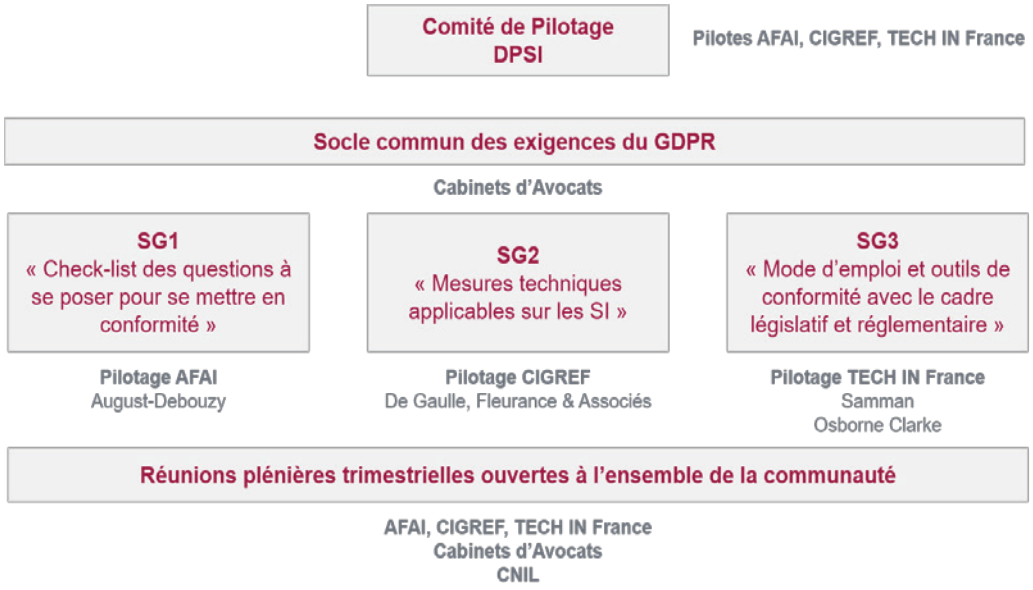
Les trois sous-groupes ont respectivement produit :

- **Une check-list des questions à se poser pour se mettre en conformité**, avec une identification des enjeux métiers, de gouvernance et de cybersécurité (piloté par l'AFAI et le cabinet August Debouzy) ; elle permettra une large sensibilisation en interne et une mesure de la maturité de l'entreprise vis-à-vis de la protection des données personnelles ;
- **Un inventaire des recommandations et mesures techniques** à potentiellement mettre en place pour un SI conforme, et ainsi renforcer la protection du SI, des données, et des droits de la personne (piloté par le CIGREF et le cabinet De Gaulle Fleurance et Associés) ;

- **Un guide juridique**, (piloté par TECH IN France et les cabinets Osborne Clarke et SAMMAN), abordant notamment les outils de gouvernance interne, les outils au bénéfice des tiers et les outils contractuels tels que résultant de la nouvelle réglementation.

Les travaux, produits après échanges avec la CNIL, ont permis de mettre en exergue l'importance d'engager un projet dédié au GDPR impliquant toutes les parties prenantes de l'entreprise, et de mener les actions d'évolution du SI, en collaboration entre clients et fournisseurs selon les responsabilités de chacun.

Ce projet n'est pas une option, mais un impératif, il doit être soutenu au plus haut niveau de l'entreprise, et disposer d'un budget spécifique et adéquat, dont la partie SI peut représenter une large partie sinon la majeure. « DPSI » a cependant aussi permis de démystifier le sujet, et de démontrer la faisabilité d'un tel projet de mise en conformité.



Gouvernance du groupe « DPSI »

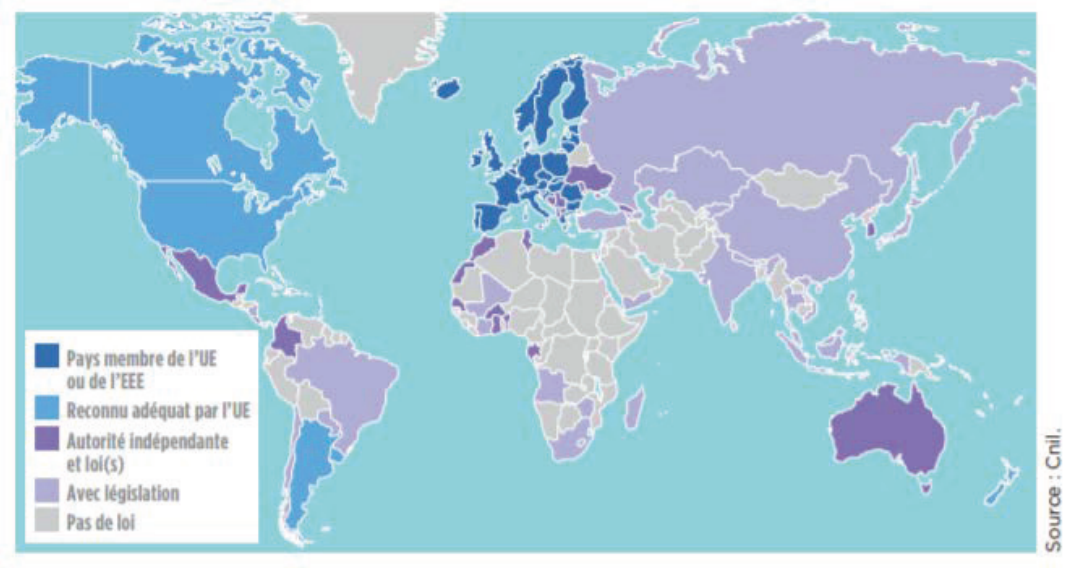
Chaque sous-groupe a recueilli les témoignages d'intervenants, représentant à la fois des clients et des fournisseurs, sur des thématiques spécifiques : cybersécurité, gouvernance d'un projet de mise en conformité GDPR en entreprise, préparation des offres logicielles aux réglementations sur les données personnelles, partage de responsabilité utilisateurs / fournisseurs, etc.

Des comités de pilotage ont eu lieu tous les deux mois avec les animateurs des trois sous-groupes pour le suivi et la coordination des travaux.

Trois plénières d'information ont été organisées durant l'année, afin de partager avec l'ensemble de l'écosystème l'avancement des travaux de chaque sous-groupe. La CNIL est intervenue à chacune de ces plénières, pour donner un regard croisé, commenter les travaux des sous-groupes, et suggérer des améliorations.

Contexte des différentes réglementations relatives aux données personnelles dans le monde

Plus de 80 pays ont adopté des réglementations spécifiques relatives à la protection des données personnelles. Ce sujet dépasse donc largement les frontières européennes, comme le montre la cartographie ci-dessous.



L'Europe a cependant une influence très forte en matière de réglementation sur la protection des données, notamment du fait du mécanisme de reconnaissance d'adéquation qui permet à la Commission européenne de reconnaitre le caractère adéquat vis-à-vis du GDPR désormais, des différents autres dispositifs réglementaires en place hors UE. Cette reconnaissance est assurée par le G29 notamment. A ce jour, des pays comme le Japon, l'Uruguay, l'Argentine, la Nouvelle-Zélande, Israël, le Lichtenstein et d'autres présentent un niveau de protection jugé adéquat par le G29.

La protection et le transfert international de données

Il existe plusieurs sources de référence pour organiser la protection des données et leur transfert par grandes zones géographiques. En voici quelques-unes :

- Les recommandations de l'OCDE ;
- Les Cross Border Privacy Rules dans la région Asie-Pacifique ;
- La Convention du Conseil de l'Europe, qui est une référence pour tous les pays signataires, dont la Russie ;
- Le Règlement européen sur la protection des données personnelles (GDPR) ;
- Le Privacy Shield qui encadre une partie des transferts entre l'Europe et les Etats-Unis.

Les diverses réglementations existantes en matière de protection des données personnelles présentent quelques éléments communs, tels que :

- La reconnaissance des droits des individus : droit d'information, droit d'accès, principe du consentement pour collecter ou transférer les données ;
- Les garanties de sécurité et de confidentialité ;
- L'existence d'un dispositif de conformité (le GDPR impose l'existence d'un tel dispositif), le principe d'accountability.

Les réglementations peuvent être transversales (couvrir toutes les industries à la fois), comme à Hong Kong, en Nouvelle-Zélande, en Corée du Sud, en Argentine ou encore au Japon, tout en encourageant l'émergence de référentiels sectoriels (type codes de conduite). A l'inverse, dans certains pays, les réglementations sont pensées dans une approche par industrie, comme en Chine et aux États-Unis principalement (réglementation spécifique aux secteurs de la santé et bancaire aux États-Unis par exemple). Dans d'autres pays enfin, plusieurs sources juridiques (droit commercial, droit du travail et autres sources) contribuent à faire émerger un corpus juridique relatif à la protection des données, comme au Brésil par exemple.

Une difficulté en matière de protection et de transfert de données pour les entreprises, encore plus pour celles qui sont globales, réside notamment dans l'interprétation des textes et la compréhension des définitions. Par exemple, tous les pays ne définissent pas de la même manière une « donnée sensible » : en Inde par exemple (qui ne dispose pas d'une réglementation spécifique sur la protection des données personnelles mais qui a un texte de loi relatif à la sécurité), le mot de passe est une donnée sensible. En Côte d'Ivoire, c'est le numéro de téléphone qui est considéré comme une donnée sensible à protéger.

Une autre difficulté naît de la différence d'approche sur la protection des données personnelles entre les juridictions. L'Union européenne érige en principe le droit à la vie privée et la protection des données personnelles tandis que les États-Unis ont une approche sectorielle de la protection des données.

Focus sur le GDPR

Il y a un changement de paradigme indiscutable s'agissant de la responsabilité des personnes traitant des données personnelles. En revanche, si la protection des droits des personnes concernées par le traitement des données personnelles est renforcée, sur le fond, le GDPR est fidèle à des principes historiques de l'UE.

Quoi ?

Le GDPR s'applique aux traitements de données à caractère personnel. Ces dernières sont définies de manière très large par le règlement. **Ainsi, constituent des données personnelles, toute information se rapportant à une personne physique identifiée ou identifiable.** Cela inclut notamment : le nom, un numéro d'identification, une adresse email, des informations génétiques, les adresses IP, etc.

La notion de traitement est tout aussi étendue mais ne diffère que marginalement de la définition qui figurait dans la Directive de 1995. Ainsi le traitement regroupe « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* ». On notera que sont notamment exclus du GDPR, les traitements n'entrant pas dans le champ d'application du droit de l'Union, les traitements des États membres dans le contexte des activités liées à la politique étrangère et de sécurité commune de l'Union ainsi que les traitements réalisés par une personne physique dans le cadre d'une activité personnelle ou domestique, etc.

Qui ?

Le GDPR fait peser en premier lieu des obligations sur les responsables de traitement et les sous-traitants. Le responsable du traitement est la personne physique ou morale qui détermine les finalités et les moyens du traitement tandis que le sous-traitant est celui qui traite des données à caractère personnel pour le compte du responsable de traitement.

Où ?

Le GDPR se caractérise par une portée territoriale étendue. Il s'applique au traitement de données personnelles effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union. Le GDPR s'applique également aux organisations qui ne sont pas établies dans l'Union mais qui visent ou monitorent des personnes résidant dans l'Union.

Source : Cabinet SAMMAN

Le GDPR prévoit notamment plusieurs outils d'accountability pour sa mise en œuvre effective comme la documentation des traitements des données, la nomination d'un Data Protection Officer ou la mise en œuvre des principes de privacy by design et de privacy by default. Le GDPR encourage également les entreprises à adopter des codes de conduite et des certifications ou labels comme cela a déjà été évoqué précédemment.

Le GDPR est découpé en 6 catégories d'exigences, auxquelles s'ajoute une catégorie générale de définitions et notions de bases :

Définitions / Notions de bases	Données à caractère personnel (« DCP ») Traitement de DCP (types, principes) Flux de DCP Responsable de traitement Sous-traitant Violation de CDP
Gouvernance interne	Rôle et responsabilité du DPO Registre des activités de traitement Privacy Impact Assessment (PIA) Privacy by design Codes de conduites et certifications
Rapport avec les data subjects	Transparence, information et consentement Gestion de l'exercice des droits des personnes : accès, opposition, rectification, effacement, portabilité, limitation Profilage et décisions automatisées
Partage de responsabilité	Stipulations contractuelles obligatoires Responsabilité du responsable de traitement Responsabilité du sous-traitant Régime de responsabilité conjointe
Transfert de données hors UE	Mécanisme de transferts existants : adéquation, clause contractuelle, BCR, Privacy Shield Dérogations
Sécurité et notification des violations de données personnelles	Mesures juridiques Mesures organisationnelles Mesures de sécurité logique Mesures de sécurité physique Privacy by design Dispositifs de détection
Voies de recours, responsabilité et sanctions	Droit de recours (réclamation, recours juridictionnel) Droit à réparation et responsabilité Sanctions

Source : CIGREF « Données Personnelles et Systèmes d'Information » (2017)

Ce qui change pour les entreprises :

- **Le concept de « privacy by design / by default »** : il s'agit d'intégrer la protection des données à caractère personnel non seulement dès la conception des produits et services mais également, par défaut, la plus protectrice possible (notamment avec le principe de minimisation introduit par le GDPR, exigeant de réduire tout traitement de données personnelles au minimum nécessaire) ; ceci revient à dire que, culturellement, il faut intégrer cette notion en amont des projets : quel que soit le projet, les équipes doivent intégrer ce souci de la protection des données à caractère personnel et cette démarche de minimisation dans leur feuille de route. Certains systèmes legacy devront potentiellement faire l'objet de privacy by re-design s'ils sont sensibles. Ce concept a été proposé par Ann Cavoukian, Commissaire à l'information et à la protection de la vie privée de l'Ontario, et encourage à introduire la privacy by design dès qu'il y a un changement dans les systèmes.

- **L'obligation de désigner un Data Protection Officer (DPO)** : la nomination du DPO n'est obligatoire que sous certaines conditions (voir ci-dessous) et les États membres ont la possibilité d'étendre cette obligation de nomination. Cependant, dès lors qu'une entreprise traite des données personnelles elle devrait envisager la nomination d'un DPO, notamment pour diffuser la culture de protection des données dans les processus internes de l'entreprise.

- **L'obligation de notification de failles et d'atteinte à la sécurité informatique** : cette obligation implique un changement de processus car elle nécessite une vigilance accrue ; aujourd'hui, la cybersécurité est un enjeu majeur : par exemple, en 2015, sur 550 contrôles de la CNIL (contrôles sur place, sur pièces ou en ligne), dans 85% des cas, la CNIL a été amenée à émettre des recommandations, faire des observations, voire des mises en demeure sur des enjeux de sécurité informatique (selon Edouard Geffray, ex-Directeur général de la CNIL « *nous [les entreprises] avons un niveau d'hygiène en matière de sécurité informatique de base qui est désespérant (…) Il faut en moyenne 240 jours pour détecter un hacker qui s'est introduit dans votre SI. Vous imaginez un cambrioleur qui se promène pendant 240 jours dans votre maison sans que vous l'ayez remarqué ?* »).

- **Les analyses d'impact sur la vie privée – EIVP, (ou Privacy Impact Assessment - PIA)**[3] : il s'agit d'anticiper les impacts d'un nouveau produit ou service sur la vie privée des clients. Un PIA, mené par le responsable de traitement, avec le concours du DPO et des sous-traitants, et doit être réalisé avant la mise en œuvre du traitement susceptible d'exposer les personnes à un risque élevé au regard de leurs droits et libertés. Cette analyse d'impact permet de mieux mettre en œuvre les principes de *privacy by design* et *privacy by default* introduits par le GDPR. Le PIA favorise une logique de conception respectueuse de la vie privée (Privacy by Design), il est ainsi un moyen pour les entreprises de montrer que leurs solutions sont

[3] Pour la réalisation d'un PIA, voir les documents CNIL suivants : « *PIA, la méthode* » : ce document indique la marche à suivre pour faire une étude d'impact sur la vie privée. Il fournit différents modèles et un guide de mesures conseillées, en précisant le domaine d'application, les responsables de l'étude, les différentes catégories de risques à prendre en compte par rapport à la notion de vie privée, et les processus de validation du PIA.« *PIA, l'outillage : modèles et bases de connaissances* » : ce document propose quant à lui une échelle et des règles pour estimer la gravité d'une violation, avec 4 niveaux de risques. Guide en 6 étapes pour se préparer au règlement européen : la 4ème étape intitulée « Gérer les risques » décrit la démarche de PIA en cas de traitements de données personnelles susceptibles d'engendrer des risques pour les droits des personnes.

respectueuses de la vie privée et assure un niveau de protection conforme aux obligations du droit de l'Union. Par ailleurs, le PIA devrait permettre à l'entreprise de s'affranchir de la plupart des déclarations ou autorisations CNIL liées aux traitements de données personnelles, et d'avoir une cartographie des différents traitements et des risques.

- **L'obligation d'informer les clients sur la finalité de l'usage de leurs données personnelles par l'entreprise** : le consentement et la définition des finalités engagent une forte responsabilité des entreprises vis-à-vis de leurs clients, en ayant l'obligation de leur « *fournir un avis clair expliquant à quelles fins leurs données sont collectées […] le consentement doit être "libre, spécifique, informé et sans ambiguïté". Il est extrêmement important que les organisations comprennent cette exigence.* »[4]

- **Le droit à la portabilité** va impliquer des évolutions substantielles, notamment dans les métiers de la banque et de l'assurance (par exemple, l'obligation de restituer à un client l'ensemble des pièces fournies par ce même client pour l'obtention d'un prêt, dans un format numérique aisément réutilisable).

Le principal enjeu du régulateur aujourd'hui est d'apporter un maximum de sécurité juridique aux entreprises dans le cadre du GDPR. L'harmonisation que permet le GDPR participe de ce renforcement de la sécurité juridique, mais un certain nombre de dispositions du GDPR sont ouvertes aux législations des États membres ce qui pourrait remettre en cause cet objectif. L'harmonisation passe également par la mise en œuvre de mécanismes de coordination entre les autorités de protection des données. Ainsi, le GDPR instaure un principe de guichet unique pour les traitements transfrontaliers de données à caractère personnel.

Par ailleurs, les droits des personnes dont les données sont traitées sont renforcés et les sanctions possibles accrues (jusqu'à 4% du chiffre d'affaires global de l'entreprise, qui est un plafond au sein de l'Union). Ainsi, au sein des entreprises, la conformité doit être gérée comme un projet, dont la majeure partie est vraisemblablement liée à l'IT. Avant d'être juridique ou légal, ce projet est global avec une forte composante SI puisque la mise en conformité nécessite la mise en place de mesures techniques liées à la sécurité des SI et à la protection des données. Il est donc absolument crucial d'y consacrer un budget qui soit proportionnel à l'enjeu. Un point d'honneur est mis sur la bonne gouvernance des données en interne. Pour de nombreuses entreprises, cette réglementation est aussi l'occasion de faire et/ou mettre à jour leurs cartographies de données.

[4] « L'impact opérationnel du règlement général sur la protection des données de l'Union Européenne sur l'informatique », Dana Simberkoff, AvePoint

Michaël NGUYEN
Head of IT Management and Control
SCOR

Pouvez-vous nous décrire la structuration de votre programme GDPR ?

La structuration du programme GDPR chez SCOR se découpe en 7 domaines, 4 relatifs au juridique et à la conformité et 3 portant sur les mesures techniques de renforcement de la protection des données :

1. Inventaire des traitements utilisant des données personnelles, ainsi que les workflows techniques qui embarquent ces données personnelles ;

2. Identification des risques sur les données personnelles SCOR, élaboration d'une matrice de risques et définition de plans de remédiation ;

3. Définition et mise en place du processus de notification de failles ;

4. Revue des contrats : identification des contrats à adapter avec les « processeurs » de données externes à SCOR, définition de clauses standards spécifiques aux données personnelles, à introduire dans ces contrats critiques ;

5. Renforcement des contrôles d'accès et traçabilité ;
    1. Gestion des accès des utilisateurs aux fichiers partagés ;
    2. Gestion des accès des utilisateurs aux applications critiques ;
    3. Gestion des accès des administrateurs aux applications (comptes à privilèges) ;

6. Définition d'une stratégie de conservation et d'archivage des données ;

7. Réalisation d'une étude sur le chiffrement des données critiques.

La roadmap effective du projet se termine en décembre 2017. Tout le premier trimestre 2018 sera consacré à la sensibilisation et à la formation de tous les collaborateurs du Groupe, IT et Métiers, aux nouveaux processus de gestion des données personnelles.

Jean-Sébastien MARIEZ
Avocat
De Gaulle Fleurance & Associés

L'obligation de notification des violations de données personnelles annonce un changement de paradigme

Alors que de nombreuses organisations disposent déjà d'un processus de gestion des incidents de sécurité, la durée moyenne de détection dépasse encore souvent un an[5] quand le GDPR impose une notification dans un délai de 72h, certes à partir du moment où la violation est connue. Des sanctions récentes prononcées par la CNIL montrent d'ailleurs que parfois, le responsable de traitement est informé de la fuite par l'autorité de contrôle elle-même à la suite, par exemple, d'un contrôle en ligne[6].

Cette nouvelle obligation issue du GDPR met l'accent sur le volet curatif des politiques de sécurité qui prolonge le volet préventif déjà prévu par la *Loi informatique et liberté*[7]. Sauf à ce qu'elle ne représente aucun « *risque pour les droits et libertés des personnes physique* », le responsable de traitement devra notifier à la CNIL les mesures prises pour remédier à la violation, atténuer ses conséquences négatives et apporter des garanties quant au risque de répétition de l'incident (art. 33 du GDPR).

La réputation du responsable de traitement sera particulièrement exposée lorsque l'information de chacune des personnes concernées sera requise, à savoir, toutes les fois où la violation représentera un « *risque élevé* » pour leurs droits et libertés. Trois exceptions sont cependant prévues. La communication aux personnes ne sera pas nécessaire lorsque des mesures telle que le chiffrement des données auront été appliquées en amont de la violation ou bien, en aval de la violation, lorsque les mesures correctives garantiront que le risque élevé n'est plus susceptible de se matérialiser. De même, si l'information individuelle des personnes nécessitait des « *efforts disproportionnés* » alors, le responsable de traitement sera autorisé à recourir à un mode de communication publique (art. 34 du GDPR).

Des éléments de complexité demeurent malgré les éclaircissements apportés par le G29 dans son avis du 3 octobre 2017[8]. Les processus en place doivent être revus en prêtant attention :

- aux **dispositifs de détection**, y compris dans le cadre des relations avec les sous-traitants ;
- à l'évaluation amont du niveau de risque associé à chaque traitement, y compris, au moyen d'**analyses d'impact.**
- à la cohérence avec les **autres obligations de notification** prévues par les textes
- à la gouvernance des incidents au moyen d'une **cellule de gestion de crise interdisciplinaire** (communication, technique, juridique).

---

[5] https://questionsdetransformation.ey.com/dossiers/quel-systeme-de-securite-pour-des-entreprises-cyber-resilientes-_f-50.html

[6] Voir https://www.cnil.fr/fr/hertz-france-sanction-pecuniaire-pour-violation-de-donnees-personnelles et https://www.cnil.fr/fr/violation-de-donnees-personnelles-avertissement-lencontre-de-la-societe-ouicar

[7] https://www.cnil.fr/fr/loi-78-17-du-6-janvier-1978-modifiee

[8] http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

CHAPITRE 1

CHECK-LIST GDPR

Piloté par **Pascal ANTONINI**,
Président de l'AFAI

Coordonné par **Bertrand HELFRE**,
Director and Leader Cybersecurity, WEAVE

Avec le concours de **Florence CHAFIOL**, Avocat Associée et **Stéphanie LAPEYRE**, Avocat, August Debouzy.

afai
Pour des systèmes d'information de confiance et créateurs de valeur

L'objectif de ce chapitre est de fournir quelques repères par rapport à l'utilisation de l'outil : check-list GDPR - v1.0 – 14092017 – FR *(voire annexes)*.

Quel est l'objectif de la check-list ?

L'outil de check-list est un guide d'auto-évaluation. C'est la 1re phase de la démarche globale de mise en conformité avec le Règlement Général de Protection des Données Personnelles (GDPR).

Cette check-list poursuit deux objectifs :

- vérifier que les différentes exigences du GDPR ont bien été prises en compte par les organisations et que les mesures adéquates ont été adoptées ;
- renforcer la communication et le partage des informations au sein des équipes (juridiques, métiers, informatiques) travaillant à la mise en conformité au GDPR.

L'outil est une liste de questions permettant une évaluation structurée du niveau de maturité de l'entreprise quant à la mise en conformité au GDPR et permet ainsi d'identifier plus facilement les éventuelles lacunes et les mesures à mettre en œuvre dans le cadre du Règlement. Il doit être perçu comme un outil d'aide et d'accompagnement pour les entreprises mais en aucun cas comme une contrainte supplémentaire. Les thèmes abordés sont essentiels pour toutes les organisations et permettent de balayer la plupart des questions à se poser dans le cadre de la mise en conformité. Le groupe de travail (SG1) composé d'une quarantaine de personnes représentant les entreprises de tous secteurs a participé à la rédaction de la check-list GDPR. Les deux principes retenus par le SG1 ont été les suivants :

- concision : établir une check-list limitée à 50 questions maximum ;
- simplicité : questions précises et fermées.

Démarche proposée

La check-list doit permettre de vérifier que toutes les obligations principales imposées par le GDPR ont été prises en compte par les différentes parties prenantes de l'entreprise : la Direction Générale, les Directions Métiers et la Direction des Systèmes d'Information, ainsi que les partenaires tiers externes. La check-list est subdivisée en trois grands thèmes correspondant aux acteurs cités ci-dessus :

- Gouvernance
- Métiers
- Systèmes d'information et Cybersécurité

En complément des réponses apportées, la check-list permet aussi de collecter des éléments factuels sur les lacunes ou les points de vigilance, lorsque la réponse à une question est négative.

Transversalité

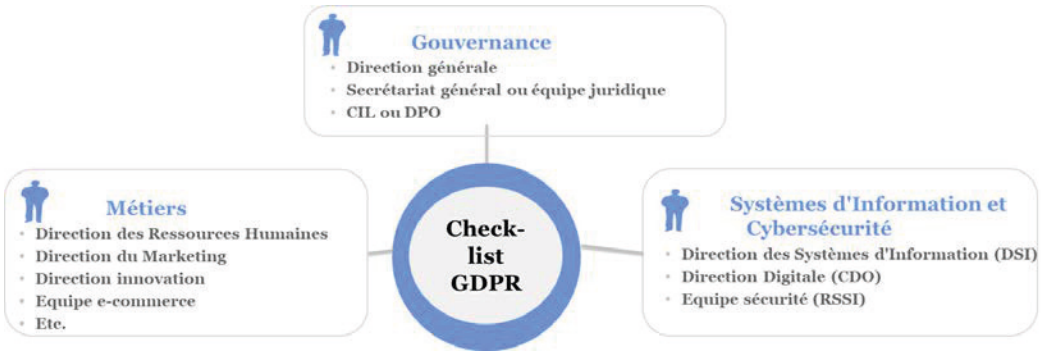
Dans tous les cas, il est primordial que toutes les directions ou les équipes citées dans ce chapitre soient impliquées dans la démarche et puissent apporter leur contribution en ce qui concerne les pratiques relatives aux données personnelles. Ainsi, c'est grâce à l'investissement et à la collaboration efficace de tous les acteurs que l'entreprise pourra acquérir une vision complète et globale des traitements de données personnelles mis en œuvre tout en respectant le périmètre de responsabilité de chacun des acteurs. En effet, il n'est pas rare de constater que chacune des équipes a une vision partielle des données qu'elle utilise sous le prisme de son domaine de compétence mais qu'aucune n'a de vision transversale (ex : SI pour les applications, Sécurité pour les mesures de sécurité, Juridique pour les aspects contractuels, Métier pour des relations directes avec des fournisseurs de solutions, …).

Pilotage

Le DPO (Data Protection Officer) ou DPD en français (Délégué à la Protection des Données), s'il est nommé, est idéalement placé pour gérer la check-list et la diffuser auprès des acteurs concernés. Cette démarche lui permet de s'approprier le périmètre de la protection des données en lui faisant rencontrer les équipes adéquates et en lui permettant d'identifier les solutions existantes et celles à mettre en œuvre. Si le DPO n'est pas encore nommé ou si le périmètre à couvrir requiert une délégation, il convient d'identifier une personne positionnée à un niveau transverse (contrôle interne, organisation, voire un détachement d'un auditeur interne) pour animer la démarche auprès des différents acteurs identifiés.

Acteurs concernés

La donnée constituant un patrimoine de plus en plus stratégique pour les entreprises, tous les acteurs et toutes les divisions de l'entreprise sont susceptibles de devoir, à un moment ou à un autre, manipuler de telles données. Ci-après sont identifiées les différentes équipes potentiellement impliquées en indiquant leur principal domaine de contribution.



Futur délégué à la protection des données (DPO)

Les missions du DPO sont notamment les suivantes (article 39 du GDPR) :

- Informer et conseiller le responsable de traitement ou le sous-traitant, ainsi que l'ensemble de leur personnel ;
- Contrôler le respect du Règlement et de la législation nationale ;
- Conseiller l'organisme sur tout sujet relatif à la protection des données à caractère personnel (notamment, sur la pertinence d'une étude d'impact) ;
- Coopérer avec l'autorité de contrôle : cette fonction est très importante, puisque le délégué devra faciliter l'accès par l'autorité aux documents et informations dans le cadre de l'exercice des missions et des pouvoirs de cette autorité.

Direction des systèmes d'information

En charge des systèmes d'information, cette direction est à même d'apporter ses connaissances sur tous les aspects techniques liés aux applications dont elle a la charge. Dans l'idéal, elle dispose d'une cartographie à jour des données traitées et des applications liées à l'utilisation de ces données, voire des traitements de données eux-mêmes. Il faut néanmoins rappeler que cette cartographie, étant établie conjointement par les DSI et les Directions Métiers, il existe dans beaucoup d'entreprises, des traitements (automatisés ou non) qui rentrent dans le champ de responsabilité des Directions Métiers. Ceci implique d'aller à la rencontre les Directions Métiers, notamment Innovation, Marketing ou Ressources Humaines pour identifier avec elles les applications concernées (site web, jeu à vocation commerciale sur internet, solution en mode Software as a Service (SaaS), …)

Équipe sécurité des systèmes d'information

En fonction de l'organisation de l'entreprise, cette équipe (au sein de la DSI ou non) est en charge de définir et de mettre en place les mesures de protection techniques et organisationnelles relatives aux différents traitements de données. L'équipe sécurité, habituée à gérer la sécurité par les risques, est en position de réaliser des études d'impact sur la vie privée (DPIA) telles que requises par le GDPR. Par ailleurs, le DPO ne disposant pas toujours des compétences nécessaires à la réalisation des analyses de risques, l'équipe sécurité est en mesure de l'assister dans l'approche et la réalisation des DPIA dans leur ensemble.

Équipe juridique

Elle doit être impliquée dans les démarches de contractualisation ou de relation avec les autorités de contrôle locales. Elle est aussi consultée pour tout ce qui concerne les mentions légales, conditions générales d'utilisation, mentions d'information, etc. Elle est donc en mesure d'apporter sa compétence sur ces aspects lors de l'inventaire des traitements (vérification de la base légale qui fonde la licéité de chacun des traitements).

Direction innovation

En fonction de l'organisation de l'entreprise, au travers de ses activités data, digital ou relation client, l'innovation est au cœur de l'utilisation de la donnée personnelle client. À ce titre, elle est donc incontournable aussi bien dans l'identification des traitements que des partenaires ou destinataires des données.

Direction marketing

En fonction de l'organisation de l'entreprise, cette direction est souvent en lien avec le client au travers de l'analyse des habitudes de consommation dudit client, de l'envoi de newsletters ou de toute autre collecte de données dans le cadre de ses activités (pour le cas du e-commerce, voir équipe e-commerce). Au même titre que l'innovation, le marketing peut être amené à réaliser des opérations avec des partenaires commerciaux en vue de collecter ou d'échanger des données personnelles.

Direction des Ressources Humaines (DRH)

En charge du périmètre des solutions concernant la gestion des ressources humaines dans l'entreprise, elle apporte la connaissance du périmètre d'un point de vue métier et de relation éventuellement directe avec ses fournisseurs. Cette direction collecte à la fois des données personnelles des collaborateurs et celles des candidats et peut être amenée à échanger ces données avec plusieurs partenaires différents.

Elle assure également la conformité vis-à-vis des règles de droit du travail, et veille notamment à ce que les obligations d'information des salariés et des instances représentatives du personnel (voire la consultation de ces dernières) soient respectées. Elle s'assure enfin que les relations avec les autres sociétés employant du personnel sur site (intérimaires, prestataires, etc.) respectent les règles applicables.

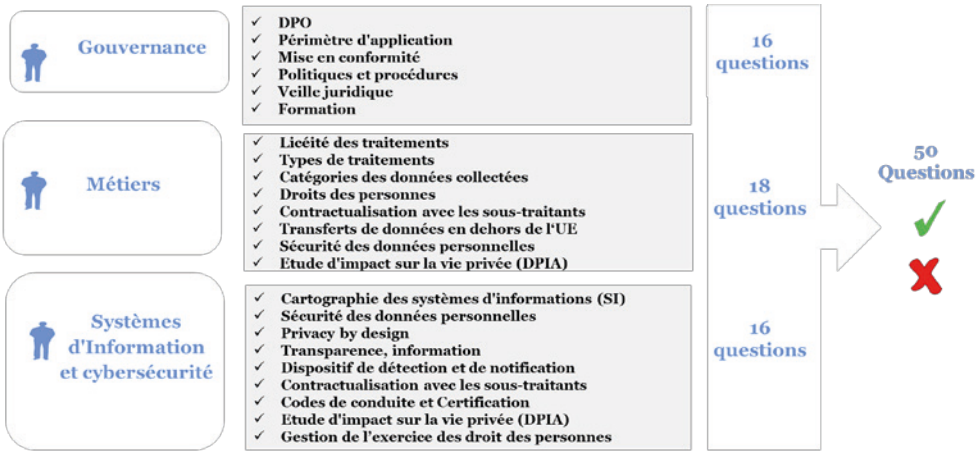
Équipe e-commerce

S'il existe dans l'organisation une équipe spécifique pour la prise en charge du e-commerce, elle doit être consultée. Le e-commerce implique par essence la collecte et le traitement de données de consommateurs et est facilement exposé aux autorités de contrôle. Les équipes peuvent être amenées à avoir recours à des prestations en mode SaaS permettant par exemple de faire de la mesure de trafic.

Sur le périmètre e-commerce, les problématiques liées au dépôt de cookies doivent faire l'objet d'une attention particulière afin d'assurer que l'ensemble des règles applicables en la matière sont respectées. Pour cette activité, on se rapprochera des équipes en charge du trafic sur le site et des équipes SI spécialisées.

Check-list GDPR

Thèmes et sous thèmes :



Comme évoqué plus haut, la check-list doit permettre de vérifier les points critiques du GDPR et d'identifier les actions à mettre en œuvre selon les directions concernées.

✓ Si la réponse est « Oui », votre entreprise est en bonne voie pour se mettre en conformité avec le GDPR.

✗ Si la réponse est « Non », la question peut vous aider à identifier les domaines que vous devez améliorer.

Les tableaux ci-dessous reprennent les différentes questions traitées dans l'outil de check-list. La colonne « THEME » » indique le thème du GDPR permettant de regrouper les différentes questions à poser.

Les trois thèmes (Gouvernance, Métiers, Système d'information/Cybersécurité) reprennent les fonctions évoquées précédemment. Pour chaque question, la direction concernée peut apporter des éléments concernant la question ou bien consulter une ou plusieurs autres fonctions.

Check-list « gouvernance »

Sous thème	#	Question	Commentaire / Exemple
DPO (délégué à la protection des données personnelles)	**1**	Avez-vous nommé DPO ? Si non, avez-vous vérifié et documenté que vous n'êtes pas soumis à cette exigence ?	D'après l'article 37 §1, la nomination d'un DPO est notamment obligatoire dans le cas où vos activités de base consistent des opérations de traitement à grande échelle impliquant un suivi systématique des personnes concernées, ou des données sensibles au sens des articles 9 et 10.
	2	Le rattachement hiérarchique du délégué à la protection des données personnelles (DPO) garantit-il son indépendance ?	
Périmètre d'application	**3**	Avez-vous déterminé le périmètre des entités / Business Unit concernées par le plan de mise en conformité ?	
	4	Avez-vous établi un registre des traitements dont vous êtes responsable, co-responsable ou sous-traitant ?	Le registre comporte le nom et les coordonnées du responsable du traitement, les finalités du traitement, les catégories de destinataires et des personnes concernées, etc.
	5	Avez-vous identifié les transferts de données personnelles hors Union Européenne ? Si oui, avez-vous formalisé les garanties mises en œuvre ou à l'étude ?	Garanties cf. chapitre V du GDPR : soit niveau de protection adéquate du pays tiers (art. 44) soit mécanisme de sauvegarde visé à l'art 46 (par ex. Binding Corporate Rules)
	6	Avez-vous réalisé un état des lieux des processus métiers traitant des données personnelles ?	
	7	Avez-vous identifié les sous-traitants traitant vos données personnelles ? Si oui, vous assurez-vous que les sous-traitants existants et futurs sont conformes aux exigences du GDPR contractuellement et par le biais de contrôles ?	
Mise en conformité	**8**	Avez-vous mis en place une organisation projet pour la mise en conformité au GDPR ?	Une organisation projet couvre généralement le(s) sponsor(s), l'équipe projet, les tâches, jalons et livrables

Sous thème	#	Question	Commentaire / Exemple
	9	Avez-vous établi une feuille de route pour la mise en conformité au GDPR ?	Une feuille de route propose généralement les projets, le recensement des moyens, la cible à atteindre, la priorité des tâches, ainsi qu'un calendrier pour atteindre ces buts.
	10	Existe-t-il un reporting périodique au Board/Comex pour s'assurer de l'avancement du plan d'action et décider d'actions correctrices ?	
	11	Le plan d'audit intègre-t-il des missions de contrôle de la mise en conformité au GDPR ?	
Politiques et procédures	**12**	Avez-vous intégré les éléments de conformité au GDPR dans vos politiques et procédures ?	Les politiques précisent les durées de conservation des données personnelles, la sécurité des données, la suppression des données, la notification en cas de violation des données personnelles, la validation périodique de la pertinence du dispositif en place, etc.
Veille juridique	**13**	Une veille juridique a-t-elle été mise en place pour suivre les évolutions réglementaires ?	Exemple : guidelines émises par le G29 (WP29)
Formation	**14**	Les politiques et procédures en lien avec le GDPR sont-elles diffusées aux collaborateurs de votre entreprise ?	Exemple : code de conduite
	15	Avez-vous intégré le GDPR à votre programme de formation RH ?	Le programme de formation inclut des dispositifs comme du E-learning, des formations régulières (Manager, SI, métiers), des actions de communication, etc.
Assurance	**16**	Avez-vous revu la couverture d'assurance de votre entreprise pour tenir en compte du GDPR ?	

Check-list « Métiers »

Sous thème	#	Question	Commentaire / Exemple
Licéité des traitements	**17**	Avez-vous identifié pour vos traitements les finalités, les personnes concernées et les catégories de données traitées ?	Ces éléments sont un préalable nécessaire à l'établissement du registre de traitements exigé par le GDPR pour chaque responsable de traitement et sous-traitant.
	18	Avez-vous vérifié la proportionnalité des données collectées aux finalités des traitements ?	Limiter par défaut le traitement de données à caractère personnel à ce qui est strictement nécessaire, en ce qui concerne la quantité de données traitées, leur accessibilité et leur période de conservation.
	19	Pouvez-vous justifier la base légale de chacun de vos traitements ?	Le traitement doit être fondé sur une base légale prévue à l'article 6 du GDPR (licéité), qui peut être : une obligation légale, l'intérêt légitime du responsable de traitement, l'exécution d'un contrat, le consentement exprimé par la personne concernée, la protection des intérêts vitaux d'une personne concernée, une mission d'intérêt ou de service public.
	20	Lorsque la base légale du traitement est le consentement, avez-vous mis en place des mécanismes de gestion de ce consentement ?	Gestion : recueil, enregistrement, modification, révocation, etc.
	21	Pour les traitements impliquant le croisement entre plusieurs catégories de données (interconnexion de fichiers), la réutilisation de données collectées lors d'un autre traitement ou l'enrichissement des données, avez-vous consulté le DPO et vérifié la conformité au GDPR ?	Si vous - effectuez des croisements entre plusieurs catégories de données collectées séparément, ou - réutilisez des données collectées pour un autre traitement, ou - utilisez des données fournies par une tierce partie, Vous devez vérifier que votre traitement est conforme aux finalités pour lesquelles les données ont été collectées ou, le cas échéant, aux consentements donnés par les personnes concernées
	22	Des durées de conservation sont-elles définies pour les données traitées ? Si oui, les durées sont-elles communiquées aux personnes concernées ?	

Sous thème	#	Question	Commentaire / Exemple
Types de traitements	**23**	Pour les traitements entrant dans le cadre du profilage, avez-vous consulté le DPO et vérifié la conformité au GDPR ?	Profilage : toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique
	24	Pour les traitements soumis à des hauts risques potentiels sur la vie privée, avez-vous consulté le DPO et vérifié le respect des conditions spécifiques ?	Exemples de traitement : vidéosurveillance, géolocalisation, whistleblowing, écoute sur le lieu de travail, contrôle d'accès aux locaux, biométrie, etc.
Catégories des données collectées	**25**	Si vous collectez des catégories particulières de données (données sensibles), avez-vous vérifié la licéité de leur collecte et de leur traitement ?	Cf. articles 9 et 10 du GDPR.
Droits des personnes	**26**	Les personnes concernées bénéficient-elles d'une information claire et compréhensible lors de la collecte des données ?	
	27	Avez-vous une procédure validée et testée pour répondre aux demandes d'exercice des droits prévus par le GDPR ? En particulier droits d'accès, de rectification, de suppression des données de droit à l'oubli, de droit à la portabilité ou de limitation de traitement ?	Y compris la notification des demandes de rectification ou de suppression aux sous-traitants ou autres tierces parties destinataires des données.
	28	Les personnes concernées peuvent-elles modifier leur consentement ?	Exemple : Self-service.
Contractualisation avec les sous-traitants	**29**	Avez-vous défini contractuellement avec vos sous-traitants des exigences en termes de protection des données ?	
Transferts de données en dehors de l'Espace Economique Européen	**30**	Si vous effectuez des transferts de données personnelles à des entreprises situées hors de l'Union Européenne, vous êtes-vous rapprochés de votre DPO ou de votre service juridique pour vérifier que les transferts effectués soient couverts par des garanties appropriées ?	
Sécurité des données personnelles	**31**	Avez-vous exprimé des exigences de protection des données personnelles vis à vis de votre service informatique ?	Exemple d'exigences de sécurité : pseudonymisation, chiffrement, stockage et transferts sécurisés, règles de purge ou d'archivage, etc.

Sous thème	#	Question	Commentaire / Exemple
	32	Etes-vous associé au processus de détection, de traitement et de notification des violations de données personnelles ?	
Etude d'impact sur la vie privée (DPIA)	**33**	Avez-vous défini des critères de décision pour déterminer si une Etude d'impact sur la vie privée (DPIA) était nécessaire ?	
	34	Si la criticité du traitement implique une étude d'impact sur la vie privée (DPIA), avez-vous effectué cette étude en coordination avec le DPO ?	

Check-list « Systèmes d'Information et cybersécurité »

Sous thème	#	Question	Commentaire / Exemple
Cartographie des systèmes d'informations (SI)	**35**	Avez-vous une cartographie exhaustive des données personnelles traitées dans votre système d'information ?	Dictionnaire de données, accès (utilisateurs, interfaces), applications, bases de données, serveurs, Datacenter, services cloud, localisation, etc.
Sécurité des données personnelles	**36**	Avez-vous intégré les éléments de conformité au GDPR dans votre politique de sécurité des systèmes d'information ?	
	37	Utilisez-vous des standards ou des guides de bonnes pratiques Security by design ?	Exemples de référentiels de sécurité : ISO27001, NIST, guide d'hygiène ANSSI, CIS critical security controls, etc.
	38	Avez-vous défini et mis en place des procédures de gestion des accès aux systèmes contenant des données personnelles ?	Conception des habilitations, ajout/suppression des droits, revues régulières des droits d'accès)
	39	Avez-vous défini et mis en place des mesures de sécurisation des accès administrateurs privilégiés ?	Bastion, enregistrement de sessions des comptes à privilèges sur les serveurs, ...)
	40	Avez-vous mis en place des mécanismes de protection des données personnelles (notamment chiffrement ou de pseudonymisation) ?	Données stockées sur les serveurs (Data at Rest) et pour le transport de ces données sur le réseau (Data in transit), (exemples : outils de tokenisation, ...)

Sous thème	#	Question	Commentaire / Exemple
Protection de la vie privée dès la conception (« privacy by design »)	**41**	Avez-vous mis en place des mécanismes d'archivage et de suppression des données personnelles ?	
	42	Ces mécanismes sont-ils alignés sur la politique de conservation (notamment avec les durées légales ou contractuelles de rétention des données) ?	
	43	Avez-vous mis en place des mécanismes permettant d'isoler les environnements de production et de non production (test, recette) ?	Segmentation réseau, pare feux, anonymisation éventuelle des données personnelles en environnements de non production.
Transparence, information	**44**	Avez-vous mis en place des mécanismes de traçabilité et de détection d'accès aux données personnelles ? (Notamment déplacement ou copie de données non autorisés déclenchant des alertes aux équipes sécurité)	Accès des utilisateurs/interfaces, déplacements et copies en masse des données à personnelles, etc.
Dispositif de détection et de notification	**45**	Avez-vous établi la procédure de détection, de traitement et de notification des violations de données personnelles ?	Procédure détaillant la détection, la réponse à incident et la communication en cellule de crise, puis l'autorité dans les 72 heures
Contractualisation avec les sous-traitants	**46**	Avez-vous défini contractuellement des exigences en termes de protection des données avec vos sous-traitants informatiques (prestataires ou fournisseurs) ?	Exemples : questionnaire de sécurité, clauses contractuelles liées à la protection des données, clause d'audit de sécurité, suppression des données à la fin de la prestation, etc.
Codes de conduite et Certification	**47**	Effectuez-vous régulièrement des contrôles / audit de sécurité de vos sous-traitants informatiques (prestataires ou fournisseurs) ?	Exemples : vérification de la mise en place des clauses de sécurité, audit technique de sécurité, tests d'intrusion, etc.
Etude d'impact sur la vie privée (DPIA)	**48**	Avez-vous défini des critères de décision pour déterminer si une Etude d'impact sur la vie privée (DPIA) était nécessaire ?	
	49	Avez-vous défini une méthode d'étude d'impact vie privée en coordination avec le DPO ?	Exemples : Etude d'impacts sur la vie privée : la méthode de la CNIL
Gestion de l'exercice des droits des personnes	**50**	Avez-vous défini et mis en œuvre une ou plusieurs solutions pour répondre aux demandes d'accès, de rectification, de suppression des données, de droit à l'oubli, de droit à la portabilité, de limitation des traitements dans vos applications ?	Sauf exception, le GDPR impose un délai maximum d'un mois pour répondre aux demandes d'exercice de leurs droits par les personnes concernées (Art. 12.3).

Florence CHAFIOL, Avocat Associée
Stéphanie LAPEYRE, Avocat
August Debouzy

Les bases légales de traitement

Pour être licite, un **traitement de données à caractère personnel doit respecter l'une des six bases légales fixées** par le GDPR. Il appartiendra alors au responsable de traitement d'identifier, pour chaque traitement, la base légale sur laquelle il se fonde et d'en informer les personnes concernées.

1. **L'exécution d'un contrat** : le traitement sera licite lorsqu'il est véritablement nécessaire dans le cadre de l'exécution d'un contrat ou dans l'intention de conclure un contrat.

2. **Une obligation légale** : le traitement sera licite lorsqu'il est effectué conformément à une obligation légale (législation de l'UE ou de l'Etat du responsable de traitement).

3. **L'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique**.

4. **L'intérêt vital** : le traitement sera licite lorsque l'intérêt vital de la personne concernée ou d'un tiers est en jeu (question de vie ou de mort ou risque d'atteinte à la santé).

5. **L'intérêt légitime** : le traitement sera licite s'il répond à un intérêt légitime poursuivi par le responsable de traitement et que cet intérêt prévaut sur les intérêts ou les droits et libertés des personnes concernées.

6. **Le consentement** : le traitement sera licite s'il repose sur le consentement de la personne concernée. Pour être valide, le consentement doit être :
   - Libre : la personne doit bénéficier d'une véritable liberté de choix (il ne doit notamment pas y avoir de déséquilibre manifeste entre la personne et le responsable de traitement ; un consentement par finalité doit être requis ; enfin, l'exécution d'un contrat ne doit pas être subordonnée à l'obtention du consentement si cela n'est pas nécessaire à une telle exécution).
   - Spécifique : si le consentement est demandé dans un document regroupant plusieurs questions/informations il convient de distinguer la partie relative à la demande de consentement sous une forme aisément accessible et formulée en des termes clairs
   - Eclairé : la personne doit bénéficier des informations nécessaires pour décider en connaissance de cause.
   - Résulter d'un acte positif et univoque : le consentement doit relever d'un comportement actif et sans ambiguïté de la personne (case à cocher par exemple ; en revanche le silence ou tout acte implicite ou passif ne constituent pas un contentement valide).

Le consentement doit pouvoir être retiré à tout moment et la personne doit être informée de cette faculté de retrait. La charge de la preuve de l'obtention du consentement repose sur le responsable de traitement.

CHAPITRE 2

RECOMMANDATIONS ET MESURES À METTRE EN PLACE POUR UN SI CONFORME

Piloté par **Régis DELAYAT**,
Vice-président du CIGREF

Coordonné par **Flora FISCHER**
Chargé de programme de recherche, CIGREF

et
Sophie BOUTEILLER,
IT Governance Officer, SCOR

Avec le concours de **Jean-Sébastien MARIEZ** et **Marie-Mathilde DELDICQUE**, Avocats, De Gaulle Fleurance & Associés.

cigref réussir le numérique

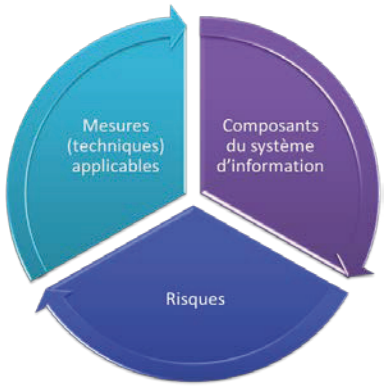
Identifier les mesures à mettre en place pour un SI conforme

Les objectifs du sous-groupe 2 (SG2) sur les « mesures techniques » visent à identifier les impacts des réglementations internationales sur les données personnelles, et du GDPR en particulier, sur les architectures des systèmes d'information (SI) des entreprises**.**

Le groupe de travail n'a pas envisagé la reconstruction d'une architecture SI en place, elle relève de choix d'entreprise et s'inscrit dans l'optimisation de l'opérationnel, et ne doit pas être remise en question du seul fait des réglementations sur les données personnelles. Pour assurer la conformité, **il sera nécessaire de mixer des actions de renforcement « classique » de la sécurité du SI et diverses actions ciblées sur les données** (de type chiffrement, pseudonymisation…). Ainsi, les participants ont travaillé à partir des architectures existantes dans leur organisation, qu'elles soient globales ou délocalisées. Chaque entreprise pourra, en fonction de son propre contexte, adapter et se réapproprier ces inventaires.

Les participants ont d'abord identifié les composants du SI qui génèrent ou véhiculent des données personnelles (messagerie, CRM…), et fait l'inventaire des risques afférents, qu'il s'agisse de risques de sécurité du SI en général, de risques liés à la protection des données personnelles, ou encore de risques liés à la protection des droits des personnes.

Les participants ont ensuite identifié les mesures et recommandations potentiellement applicables en fonction de chaque typologie de risques, pour assurer la conformité du SI.



Les risques par composant du SI ainsi que les mesures et recommandations à mettre en place sont détaillés plus bas dans le document, et dans un fichier Excel joint à ce rapport.

Par ailleurs, au-delà de ce travail d'identification et de partage d'expérience entre les participants, le SG2 a fait intervenir des fournisseurs[9] de solutions logicielles embarquant des données personnelles (RH, CRM, messagerie, etc.), *on-premise* et *SaaS*, pour identifier les mesures techniques proposées en standard ou en option dans leurs offres et informer les participants sur la manière dont ils se préparent eux-mêmes pour être conformes en mai 2018.

A noter, les options de chiffrement proposées par les fournisseurs ne sont en général pas retenues par les clients, d'une part par crainte d'avoir à gérer une complexité croissante d'outils de chiffrement (chaque fournisseur proposant sa solution), d'autre part par crainte de voir les coûts liés au SI augmenter (chaque solution de chiffrement étant une option généralement payante). Certaines entreprises étudient donc la possibilité de développer leur propre outil de chiffrement.

Pour alimenter ses réflexions, le SG2 a également choisi de s'appuyer sur un cas d'usage : le présent document détaille un service de CRM, développé au sein de groupe de travail par Jérôme Capirossi d'UNEXX.

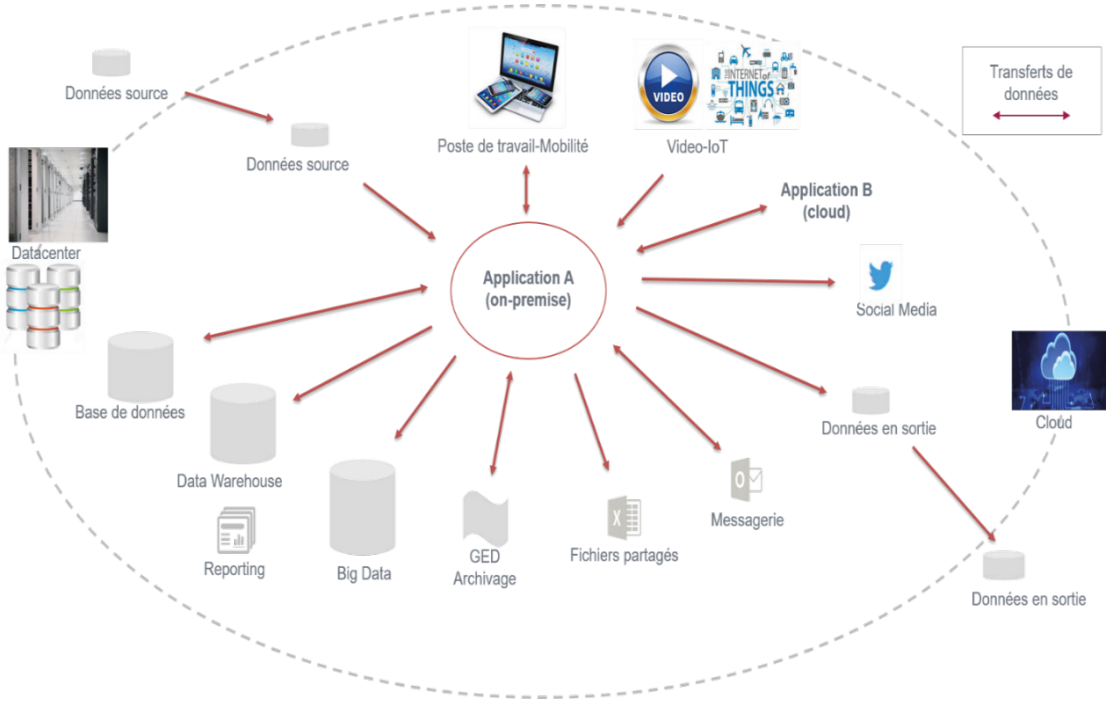
[9] Microsoft, Salesforce et Workday.

Mesures potentiellement applicables sur les SI

Approche « composants SI »

Par « composants du système d'information », il faut comprendre tout ce qui supporte les services et les flux associés : les bases de données, le *Cloud*, les *datacenters*, les postes de travail, l'*IoT* (*Internet of Things*), les messageries, les plateformes de traitement *Big Data*, etc.

Les mesures identifiées visent non seulement à **protéger tous les composants et applicatifs, mais aussi les flux qui existent entre eux** (représentés par les flèches dans le schéma ci-dessous) :



Source : CIGREF, « Données Personnelles et Systèmes d'Information » (2017)

Les types de risques par composants sont répertoriés en annexes.

François CORNELY
Licensing executive
MICROSOFT

Quelles sont les solutions de cybersécurité proposées par Microsoft ?

En termes de cybersécurité, Microsoft s'attache à protéger quatre dimensions essentielles : l'infrastructure, les matériels, les données et les identités :

- **La protection des terminaux** consiste à protéger les appareils, à détecter des activités suspectes. Microsoft peut répondre en bloquant les terminaux, ou *via* :
  - Le chiffrement de données avec *Bitlocker*
  - L'analyse de pièces jointes avec *Advanced Threat Protection*
  - La protection du système Windows contre les menaces sophistiquées avec Windows Defender ATP
- **La protection de l'identité** peut se faire avec diverses solutions **:**
  - Windows Hello (biométrie)
  - Credential Guard
  - Enterprise Mobility and Security : protection de l'identité et accès conditionnel (le système s'auto-adapte avec du machine learning)
- **La protection de la donnée** s'effectue notamment avec : la solution *Azure Information Protection* qui fait de la gestion du chiffrement et de la protection de la donnée à un haut niveau de granularité. Le chiffrement doit suivre le cycle de vie de la donnée. C'est ce que l'on appelle des « droits digitaux ». Microsoft élabore donc des stratégies de chiffrement en fonction du niveau de sensibilité des données.
- **La protection de l'infrastructure :** sur ce point, les solutions proposées par Microsoft permettent :
  - Une visibilité complète, le contrôle et la sécurité des applications SaaS et des ressources Azure
  - La centralisation et la corrélation des logs de sécurité
  - La gestion des secrets et des clefs cryptographiques

Typologie de risques

Une fois les composants SI identifiés, le SG2 a répertorié les risques liés à ces composants (voir annexes – tableau onglet 2). Trois typologies de risques ont été identifiées :

- La sécurité du SI : il faut prendre conscience de la criticité du SI en sa qualité de « berceau des données », comme le formule l'ANSSI dans son Guide d'Hygiène Informatique : Renforcer la sécurité de son système d'information en 42 mesures.
    - Cette typologie de risque soulève des problématiques comme l'intrusion du SI par un *malware,* l'usurpation d'un compte utilisateur ou encore le défaut d'application des mises à jour de sécurité.
- La protection des données personnelles : elle consiste à définir la marche à suivre en cas, par exemple, de défaut de cartographie actualisée des données personnelles et des traitements, de divulgation malveillante de données personnelles, ou encore à décrire les dispositifs de chiffrement et d'anonymisation/pseudonymisation.
- Les droits de la personne : comment garantir le droit à la portabilité, le droit à l'oubli ou tout ce qui a trait à la transparence des traitements, au profilage, à la rétention des données, au consentement, etc. ? Cette catégorie très large a été découpée par grandes familles de risques, et fait l'objet d'un développement détaillé, proposé ci-après par le Cabinet De Gaulle, Fleurance & Associés :
    - La non disponibilité ;
    - Le défaut d'intégrité ;
    - La perte de confidentialité ;
    - L'absence de traçabilité ;
    - Les usages illicites ;
    - La répudiabilité.

Michel BENARD
Urbaniste SI
LES MOUSQUETAIRES

Comment la dimension risque est-elle traitée au sein du Groupement des Mousquetaires ?

Dans la dimension du risque, il faut prendre en compte :

Les différentes catégories de données personnelles, notamment celles dont le traitement demandait jusqu'ici des autorisations spécifiques : données de localisation, données de santé ou génétiques, données liées à des condamnations, etc.

Le volume des données personnelles, c'est-à-dire le nombre de "personnes concernées" stockées dans tel ou tel système informatique, mais aussi circulant dans les flux entre systèmes par unité de temps. Il faut pouvoir anticiper les coûts de notification aux personnes concernées en cas d'atteinte à la sécurité dudit système.

Il est nécessaire de développer également des **vues du SI**, faites selon un point de vue "juridique" : une vue où l'on verrait par exemple les applications et les rôles de "Data Processor" et "Data Controller" qui lui sont liés (pour reprendre le vocabulaire du GDPR), ainsi que la localisation géographique et/ou les acteurs ayant accès aux applications.

Il existe un embryon de cette vue dans le modèle de référence de la commission européenne (EIRA – Legal view).

Mesures applicables et recommandations

Les mesures (techniques, organisationnelles, juridiques) potentiellement applicables aux 3 typologies de risques identifiées précédemment sont détaillées en annexes. Par exemple, voici **une série de mesures proposées pour gérer le risque « Transfert non sécurisé de données personnelles ».**

Composants du SI exposés à ce risque
Cloud
Applications
Base de Données
Datawarehouse
Big Data
GED-Archivage
Fichiers Partagés
Messagerie
Données en sortie

Mesures potentiellement applicables pour se protéger de ce risque
Intégrer les contraintes dès la phase de design (privacy-by-design)
Politique sur les droits et devoirs en matière de sortie des données
Chiffrement et anonymisation
Encadrement contractuel avec le partenaire (NDA, clause de confidentialité, clause de suppression des données…)
Contrôle des accès
Gestion centralisée des logs (SIEM, Security Information Event Management)
EDRM, Enterprise Digital Right Management (Protection bureautique avec chiffrement, watermarking…)
Limitation des accès internet
Interdiction de clés USB (dans certains pays)
Blocage de sites de transferts (type Wetransfer, Dropbox…)
Détection de téléchargements/transferts de fichiers importants
Intégration de données « pièges »
Audit
Sensibilisation/Formation utilisateurs et IT
Filtrage IP des applications multi-tiers

Mesures applicables pour se protéger des risques identifiés

Rappel : les composants SI sont répertoriés dans l'onglet 1 du tableau disponible en annexes et les mesures techniques potentiellement applicables aux risques des 3 typologies de risques sont répertoriées dans l'onglet 2. Le tableau qui suit met en évidence les composants techniques exposés au trois types de risques (Sécurité SI, Protection des données, Droits des personnes). A la suite du tableau sont listées les mesures techniques et recommandations applicables, de manière non exhaustive.

Thierry MATHOULIN, Benjamin ALLOUL, Bernhard VON SONNLEITHNER
WORKDAY

Quels sont les aspects techniques et juridiques de la mise en conformité chez Workday ?

Créé en 2005, Workday, l'un des leaders des applications Cloud de Finance et RH a construit une nouvelle génération d'application Finance et RH en prenant en compte les évolutions technologiques : architecture unique, sécurisée, en mode SaaS, partagée par tous les clients. Workday s'attache à inclure les mesures de protection des données dans tous ses développements d'applications, de processus ou de services qui utilisent des données personnelles afin de rester en conformité avec le GDPR.

- **Aspects juridiques**

Workday agit comme un sous-traitant sur les données personnelles des clients soumises électroniquement dans ses applications en mode « software as a service » (« SaaS »). Dans ce cadre, Workday traite uniquement les données personnelles selon les instructions de ses clients qui demeurent responsables de traitement à tout instant.

Workday propose un accord détaillé et complet *(« Data processing agreement »)* qui définit les engagements contractuels forts de Workday concernant le traitement des données personnelles de ses clients dans le cadre de ses applications SaaS. La société mère de Workday est elle-même certifiée « Privacy Shield frameworks » EU-US et Suisse-US, maintenu par le département du commerce américain. Workday propose également à ses clients de la communauté européenne les clauses contractuelles types afin de légaliser les transferts de données personnelles en dehors de l'Espace Economique Européen.

- **Aspects techniques**

Pour les clients européens, Workday opère deux « datacenters » situés dans l'Espace Economique Européen. Actuellement, le « datacenter » principal se situe à Dublin en Irlande et le « datacenter » secondaire est situé à Amsterdam aux Pays-Bas.

En tant que fournisseur d'une solution SaaS, Workday assure l'intégration de la gestion de l'infrastructure sur laquelle repose son service, l'infrastructure sur laquelle les clients opèrent le service ainsi que la maintenance du service. Les clients sont responsables de la sécurité de leur système d'information et de l'administration de leur environnement applicatif, qu'ils alimentent avec leurs propres données. Workday propose une solution unifiée qui permet aux clients de générer directement leurs reporting. Pour Workday, les données disponibles dans la plateforme restent la propriété de leurs clients.

Concernant la sécurisation, ce sont les clients qui gèrent les authentifications afin de savoir qui se connecte sur la plateforme. Ce sont également les clients qui gèrent le niveau d'accès des collaborateurs aux données. Le cadre, relativement flexible, permet à chaque entreprise de répondre à des besoins spécifiques. L'ensemble des activités des utilisateurs est tracé par Workday, l'ensemble des changements est conservé « ad vitam aeternam ». La traçabilité de la lecture dans le système est également possible.

Typologie 1 : Sécurité SI

Les composants SI concernés par les risques touchant à la sécurité du SI sont les suivants :

Types de Risques	Réseau	Datacenter	Cloud	Workplace	Données source	Video-IoT	Application	Database	DWH	Big Data	GED-Archivage	Fichiers Partagés	Messagerie	Données sortie	Réseaux Sociaux
Sécurité du SI															
Intrusion physique dans le datacenter ou dans les locaux															
Perte ou vol d'un équipement															
Destruction d'un équipement physique, d'un composant software ou de données															
Intrusion extérieure dans le réseau															
Inaccessibilité d'un service															
Infiltration via malware															
Gestion défaillante des droits d'accès															
Usurpation d'identité d'un compte utilisateur															
Usurpation d'un compte administrateur															
Exfiltration de données															
Interception d'échanges															
Défaut d'application des mises à jour de sécurité															
Non détection de vulnérabilités															
Incapacité à tracer un incident ou des accès															
Incapacité à détecter une atteinte aux données															
Défaut de pilotage d'un sous-traitant / fournisseur (IoT)															
Négligence d'un sous-traitant / fournisseur (IoT)															
Intervention frauduleuse d'un sous-traitant															

Les mesures et recommandations sur la typologie de risque « Sécurité SI » sont essentiellement des actions de renforcement de la sécurité globale du SI, elles ne traitent pas directement de la protection des données en elle-même, mais s'attachent à sécuriser le système d'information en tant que « *berceau des données* »[10].

[10] ANSSI, Guide d'Hygiène Informatique : Renforcer la sécurité de son système d'information en 42 mesures

Mesures techniques pour chaque type de risques identifié concernant la Sécurité du SI :

Intrusion physique dans le *datacenter* ou dans les locaux

- Système de contrôle des accès physiques : badge, contrôle identité (scanner biométriques, etc.), accès renforcé pour certains espaces sensibles (salles serveurs fermées, etc…), caméras vidéo-surveillance, alarmes, etc…
- Exigences contractuelles (contrats d'hébergement, partenaires intervenant dans les locaux)
- Chiffrement wifi et accès contrôlé par mot de passe
- Blocage des ports sur les équipements
- Network Access Control (méthode informatique définissant un protocole d'identification pour accéder à un réseau d'entreprise, et prenant en compte les éventuelles restrictions d'usages par identifiants.)

Perte ou vol d'un équipement

- Authentification forte (2-factor, tentatives limitées, mots de passe bios et Windows…)
- Chiffrement des postes et des mobiles (Bitlocker, Mobileiron, etc…)
- Usage limité/contrôlé du BYOD
- Blocage des ports USB
- Effacement à distance des disques des mobiles
- Interdiction de stockage sur disque dur
- Sauvegardes réseau
- Gestion centralisée des configurations
- Procédure de décommissionnement des équipements (serveurs, PC, mobiles…)
- Chiffrement des disques du SAN pour les serveurs

Destruction d'un équipement physique, d'un composant software ou de données

- Contrat de maintenance fournisseur (accès à un équipement similaire, restauration, réversibilité, etc…)
- Sauvegardes adaptées (cycle de vie…)
- Chiffrement de surface
- Sauvegarde des configurations et des procédures de Maintien en Conditions Opérationnelles (MCO)

Intrusion extérieure dans le réseau

- Protection type filtrage internet (BlueCoat, etc…)
- Protection WAF, firewall, reverse proxy
- Limitation des flux
- Segmentation réseau VLAN
- Sécurisation des points d'accès (wifi WPA)
- Filtrage de port des VPN des partenaires externes
- URL et contrôle d'accès nominatif
- IPS

- Blocage des ports
- Utilisation du chiffrement par défaut des communications
- Sauvegarde des logs réseaux
- Mise en place d'un SOC (Security Operation Center)
- Network Access Control

Inaccessibilité d'un service

- Plan de Continuité d'Activité
- Dual data center (actif/actif)
- Haute disponibilité

Infiltration via malware

- Politique de veille éditeurs (système + middleware)
- Patch management
- Anti-malware (et anti-virus)
- Filtrage url et ports
- Passerelles SMTP (ProofPoint)
- Blocage webmail
- Protection contre les menaces réseau avancées (ATP, Advanced Threat Protection)
- Sauvegardes et restaurations
- Sensibilisation des utilisateurs
- Procédure d'alerte en cas d'urgence
- SOC de 3ème génération incluant une analyse d'écart comportemental

Gestion défaillante des droits d'accès

- Outillage d'identification, de classification et de revue des accès
- Attribution automatique des accès (GDI/GDA), et workflow associés
- Security entitlement
- Audit régulier des droits d'accès
- Politique de changement de mots de passe
- Gestion centralisée des logs (SIEM, Security Information Event Management)
- Mise en place d'un SOC
- Mise en place de scénarios d'attaque métier dans les règles du moteur de corrélation (SIEM)

Usurpation d'identité d'un compte utilisateur

- Politique de mots de passe (complexité, changement régulier…)
- Sensibilisation utilisateur
- Norme de flux https/sftp
- Norme sur les cookies et les identifications
- Gestion centralisée des logs (SIEM, Security Information Event Management) (par exemple, détection d'un même compte accédant à plusieurs postes)
- Authentification forte à 2 facteurs

Usurpation d'un compte administrateur

- Comptes "administrateur" (privilèges forts) séparés des comptes "utilisateur" (usage bureautique)
- Contrôle d'accès renforcé
- Politique de mots de passe renforcée
- Outil de gestion des accès et renouvellement automatique sur des comptes génériques (type CyberArk)
- Notification automatique des accès IP suspects
- Gestion nominative des accès administrateurs
- Limitation des administrateurs de domaines au strict minimum, et séparation complète de leurs environnements de travail et de leur environnement d'administration de l'Active Directory
- Utilisation de connexion centralisée et tracée des comptes administrateurs (Bastion type Wallix, Centrify…)
- Revue des comptes administrateurs (et de leurs droits)

Exfiltration de données

- Politique sur les droits et devoirs en matière de sortie des données
- Chiffrement, anonymisation et pseudonymisation
- Anonymisation persistante
- Encadrement contractuel avec le partenaire (NDA - clause de confidentialité, clause de suppression des données…)
- Gestion centralisée des logs (SIEM, Security Information Event Management), et synchronisation des équipements
- EDRM, Enterprise Digital Right Management (protection bureautique avec chiffrement, ou watermarking, qui consiste à cacher un copyright dans un fichier)
- Limitation des accès internet
- Blocage des ports USB pour le transfert de données (clés USB, disques durs externes, téléphones portables, graveurs de CD/DVD/Blueray externes, etc..)
- Blocage de sites de transferts (type Wetransfer, Dropbox…)
- Détection de téléchargements/transferts de fichiers importants
- Intégration de données pièges pour traçabilité de la source de l'exfiltration
- Mise en place d'une politique de DLP (Data Leakage Prevention) et des outils associés

Interception d'échanges

- Protection via des flux sécurisés (TLS/SSL, https, sftp, …)
- Traçabilité des flux (garantie arrivée) (répété qqs lignes après)
- Installation clé WPA sur le réseau wifi
- Chiffrement au niveau applicatif (chiffrement de signature)
- Chiffrement « datacentrique »
- Politique de mots de passe

Défaut d'application des mises à jour de sécurité

- Politique de gestion des patchs
- Outil de contrôle de mise à niveau applicatif, intégrant des scans de vulnérabilité périodiques
- Tests de pénétration avec rapport et plan de remédiation
- Projet de normalisation et gestion de l'obsolescence
- Patchs virtuels (ex. pour simuler les patchs au niveau réseau). IPS (Intrusion Prevention System)
- Déploiement d'un IDS (Intrusion Detection System)
- Automatisation du patching des équipements auprès du fournisseur
- Sensibilisation des équipes techniques
- Dispositifs de contrôle interne (contrôle ad hoc dans le cadre de contrôle interne de l'entité)
- Solution de conteneurisation des applicatifs

Non détection de vulnérabilités

- Test intrusion et scans de vulnérabilité réguliers
- Politique de patching
- Host Intrusion Prevention System (HIPS) pour permettre le patching virtuel des vulnérabilités
- Analyse de qualité de code, et respect standard & normes sécurité (type Fortify)
- Production de normes & standards : master, code, configuration middleware, etc.
- Procédure d'alerte et d'application urgente de patch
- Inventaire ponctuel qui permet de détecter des non conformités et vulnérabilités potentielles
- Veille vulnérabilités
- Sensibilisation utilisateur

Incapacité à tracer un incident ou des accès

- Remontée centralisée des logs et moteurs de corrélation (SIEM)
- SOC
- Service forensic (équipe dédiée pour réponse aux incidents et à la veille)
- Procédure de gestion de crise (pour être efficiente, doit être testée périodiquement, dans son ensemble)

Incapacité à détecter une atteinte aux données

- SIEM : qualification des incidents, contrôle d'intégrité (signature cryptographique, hash, CRC), logs sur les accès aux données
- Audit de sécurité
- Tests d'intrusion
- Sensibilisation à la remontée d'incidents/doutes de compromission
- Veille sur internet pour recherche de traces de compromission ou de revente des données

Défaut de pilotage d'un sous-traitant / fournisseur (IoT)

- Encadrement contractuel (clauses contractuelles types approuvées par la Commission et/ou la CNIL, BCR)
- NDA
- SLA
- Reporting
- Audit physique et logique
- Obtention d'un rapport d'audit d'un tiers de confiance, i.e. un auditeur indépendant attestant la bonne exécution des services (ISAE 3402, SSAE16…)
- Validation des procédures de backup
- Vérification de la bonne gestion/corrélation des logs
- Mise en concurrence
- Bilan de conformité annuel

Négligence d'un sous-traitant / fournisseur (IoT)

- Contrôles préalables à la contractualisation (clauses contractuelles types approuvées par la Commission et/ou la CNIL, BCR)
- Intégration de clauses contractuelles de rupture en cas de négligence
- Revue opérationnelle régulière avec le sous-traitant
- Utilisation de la stéganographie (dissimulation de données dans d'autres données) ou de données pièges pour identifier la source du problème
- Gestion des incidents et notification à l'autorité de contrôle et/ou aux personnes concernées
- Audit régulier sur sous-traitant

Intervention frauduleuse d'un sous-traitant

- Service de fraude avec contrôle et surveillance
- Vérifications de précaution sur la santé financière du sous-traitant
- Encadrement contractuel (clauses contractuelles types approuvées par la Commission et/ou par la CNIL, BCR)
- Contrôle des accès
- VPN partenaire
- Gestion des incidents et notification à l'autorité de contrôle et/ou aux personnes concernées
- Utilisation de la stéganographie, ou insertion de données pièges, pour identifier la source du problème
- Audit régulier du sous-traitant

Typologie 2 : Protection des données

Les composants SI concernés par les risques touchant à la protection des données sont les suivants :

Types de Risques	Réseau	Datacenter	Cloud	Workplace	Données source	Video-IoT	Application	Database	DWH	Big Data	GED-Archivage	Fichiers Partagés	Messagerie	Données sortie	Réseaux Sociaux
Protection des données															
Défaut de cartographie (actualisée) des données (défaut de tenue d'un registre des traitements)															
Localisation non autorisée de données personnelles															
Non respect des réglementations locales (ex. égalité des chances aux US, ...)															
Absence de cloisonnement des données personnelles															
Non respect des règles de rétention des données (durée de conservation)															
Non respect des formalités préalables applicables au traitement															
Transfert non sécurisé de données personnelles															
Transferts non encadrés de données hors UE															
Accès non conforme ou non encadré aux données personnelles															
Propagation malveillante de données personnelles															
Divulgation de données personnelles par inadvertance															
Vol de données															
Perte d'intégrité des données															
Détention ou utilisation abusive de données personnelles															
Détournement de finalité de traitements de données personnelles du fait d'une mauvaise anonymisation															

Reconstitution de l'identité d'une personne et enrichissement de son profil par corrélation entre plusieurs sources internes ou externes (big data)															
Défaut de PIA															
Défaut de privacy by design (absence de règles sur la minimisation des données à celles strictement nécessaires, non-prise en compte)															
Défaut de notification d'une atteinte aux données															

Les mesures et recommandations potentiellement applicables sur la typologie de risque « Protection des données » sont les suivantes :

Défaut de cartographie (actualisée) des données et des traitements (défaut de tenue d'un registre des traitements et/ou des violations de données personnelles)

- Procédure de cartographie/inventaire des données métiers (catégories de données, finalités, destinataires, durée de conservation, types de support, etc…), régulièrement tenu à jour et analysé
- Registre du CIL/DPO (obligatoire)
- Dictionnaire de données (catégories de données : données courantes, données perçues comme sensibles, données sensibles)

Localisation non autorisée de données personnelles

- Information/sensibilisation sur les contraintes de localisation des données dans les pays concernés
- Maîtrise des données et traitements des services concernés
- Déploiement d'une solution de data management
- Revue des contrats des sous-traitants
- Insertion de clauses spécifiques

Non-respect des réglementations locales (ex. égalité des chances aux US, …)

- Sensibilisation/formation des équipes métiers et IT
- Gestion des droits d'accès
- Cartographie des données et des réglementations applicables localement
- Déclaration simplifiée/normale, et autorisation préalable
- Data masking (anonymisation dynamique/ non persistante)
- Non-respect des formalités préalables applicables au traitement en France (déclaration simplifiée, déclaration normale, autorisation préalable de la CNIL exigible jusqu'au 25 mai 2018).

Absence de cloisonnement des données personnelles

- Cloisonnement fonctionnel (logique) et infra dédiée (physique) si nécessaire
- Sensibilisation/Formation des équipes métiers et IT
- Gestion des droits d'accès
- Gouvernance de la donnée interne
- Chiffrement des bases de données

Non-respect des règles de rétention (durée de conservation) des données

- Politique de rétention/conservation des données
- Mise en place d'une gouvernance de la donnée en interne
- Sensibilisation/formation des équipes métiers et IT
- Gestion des droits d'accès
- Mise en place de traitements automatisés de purge
- Gestion des logs
- Audits outillés
- Utilisation de dispositifs de Privacy by Design ou de Privacy by Re-Design
- Intégration de marqueurs des données

Transfert non sécurisé de données personnelles

- Intégrer les contraintes dès la phase de design (privacy-by-design)
- Politique sur les droits et devoirs en matière de transfert interne/externe des données
- Chiffrement et anonymisation
- Encadrement contractuel avec le partenaire (NDA, clause de confidentialité, clause de suppression des données…)
- Contrôle des accès
- Gestion centralisée des logs (SIEM, Security Information Event Management)
- EDRM, Enterprise Digital Right Management (protection bureautique avec chiffrement, ou watermarking qui consiste à introduire un copyright dans un fichier)
- Mise en place d'outils de DLP
- Limitation des accès webmail
- Interdiction de clés USB (dans certains pays)
- Blocage de sites de transferts (type Wetransfer, Dropbox…)
- Détection de téléchargements/transferts de fichiers importants
- Intégration de données pièges (stéganographie)
- Audit
- Sensibilisation/Formation utilisateurs et IT
- Filtrage IP des applications multi-tiers (firewalls applicatifs)
- Mise en place d'une politique de DLP (Data Leakage Prevention) et des outils associés
- Gestion des incidents et notification à l'autorité de contrôle et/ou aux personnes concernées

Transferts non encadrés de données hors UE

- Définition et validation officielle de règles contraignantes d'entreprise (ou Binding Corporate Rules - BCR)
- Clauses contractuelles types
- Accord explicite et éclairé des individus
- Marquage et traçabilité des données
- Contrôle des accès

Accès non conforme ou non encadré aux données personnelles

- Politique de gestion des habilitations, de gestion des accès, et de gestion des identifications
- Sensibilisation utilisateur et IT
- Audits réguliers
- Cloisonnement des données
- Gestion des incidents et notification à l'autorité de contrôle et/ou aux personnes concernées

Propagation malveillante de données personnelles

- Veille sur internet (web, réseaux sociaux, Dark Web ou Black Market)
- Chiffrement, pseudonymisation, anonymisation
- Intégration de données pièges (fingerprinting)
- Contrôle des accès
- Gestion des logs
- Audits
- Politiques et moyens de prévention, détection, alerte, data breach, et réaction
- Tests d'activation de la cellule de crise
- Gestion des incidents et notification à l'autorité de contrôle et/ou aux personnes concernées

Divulgation de données personnelles par inadvertance

- Sensibilisation utilisateur et IT
- Politique d'utilisation des réseaux sociaux
- Contrôle des accès
- Gestion des logs
- Audit
- Filtrage IP des applications multi-tiers
- Notification immédiate (lorsque nécessaire) à l'autorité de contrôle et/ou aux personnes concernées
- Transmission sécurisée des données (flux chiffrés)

Vol de données

- Mesures de sécurité du SI
- Politique de gestion des demandes de rançon

- Politique de notification (dont formulaire CNIL de notification)
- Politique de gestion de crise
- Cloisonnement des équipements
- Contrôle des accès
- Chiffrement base de données
- Chiffrement disques
- Blocage des ports USB
- Blocage des sites de transfert
- Veille sur les marchés clandestins (Dark web / Black Market)
- Validation contractuelle
- EDRM
- Gestion et corrélation des logs (mise en place d'un SIEM)
- Filtrage IP des applications multi-tiers
- Gestion des incidents et notification à l'autorité de contrôle et/ou aux personnes concernées
- Politique de changement des mots de passe
- Procédure d'inforensic

Perte d'intégrité des données

- Sauvegardes et tests réguliers des sauvegardes
- Gestion et corrélation des logs
- Système de détection précoce d'atteinte volumétrique (cryptolocker)
- Traçabilité des actions sur les services (logs applicatifs)
- Audits
- Contrôle d'intégrité (CRC, signature cryptographique…)
- Test du bon fonctionnement des applications
- Qualification des incidents utilisateurs
- Gestion des incidents et notification à l'autorité de contrôle et/ou aux personnes concernées

Détention ou utilisation abusive de données personnelles

- Contrôle des accès (validation de la demande, séparation des tâches, revue des accès…)
- Sensibilisation/formation utilisateurs et IT
- Alignement entre données détenues et finalité du traitement
- Politique de rétention des données
- Gestion et corrélation des logs
- Encadrement contractuel
- Mesures de traçabilité, audit, notification
- Gestion des incidents et notification à l'autorité de contrôle et/ou aux personnes concernées

Détournement de finalité de traitements de données personnelles du fait d'une mauvaise anonymisation

- Inventaire des traitements de données personnelles

- Intégration de la privacy-by-design dans la méthodologie projet
- Déclaration des traitements
- Minimisation des données (privacy by design)
- Implication du délégué à la protection des données (CIL/ DPO) dans les projets
- Gestion des incidents et notification à l'autorité de contrôle et/ou aux personnes concernées

Reconstitution de l'identité d'une personne et enrichissement de son profil par corrélation entre plusieurs sources internes ou externes (Big Data)

- Anonymisation permanente
- Audit de la robustesse de l'anonymisation (exemple de techniques d'anonymisation : évaluation k-anonymat, L-diversité, t-proximité)
- Utilisation de données agrégées ou généralisées
- Pas de données personnelles dans les traitements de Big Data
- Sensibilisation/formation utilisateurs
- Limitation et contrôle des accès aux données personnelles
- Mise en place d'une charte éthique spécifique
- Traçabilité et audit

Défaut de PIA/ EIVP

- Intégration du PIA dans la méthodologie projet
- Méthodologie PIA/ EIVP (dont analyse de risque)

Défaut de privacy by design (absence de règles sur la minimisation des données à celles strictement nécessaires et/ou non application des règles sur la minimisation)

- Politiques de sécurité et charte utilisateur du SI
- Intégration des équipes Sécurité dans les projets
- Formation des équipes
- Déploiement d'exigences de bonne pratique Privacy by Design (minimisation, accès strictement nécessaires…)
- Politique de minimisation des données (privacy by design)
- Vérification de la privacy-by-design dans les phases de recettes
- Intégration d'une procédure de "Privacy by Re-Design" (gestion des évolutions)

Défaut de notification d'une atteinte aux données

- Procédure de qualification des incidents de sécurité
- Procédure de notification précisant notamment quand une notification est nécessaire et à qui (à l'autorité de contrôle, à la personne)
- Suivi et évaluation des conséquences
- Implication du délégué à la protection des données (CIL/ DPO)
- Formation des équipes

Typologie 3 : Droits des personnes

Les composants SI concernés par les risques liés au respect des droits des personnes sont les suivants :

Types de Risques	Réseau	Datacenter	Cloud	Workplace	Données source	Video-IoT	Application	Database	DWH	Big Data	GED-Archivage	Fichiers Partagés	Messagerie	Données sortie	Réseaux Sociaux
Droits de la personne															
Incapacité à répondre aux droits des personnes (exécution des droits)															
Information															
Transparence du traitement															
Preuve du consentement															
Retrait du consentement (opposition ou suppression)															
Respect de la limite du traitement															
Accès															
Rectification															
Effacement															
Portabilité															
Profilage															
Données des mineurs															

Un focus fort au sein du groupe de travail a été fait sur le respect des droits de la personne, en ligne avec le GDPR qui place l'individu au centre des préoccupations. Le droit des personnes est en effet renforcé notamment autour des droits à l'accès, à l'oubli, à la portabilité, et cela nécessite une approche globale (à la fois sur la gouvernance, la sensibilisation, les aspects techniques de durée de conservation, de traçabilité, de traitements des données, etc.). Les recommandations proposées pour la typologie de risque « Droits des personnes » sont les suivantes :

Incapacité à répondre aux droits des personnes (exécution des droits) :

- L'exécution des droits de la personne impose avant tout de bien savoir authentifier le demandeur. L'entreprise a 2 mois pour répondre à la demande. Un registre centralisé des données personnelles doit être détenu/accessible par le DPO
- Intégration des obligations du droit des personnes dès la conception des nouveaux services (privacy-by-design). Prévoir aussi de le faire à l'occasion d'un privacy-by-re-design pour les services legacy sensibles (éventuellement via des procédures manuelles de contournement…)

- Politique pour les services existants dans lesquels la réponse aux droits des personnes n'a pas été prévue à l'origine
- CIL/DPO, point de contact unique, et instructions pour le contacter
- Accès libre-service pour une partie des informations, possibilité de rectification
- Catégorisation des traitements
- Rationalisation du processus de recueil et mise à jour des consentements
- Traçabilité des consentements
- Limitation du traitement
- Limitation de la durée de conservation
- Purges automatisées, ou alertes avant atteinte de la limite rétention
- Outil de text mining sémantique (détection des termes sensibles ou injurieux / champs commentaires)
- Règles des possibilités de profilage
- Politique de non-référencement des mineurs (sauf consentement formel et tracé des parents)

Information (clarté sur les politiques de confidentialité, les objectifs de collecte, les conditions générales de vente, à valider via une case à cocher…)

- Politique de confidentialité et protection des données à caractère personnel (comprenant les informations sur l'identité et les coordonnées du RP, les coordonnées du DPO, la nature des données collectées, les finalités, la durée de conservation, les destinataires, les éventuels transferts vers des pays tiers, etc.)
- Information par un message au moment de la collecte des données (nature des données collectées, finalités, destinataires, comment exercer ses droits d'accès, d'opposition et de modification des données, etc.); par exemple, sur internet via un message facilement accessible sur le site; salarié: dans son contrat de travail, etc.

Transparence du traitement :

- Information de la personne concernée de la nature des données collectées et des finalités de traitement, identité du RP, etc.

Preuve du consentement

- Vérifier si le traitement ne repose pas sur une autre base légale que le consentement (obligation légale, sauvegarde de la vie, mission de service public, contrat ou mesures prises avec la personne, intérêt légitime)
- S'assurer que le traitement ne puisse pas être mis en œuvre sans consentement
- S'assurer que le consentement sera obtenu de manière libre
- S'assurer que le consentement sera obtenu de manière éclairée et transparente quant aux finalités du traitement
- S'assurer que le consentement sera obtenu de manière spécifique à une finalité
- En cas de sous-traitance, encadrer les obligations de chacun dans un document écrit, explicite et accepté des deux parties
- Pour un site internet : opt-in; cookies (avec un bandeau); email récapitulatif
- Pour un salarié ou un partenaire commercial : contrat signé

Retrait du consentement (opposition ou suppression)

- Vérifier que le traitement ne fait pas l'objet d'une exception interdisant à la personne de s'opposer au traitement (obligation légale, exclusion dans l'acte portant création du traitement)
- Déterminer les moyens pratiques qui vont être mis en œuvre pour permettre l'exercice du droit d'opposition. Ce droit doit pouvoir être exercé le plus rapidement possible, sans jamais excéder deux mois, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches à effectuer ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais.
- Exemple : pour un site internet, créer un formulaire, facilement accessible, avec des cases à décocher (dit « opt-out ») ou prévoir la possibilité de se désinscrire d'un service (suppression de compte).
- Vérifier que les demandes d'exercice du droit d'opposition faites par voie postale sont signées et accompagnées de la photocopie d'un titre d'identité (qui ne devrait pas être conservée sauf en cas de besoin de conserver une preuve) et qu'elles précisent l'adresse à laquelle doit parvenir la réponse.
- Vérifier que les demandes d'exercice du droit d'opposition faites par voie électronique (en utilisant un canal chiffré si la transmission se fait via Internet) sont accompagnées d'un titre d'identité numérisé (qui ne devrait pas être conservé sauf en cas de besoin de conservation d'une preuve, et ce, en noir et blanc, en faible définition et sous la forme d'un fichier chiffré).
- S'assurer que le motif légitime des personnes exerçant leur droit d'opposition est fourni et apprécié
- S'assurer que tous les destinataires du traitement seront informés des oppositions exercées par des personnes concernées

Respect de la limite du traitement

- Vérifier que le ou les motifs pour lesquels l'effacement est demandé s'appliquent :
    - L'exactitude des données à caractère personnel est contestée par la personne concernée, pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel ;
    - Le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation ;
    - Le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ;
    - La personne concernée s'est opposée au traitement, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée
- Déterminer les moyens pratiques qui vont être mis en œuvre pour permettre l'exercice du droit de limitation. Ce droit doit pouvoir être exercé le plus rapidement possible, sans jamais excéder deux mois pour des données, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais excédant le coût de la reproduction

Accès

- Déterminer les moyens pratiques qui vont être mis en œuvre pour permettre l'exercice du droit d'accès. Ce droit doit pouvoir être exercé le plus rapidement possible, sans jamais excéder deux mois pour des données, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais excédant le coût de la reproduction
- Vérifier que les demandes d'exercice du droit d'accès faites sur place permettent de s'assurer de l'identité des demandeurs et des personnes qu'ils peuvent mandater
- Vérifier que les demandes d'exercice du droit d'accès faites par voie postale sont signées et accompagnées de la photocopie d'un titre d'identité (qui ne devrait pas être conservée sauf en cas de besoin de conserver une preuve) et qu'elles précisent l'adresse à laquelle doit parvenir la réponse
- Vérifier que les demandes d'exercice du droit d'accès faites par voie électronique (en utilisant un canal chiffré si la transmission se fait via Internet) sont accompagnées d'un titre d'identité numérisé (qui ne devrait pas être conservé sauf en cas de besoin de conservation d'une preuve, et ce, en noir et blanc, en faible définition et sous la forme d'un fichier chiffré)
- S'assurer de la possibilité de fournir toutes les informations qui peuvent être demandées par les personnes concernées, tout en protégeant les DCP des tiers
- S'assurer que l'identité des demandeurs et que la légitimité des limitations demandées seront vérifiées
- S'assurer qu'une confirmation sera fournie aux demandeurs.
- S'assurer que les tiers à qui des données auraient été transmises seront informés des demandes de limitation

Rectification

- Vérifier que le traitement ne fait pas l'objet d'une exception (exemple : sûreté de l'État, défense ou sécurité publique)
- Déterminer les moyens pratiques qui vont être mis en œuvre pour permettre l'exercice du droit de rectification. Ce droit doit pouvoir être exercé le plus rapidement possible, sans jamais excéder deux mois, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches à effectuer ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais
- S'assurer que l'identité des demandeurs et que la véracité des rectifications demandées seront vérifiées
- S'assurer qu'une confirmation sera fournie aux demandeurs
- S'assurer que les tiers à qui des données auraient été transmises seront informés des rectifications faites

Effacement, droit à l'oubli

- Vérifier que le ou les motifs pour lesquels l'effacement est demandé s'appliquent. Cela peut concerner les cas où :
    - Les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;
    - La personne concernée retire le consentement sur lequel est fondé le traitement, et il n'existe pas d'autre fondement juridique au traitement ;
    - La personne concernée s'oppose au traitement et il n'existe pas de motif légitime impérieux pour le traitement ;
    - Les données à caractère personnel ont fait l'objet d'un traitement illicite
    - Les données à caractère personnel doivent être effacées pour respecter une obligation légale, etc.
- Déterminer les moyens pratiques qui vont être mis en œuvre pour permettre l'exercice du droit d'effacement. Ce droit doit pouvoir être exercé le plus rapidement possible, sans jamais excéder deux mois, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches à effectuer ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais
- S'assurer que l'identité des demandeurs et que la légitimité de l'effacement demandé seront vérifiées
- S'assurer qu'une confirmation sera fournie aux demandeurs
- S'assurer que les tiers à qui des données auraient été transmises seront informés des demandes d'effacement

Portabilité

- Vérifier que le traitement ne fait pas l'objet d'une exception (exemple : missions d'intérêt public ou relevant de l'exercice de l'autorité publique).
- Déterminer les moyens pratiques qui vont être mis en œuvre pour permettre l'exercice du droit à la portabilité. Ce droit doit pouvoir être exercé le plus rapidement possible, sans jamais excéder deux mois, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches à effectuer ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais
- S'assurer que l'identité des demandeurs et que la légitimité de la portabilité demandée seront vérifiées
- S'assurer qu'une confirmation sera fournie aux demandeurs
- S'assurer que les tiers à qui des données auraient été transmises seront informés de la portabilité faite

Profilage

- Vérifier que le traitement ne fait pas l'objet d'une exception (exemple : le profilage est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement, consentement explicite, etc.)
- Déterminer les moyens pratiques qui vont être mis en œuvre pour permettre l'exercice du droit à s'opposer au profilage. Ce droit doit pouvoir être exercé le

plus rapidement possible, sans jamais excéder deux mois, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches à effectuer ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais

Données des mineurs

- Vérifier l'âge du mineur (si + ou - de 16 ans). Si - de 16 ans, le traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant

Les pratiques et recommandations formulées précédemment (qui n'ont pas vocation à être exhaustives) sont suffisamment génériques pour pouvoir être déclinées dans chaque entreprise, selon leur degré d'avancement en matière de protection du SI et des données personnelles.

Rappelons que la protection des données personnelles est transversale à toute l'entreprise, et impose une réelle gouvernance, devenue incontournable avec le GDPR.

S'il fallait retenir un point, on pourrait dire que tout l'intérêt de ce travail d'inventaire repose sur la capacité de l'entreprise à traiter ensemble les risques de cybersécurité et de privacy, en étant à la fois dans une démarche de prévention, de détection des risques, et de réaction (c'est-à-dire mise en œuvre d'un plan d'action méthodique, pour savoir répondre à l'ensemble des événements de manière efficace et rapide –l'obligation de notification de faille est une bonne illustration de réaction).

Mylène JAROSSAY
Chief Information Security Officer
LVMH

Quelle approche LVMH a privilégié dans sa mise en conformité avec le GDPR ?

L'approche sur les données personnelles est orientée vers une logique de Security and privacy by design dans les projets. L'idée est de faire converger les approches sécurité et privacy au niveau des processus et des outils, car si les risques ne sont pas examinés sous le même angle dans les deux cas, ils conduisent généralement à la mise en œuvre de solutions communes.

Cette approche est soutenue par une formation destinée aux chefs de projets, intégrant des analyses de risques et des études d'impact sur la vie privée pour les projets qui le requièrent.

Elle repose également sur la formalisation d'une politique de sécurité vis-à-vis des fournisseurs tiers, politique sur laquelle les tiers doivent s'engager dès l'étape de consultation.

En termes de mesures techniques de sécurité, des moyens de protection sont à étudier, mais également des mesures de surveillance et de détection, en complément ou lorsque les mesures de prévention ne sont pas ou ne sont que partiellement applicables

Le GDPR va nécessiter de mettre en place des solutions de chiffrement. Il faudra alors soit choisir les outils proposés nativement par les éditeurs en complément de leur offre applicative, soit se doter de solutions transverses de type CASB pour pouvoir traiter le chiffrement de données de plusieurs applications du Système d'Information et garder le contrôle sur ce chiffrement.

LIEN CEULEMANS
Senior Director, Legal - EMEA Privacy,
Salesforce

La responsabilité des fournisseurs en matière de conformité GDPR : un exemple avec Salesforce

La protection des données à caractère personnel est une responsabilité partagée entre Salesforce et ses clients. A cette fin, Salesforce s'engage à respecter les obligations issues du GDPR dans la fourniture de ses services. Salesforce se tient également prête à assister ses clients dans leurs efforts de mise en conformité avec le GDPR.

En ce qui concerne les relations avec les sous-traitants, Salesforce met à disposition de ses clients et prospects pour chaque service proposé, la liste des sous-traitants auxquels Salesforce peut faire appel. Cette liste comprend notamment l'identité du sous-traitant, l'activité de traitement sous-traitée (par exemple, hébergement des données, support client...) et la localisation du sous-traitant.

Salesforce propose à ses clients un mécanisme de souscription à des notifications préalables en cas de nouveaux sous-traitants. Un client pourra ainsi s'opposer au recours par Salesforce à un nouveau sous-traitant en avertissant Salesforce promptement par écrit et aura la possibilité in fine de mettre un terme au service concerné si aucune solution alternative n'est trouvée.

Par ailleurs, Salesforce met à disposition de ses clients et prospects sa Documentation "Trust and Compliance" dans laquelle Salesforce décrit l'architecture et l'infrastructure des services, les audits et les certifications liés à la sécurité et à la confidentialité des données, les contrôles administratifs, techniques et physiques mis en place par Salesforce.

Dans le cadre de transferts de données vers des pays n'offrant pas un niveau de protection adéquat, Salesforce s'assure du respect de la réglementation applicable et du niveau de protection des données à caractère personnel en s'appuyant sur ses BCR (Binding Corporate Rules) pour sous-traitants, sur le Privacy Shield et sur les clauses contractuelles types de la Commission européenne.

[Salesforce a récemment publié plusieurs communiqués et documents sur le GDPR à destination du public, disponibles sur le site Internet de Salesforce : https://www.salesforce.com/campaign/gdpr/]

Illustration concrète de l'approche par le cas CRM

Par **Jérôme CAPIROSSI**
General Manager, UNEXX
Auteur de *Architecture d'Entreprise*

Objectifs du cas

Ce cas d'application a pour objectif d'illustrer la mise en œuvre de la démarche du livre blanc. Il ne prend en compte qu'une partie de l'activité « Gestion de la Relation Client » GRC, ou CRM en anglais, d'une entreprise fictive, et encore, de façon simplifiée, afin de le rendre accessible à un non spécialiste.

L'intérêt de l'activité de CRM est qu'on la trouve dans quasiment toutes les entreprises, et qu'elle soulève des questions typiques relatives à la mise en conformité avec le Règlement Général sur la Protection des Données, ou GDPR en anglais.

De par sa simplicité, ce cas ne constitue pas une recommandation formelle de démarche d'application, son seul but est d'illustrer les recommandations du livre blanc. Il permet notamment de se figurer l'importance et de l'impact de la GDPR sur l'organisation et les systèmes d'information afin de prévoir et de lancer les chantiers utiles et nécessaires.

Contexte du cas

Entreprise : **B-AS-USUAL**

Business : Vente et Maintenance de copieurs-scanners-imprimantes

Chiffre d'Affaire : **360 M€**

Nombre d'employés : **1 200 personnes**

La future mise en application du GDPR préoccupe le comité de direction de **B-AS-USUAL** dont la performance repose sur une prospection active de son Marché et sur un service toujours à l'écoute de ses clients.

Le cœur de la stratégie de **B-AS-USUAL** est le digital. L'entreprise a lancé plusieurs initiatives stratégiques afin de développer des canaux de communication intuitifs et rapides avec ses clients. Elle avait pour objectif de rendre la prise de commande et la livraison les plus fluides possibles, avec une attention toute particulière à l'expérience client.

Le principal facteur de succès de cette stratégie est la confiance du client.

Dans la ligne de cette stratégie, **B-AS-USUAL** veut montrer qu'elle est digne de la confiance que lui font ses clients et veut gagner celle de ses prospects. Elle se donne comme objectif non seulement de se mettre en conformité avec le GDPR, l'organisation et les systèmes de gouvernance de données personnelles, mais également de démontrer que la confiance qu'elle réclame de la part de ses clients, est méritée.

Pour cela, **B-AS-USUAL** souhaite réaliser une première étude d'impact pour identifier les chantiers qui devront être lancés. Elle débute son étude par le domaine CRM. C'est l'objet du cas.

Démarche

La démarche d'application illustrée par le cas, bien que simple, s'inspire des bonnes pratiques d'évaluation des risques, comme la méthode MEHARI.

Elle ne remplace pas un PIA[11] qui doit être envisagé pour certains traitements, lorsqu'ils sont nouveaux ou critiques.

Lors de **la phase 1** on identifie les systèmes, les données personnelles et leurs usages, ainsi que les traitements.

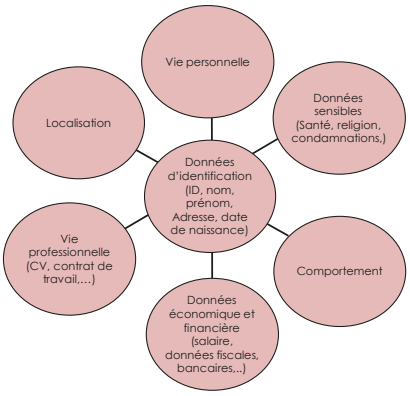
Lors de **la phase 2**, en analysant les éléments fournis par la phase 1, on identifie les risques en tenant compte des spécificités du business de l'entreprise.

Pendant **la phase 3** on définit les mesures et les actions qui vont maîtriser, et minimiser l'impact des risques.

PHASE 1 : identification des données personnelles

Selon leur objet les données personnelles peuvent être catégorisées. Chaque catégorie correspond à un risque spécifique, et par conséquent, être soumise à une régulation spécifique, au-delà du RGDP, telles les données sensibles portant sur la religion, la santé, le casier judiciaire…

En tenant compte de la multitude des données, fréquemment gérées par les systèmes d'information et les processus métier, faire un inventaire complet des données personnelles est une gageure.



Source CIGREF « Economie des données personnelles » (2015)

PHASE 2 : Identifier les risques

L'identification des risques est réalisée en 2 étapes :

- Etape 1 : Les risques provenant d'usages spécifiques à l'entreprise des données personnelles.

[11] Privacy Impact Assessment

- Etape 2 : Les risques communs à toutes les données personnelles liés à l'efficacité de la cybersécurité de l'entreprise
  -

Les risques sont qualifiés au regard de leurs impacts et de leurs probabilités de réalisation. Des risques avec des probabilités très faibles et des impacts importants, doivent être considérés.

PHASE 3 : Définir les mesures et réaliser le plan d'action

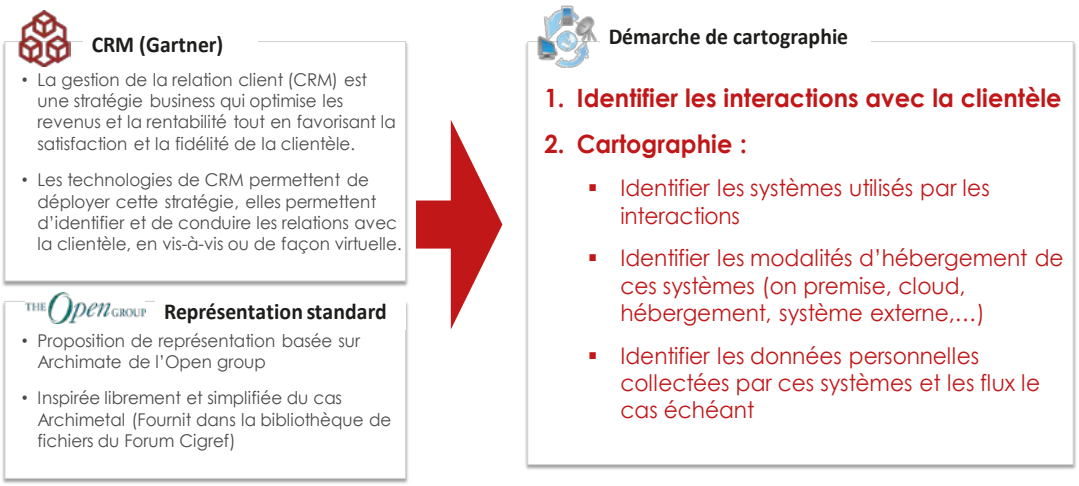
Le plan d'action permet de projeter dans le temps les mesures organisationnelles et techniques qui vont minimiser, détecter, prévenir les risques identifiés à l'étape précédente. Les mesures sont classées comme obligatoires ou souhaitables afin d'établir le plan d'action de court terme, constitué des mesures obligatoires sur les risques critiques et de long terme, comprenant les mesures souhaitables.

PHASE 1 : identification des données personnelles et des systèmes

La CRM couvre toutes activités de l'entreprise qui entrainent un contact avec le client ou le prospect. Ce sont typiquement : la prospection, la vente, le service après-vente. Menées sur plusieurs canaux, avec une exigence de cohérence et d'expérience homogène pour le client, la CRM peut rapidement s'avérer complexe.

Il s'agit dans cette phase d'établir une cartographie des données personnelles et des systèmes qui en assurent les traitements. La démarche de cartographie proposée s'appuie sur une approche standard, diffusée et soutenue par l'OpenGroup : Archimate[12]. Cette démarche flexible, permet de ne mobiliser que les concepts utiles au point de vue que l'on souhaite développer et analyser, dans notre cas, il s'agit des liens entre métier, fonctions, systèmes et données personnelles.

Pour la GDPR, an a défini un point de vue simple qui peut se greffer sur une cartographie d'entreprise et en réutiliser les concepts existants.



[12] Voir références

Les activités de la CRM

Lorsqu'on parcourt les activités de la CRM, on distingue principalement deux acteurs externes à l'entreprise : les suspects et les clients. Chacun d'eux adopte des rôles spécifiques suivant les interactions qu'il mène avec l'entreprise.

- **Le suspect**

Un suspect n'a pas encore montré d'intérêt pour une offre de l'entreprise. Pour une grande partie d'entre eux, l'entreprise n'a même pas suffisamment de données pour établir si la probabilité de manifester un intérêt n'est pas nulle. L'entreprise doit enrichir les données qu'il possède à son sujet et affiner la qualification. Généralement les suspects sont obtenus par achat de fichiers de données.

Plus qu'un rôle, le suspect doit atteindre un état, dans notre cas, « qualifié » qui lui permettra de devenir prospect, ce qui le rendra cible d'une prospection, d'où le rôle « à qualifier ». Pour cela, un suspect mobilise les services métier « Se procure les suspects » et « Qualifie les données »

- **Les clients et les prospects**

Les prospects réunissent les suspects qualifiés et les clients que l'entreprise souhaite prospecter dans le cadre d'activités de cross-selling ou d'up-selling13, par exemple. Pour ses prospects, l'entreprise active le service « Proposer un produit ». S'il manifeste un intérêt au point de vouloir acheter le produit, le client ou le prospect prend le rôle d'« acheteur » et active le service métier « vend un produit ». Et ainsi de suite, s'agissant des autres rôles et services. Vis-à-vis du service « vend un produit », client et prospect ne seront pas traités de la même façon, de même que, généralement, ils ne feront pas l'objet de mêmes offres, vis-à-vis du service « Proposer un produit »

- **Questions relatives aux données personnelles**

A ce stade de la cartographie, on doit s'interroger sur le caractère légitime du traitement des données personnelles que réalise l'entreprise. La question du traitement légitime requiert un travail préalable de l'entreprise dont le résultat est consigné dans la politique des données personnelles. Cette politique permet aux responsables de traitement de l'entreprise d'identifier leurs obligations vis-à-vis de la conformité au GDPR. Au regard de sa politique des données personnelles, B-AS-USAL convient que les services métiers : « Se procure les suspects », « Qualifie les données » et « Proposer un produit », ne sont pas légitimes. Ils doivent être conformes au GDPR. Ne le sont pas davantage, « Enquête de qualité » et « gérer le compte de fidélité ».

Cependant, conformément à sa stratégie, B-AS-USAL souhaite faire une revue du niveau de sécurité des services légitimes, afin de s'assurer des failles de confidentialité à propos des données personnelles de ses clients.

---

[13] Cross-selling, c'est vendre une nouvelle offre à un client existant, up-selling, c'est vendre une option supplémentaire, ou de gamme supérieure, à l'offre que le client possède déjà

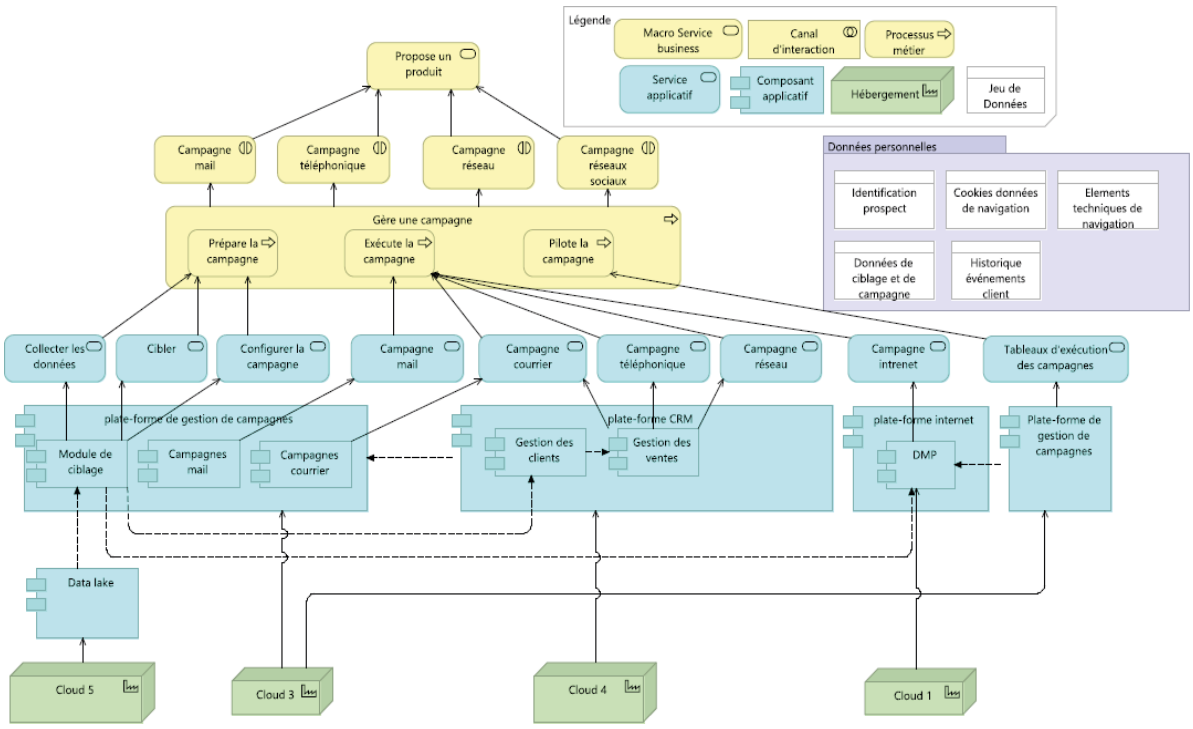
- **Cartographie des services métier des clients liés aux campagnes marketing**

Dans le cadre du cas d'application, on ne développe que le service « Proposer un produit ».

Identification des systèmes

Le service métier « Proposer un produit » permet d'exécuter le plan Marketing de l'entreprise. Celui-ci, outre des opérations de communication et de publicité, définit des campagnes de sollicitation des prospects. Enfin, elle pilote opérationnellement les remontées et les ventes générées, elle peut réajuster certaines campagnes au regard des remontées, les réajustements internet, grâce à la DMP, interviennent immédiatement.

Identification des systèmes



- **Identification des traitements**

Le service métier « Propose un produit » fait partie du traitement CRM sous la responsabilité de l'entreprise. Selon la politique de gouvernance des données personnelles, ce n'est pas un traitement légitime. Il faut noter que plusieurs campagnes téléphoniques sont sous-traitées à un prestataire externe. Elles nécessitent de mettre en place un dispositif particulier pour permettre au responsable de traitement d'assurer ses obligations vis-à-vis des données personnelles des prospects.

- **Identification des données**

Données	Description	Classification	Macro-service applicatifs
Identification prospect	Le prospect est un contact qualifié dont on sait évaluer l'intérêt pour une offre Un prospect est aussi un client	Données d'Identification	Collecter les données Cibler Campagne email Campagne courrier Campagne téléphonique Campagne réseau Campagne internet
Données de navigation	Historique de navigation du prospect client	Données de comportement	Campagne internet
Données de ciblage du prospect	Données de description du Client ou du prospect (CSP, date dernier achat, montant, etc..)	Données de comportement	Collecter les données Cibler
Données techniques de navigation	Ce sont les adresses IP, cookies et autres données collectées lors des échanges entre serveurs et navigateur mobile	Données d'identification	Campagne internet
Historique des événements clients	Collecte les retours des prospects et les archives s'agissant de clients	Données de comportement	Campagne email Campagne courrier Campagne téléphonique Campagne réseau Campagne internet

On remarque que bien que les données clients sont issues d'un traitement légitime, dans ce cas elles sont utilisées dans un traitement non légitime, l'entreprise doit donc se mettre en conformité avec le règlement européen.

PHASE 2 : identifier les risques liés aux données personnelles

La cartographie permet d'avoir une vue d'ensemble des liens opérationnels entre données et traitements, ainsi que de mettre en avant les caractéristiques intéressantes pour la gestion des données personnelles.

Le premier paragraphe décrit l'analyse des risques spécifiques, liés aux jeux de données personnelles. On a choisi les données d'identification prospect/client, car, si elles ne présentent pas comme les données de santé des risques majeurs de non-conformité, elles se situent à la limite et permettent ainsi d'illustrer certaines particularités.

Le second paragraphe identifie les risques de confidentialité sur la base du référentiel de l'ANSSI tel que le préconise le livre blanc, complété par les risques propres aux données et ceux découlant de la non-conformité au droit à l'information.

Risques spécifiques aux jeux de données

La première opération consiste à identifier les données personnelles qui présentent un risque spécifique. Ces données sont celles qui entrent dans le périmètre d'un traitement non légitime. A titre d'exemple, la matrice ci-dessous rapporte les jeux de données identifiés dans la cartographie.

Ni le service « Sourcing et qualification des suspects », ni celui « Proposer un produit » n'ont été considérés comme traitements légitimes. Il s'ensuit que les données associées à ces traitements sont soumises au GDPR. D'autre part, le service « Vend un produit » est légitime, selon la politique de données personnelles. Cependant, certaines données qu'il collecte, n'entrent pas dans le caractère légitime du traitement. Ces données sont également soumises au GDPR.

Données	Gestion des suspects	Prospection	Vente
Identification prospect		x	
Données de navigation		x	x
Données de ciblage du prospect		x	x
Données techniques de navigation		x	x
Historique des événements clients		x	

Une fois que les jeux de données présentant des risques spécifiques sont identifiés, il faut entrer dans le détail et identifier les risques. Cela peut être réalisé en utilisant le « framework » des risques de données personnelles présenté par le livre blanc et en l'appliquant à chaque jeu de données. A titre d'exemple, ce travail d'analyse donne lieu à l'établissement d'une fiche par jeu de données.

Risques de confidentialité des données personnelles

Le livre blanc montre bien que l'exigence de base, avant toute exigence spécifique, est une maturité suffisante de la cybersécurité de l'entreprise. En effet, sans répondre à cette exigence de maturité, il sera difficile pour l'entreprise d'assurer la confidentialité, l'intégrité et la disponibilité de ses données personnelles. L'audit de cybersécurité est réalisé en utilisant le « framework » décrit dans le livre blanc. Ce Framework concerne l'ensemble du Système d'Information, et motivera la mise en œuvre de mesures globales. Il permet de juxtaposer 3 dimensions : le droit à la personne, les risques SI avec impacts sur les données inspirés du Framework de l'ANSSI, les risques de données.

Risques SI avec impact sur les données	Fréquence	Gravité
Perte ou vol d'un PC Portable ou support de stockage		
Exfiltration de données	1	3
Infiltration via malware		
Vol de disque physique		
Vol au travers d'écoutes réseau		
Vol au travers d'opérations de branchement (principalement lié au SAN)		
Vol par un Administrateur Système, File Server ou DBA	2	4
Vol d'emails par phishing et usurpation d'identité		
Vol d'emails par un administrateur	2	4
Usurpation d'identité d'un compte utilisateur		
Usurpation d'un compte d'exploitation technique (OS, DB…)		
Obtention par voix officielle d'un compte injustifié		
Attaque d'une application cliente du référentiel d'identité		
Interception de flux d'échange		
Usurpation d'un compte d'exploitation EAI		

Au regard des risques liés au Système d'information, nous avons identifié 3 risques dont les fréquences estimées sont faibles au regard des mesures déjà en place, elles doivent cependant être mises à jour pour accroître leur efficacité.

Droit de la personne	Non - conformité
Information	
Transparence du traitement	2
Preuve du consentement	
Retrait du consentement	4
Respect de la finalité du traitement	
Accès	
Rectification	4
Effacement	4
Portabilité	
Profilage	
Données des mineurs	
Volonté post-mortem	

S'agissant du droit à la personne, on identifie une non-conformité à laquelle B-AS-USUAL répond partiellement, donc quantifiée à 2, et 3 non conformités graves quantifiées à 4. La fréquence d'occurrence est maximale puisque c'est avéré.

Phase 3 : Définir les mesures et réaliser le plan d'action

Définir les mesures transverses

Une fois les risques identifiés et qualifiés, il reste à définir le plan d'action qui va conduire l'entreprise à améliorer son niveau de conformité. La démarche consiste :

- à identifier d'abord les mesures transverses qui font faire évoluer le niveau de maturité de la cybersécurité des données, des risques propres aux données et au droit à l'information
- puis à les compléter des mesures spécifiques, maîtrisant les risques liés aux jeux de données

Mesures	Action
Perte ou vol d'un PC Portable ou support de stockage	
Authentification forte du poste	
Chiffrement des données du poste	x
Usage limité ou contrôlé du BYOD	
Blocage des ports USB	
Effacement disque dur laptops à distance	
Sauvegarde réseau (recommandation de ne rien stocker sur le disque dur)	x
Gestion standard centralisée des configurations	
Exfiltration de données	
Blocage des sites internet de transferts (dropbox, wetransfer, …)	x
Détection des uploads de fichiers volumineux vers internet	x
Blocage des ports USB	x
Infiltration via malware	
Antivirus fiable et mis à jour régulièrement	x
Filtre et sensibilisation au spam , phishing…	x

Certains risques, comme « Défaut de notification en cas d'une atteinte aux données » dans la catégorie « Risques de données », ou bien « Preuve du consentement » dans la catégorie « Droit à l'information », peuvent conduire à acquérir et déployer de nouveaux composants du Système d'Information, fournissant un service mutualisé.

Définir les mesures spécifiques

Les mesures spécifiques complètent les mesures du paragraphe précèdent en permettant de maîtriser les risques spécifiques non encore traités par le plan d'action.

A la différence des mesures précédentes, les mesures spécifiques sont localisées sur un ou plusieurs composants du Système d'Information.

Par exemple, reprenant la fiche sur les « données d'identification prospect », nous pouvons évoquer les mesures suivantes :

- Chiffrer les données hébergées par Cloud
- Vérifier que les contrats de sous-traitances incluent les obligations liées aux données personnelles et le périmètre des responsabilités associées, ainsi que les mesures organisationnelles et techniques assurant leur mise en œuvre
- Chiffrer le canal de communication des flux critiques, s'assurer qu'ils ont un niveau de traçabilité suffisant
- Mettre à jour les procédures et les fonctions d'habilitation des exploitants et des datascientists
- Obfusquer les données de test
- Les risques de données mentionnées ainsi que les risques de confidentialité liés aux plates-formes du Système d'information, indique que plutôt que de mettre à niveau chaque plate-forme, il est légitime d'instruire la question de construire un référentiel client.
- Et d'autres encore…

Les questions liées à l'architecture du système d'information

Comme nous l'avons vu précédemment, certaines mesures de maîtrise des risques pourraient éventuellement légitimer d'instruire des scénarios d'évolution de l'architecture du Système d'Information. Ces questions sont plus délicates à traiter qu'une mesure ponctuelle requérant le simple ajout d'une fonctionnalité à un composant applicatif.

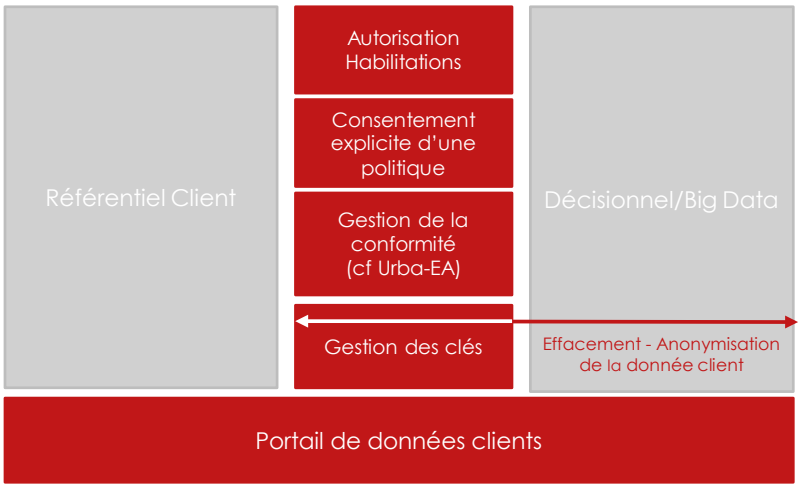
Ainsi, il peut être intéressant de centraliser les données personnelles relevant du règlement européen afin de centraliser les fonctions permettant d'exercer les droits à l'information typiquement le consentement, l'information, le droit à l'oubli.

Selon son contexte business, l'entreprise peut souhaiter centraliser les données ou bien, juste les liens référençant les données. En effet, la question de la localisation des données personnelles dans le système d'information se pose fréquemment aux entreprises. Cette question est cruciale pour permettre aux personnes, clients, fournisseurs, collaborateurs, d'exercer leur droit à l'information.

D'autre part, la diffusion des systèmes big data qui ont la particularité de charger les données telles quelles avant de les traiter, posent des problèmes vis-à-vis du droit à l'oubli. Ils doivent faire l'objet de mesures spécifiques :

- soit dans la politique des données qui établit que ceux-ci ne doivent être alimentés que de données personnelles obfusquées,
- soit d'un dispositif technique qui permette l'oubli des personnes relevant de l'exercice du droit à l'information, c'est-à-dire hors traitement légitime.

Il peut donc être intéressant de construire un registre centralisé au sein du système d'information qui rassemble les liens référençant les données personnelles et qui consolide l'ensemble des preuves d'information, de consentement, de notification etc.



Source : Opengroup - Archimetal case study version 2 – 2016

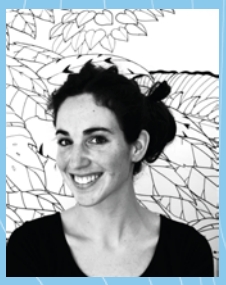
Glossaire :

- **Traitement légitime** : D'après le considérant 47 du GDPR, toute entreprise peut collecter et traiter des données personnelles sans le consentement des personnes concernées, si elle peut prouver qu'elle agit dans le cadre de ses « **intérêts légitimes** », tant que ceux-ci ne prévalent pas sur les intérêts et droit des personnes. En outre, le considérant stipule que « *en tout état de cause, l'existence d'un intérêt légitime devrait faire l'objet d'une évaluation attentive, notamment afin de déterminer si une personne concernée peut raisonnablement s'attendre, au moment et dans le cadre de la collecte des données à caractère personnel, à ce que celles-ci fassent l'objet d'un traitement à une fin donnée.* »
- **Cross selling** : Proposer des offres à des clients de l'entreprise ayant déjà acquis une première offre.
- **Data Management Platform (DMP)** : une plate-forme qui permet de gérer les visiteurs des sistes internet de l'entreprise, notamment via le système des cookies.
- **Software As a Service** (SaaS) : application metier fournie en mode Cloud par un éditeur
- **Up-selling** : Proposer de monter en gamme une offre à un client qui l'a déjà acquise, en ajoutant une ou plusieurs options, ou en relevant sont niveau de service.

CHAPITRE 3

MODE D'EMPLOI ET OUTILS DE CONFORMITE AVEC LE CADRE LEGISLATIF ET REGLEMENTAIRE

Piloté par **Loïc Rivière**
Délégué général,
TECH IN France



Coordonné par **Camille Parra**
Responsable Affaires publiques,
TECH IN France

Avec le concours de :

Thaima SAMMAN, Associée-fondatrice, SAMMAN

Béatrice DELMAS-LINEL, Associée gérante, Osborne Clarke

Lise BRETEAU, Associée, Osborne Clarke

Marc DREVON, Avocat, SAMMAN

TECH IN France tient particulièrement à remercier les avocats pour leur implication dans la rédaction de ce chapitre juridique.

TECH IN FRANCE

Le GDPR renouvelle l'approche de la protection des données personnelles en instaurant de nouvelles règles et de nouveaux outils de conformité, que l'on se propose de synthétiser en trois grands volets :

- la gestion interne, par les outils de gouvernance visant à l'auto-responsabilité des entreprises ("accountability");
- la démonstration de cette responsabilité vis-à-vis du public et des partenaires, via des outils de confiance;
- la gestion contractuelle des obligations et responsabilités, via la nouvelle structuration des clauses contractuelles.

Les outils de gouvernance

Le règlement impose aux entreprises d'internaliser les outils de la conformité et d'être, à tout moment en mesure de démontrer leur conformité au règlement.

Le système français reposait jusqu'à présent sur un principe d'autorisation *Ex Ante*. Désormais, la protection des données personnelles repose sur une logique de contrôle *Ex Post* par l'autorité de contrôle facilitée par les obligations de transparence au premier rang desquelles figure le registre. Le régime issu du GDPR dépasse à la fois (i) la régulation classique d'encadrement préalable et (ii) le régime libéral ayant pour seules bornes la sanction pénale et la responsabilité contractuelle. En effet, l'autorité publique, en plus de détenir le pouvoir de sanction *Ex Post*, définit les finalités et les objectifs de protection des données personnelles tandis que les moyens et instruments nécessaires à la poursuite de ces objectifs sont internalisées dans les entreprises au travers d'outils de compliance dont certains sont obligatoires tandis que d'autres sont facultatifs, mais promus.

Thaima Samman
Associée fondatrice
Cabinet SAMMAN

> *Portant le principe de l'accountability, le GDPR instaure un dialogue de coopération entre entreprises et régulateur par la création et la promotion d'outils de compliance obligatoires ou volontaires.*

Ainsi, cette régulation intelligente n'opère pas à proprement parler un transfert de pouvoirs aux entreprises mais instaure un dialogue de coopération régulatrice entre entreprises et régulateur. Cette logique se matérialise par les dispositions du GDPR selon lesquelles les États membres, les autorités de contrôle, le comité et la Commission encouragent l'élaboration de codes de conduite et la mise en place de mécanismes de certification.

Par ailleurs, cette régulation intelligente prend littéralement chair par la mise en place du *Data Protection Officer* (DPO) qui est tourné tant vers l'interne, en ayant pour mission d'informer et de conseiller l'entreprise que vers l'externe en tant que coordonnateur entre l'entreprise et le régulateur.

Le DPO est obligatoire pour certaines entreprises, mais il est plus généralement indispensable à toute entreprise qui traite des données de s'interroger sur l'intérêt d'un tel poste en son sein. Selon l'activité et selon les traitements effectués par l'entreprise, ce DPO peut être un véritable atout de gouvernance interne et de confiance vis-à-vis des tiers.

La documentation de la conformité

Le registre des activités de traitement représente l'outil de base de la gestion opérationnelle de la conformité et constitue la première obligation de preuve de la conformité. Il remplace l'obligation d'effectuer des formalités préalables de déclaration des traitements (sauf exception).

Source : Cabinet SAMMAN

Les entreprises tenues d'avoir un registre sont :

- Les entreprises de plus de 250 salariés ;
- Les entreprises de moins de 250 salariés qui effectuent des traitements :
  - De manière non occasionnelle ; ou
  - Susceptibles de comporter un risque pour les droits et des libertés des personnes concernées ; ou
  - Portant sur des données sensibles (article 9 (1)) ou des condamnations pénales.

Cette définition est assez large pour couvrir la grande majorité des entreprises et même si l'entreprise ne tombe pas sous le coup de cette obligation, il est bien sûr recommandé de tenir un tel registre.

Le contenu du registre est détaillé dans le GDPR. Il doit comporter les informations suivantes :

Pour les responsables de traitement	Pour les sous-traitants
• Nom et coordonnées du responsable du traitement, de son représentant et du DPO ; • Finalités du traitement ; • Catégories de personnes et de données à caractère personnel ; • Catégories de destinataires ; • Transfert vers pays tiers ; • Délais de conservation ou les moyens de déterminer ce délai de conservation ; et • Description des mesures de sécurité si possible	• Nom et coordonnées du responsable du traitement et du/des sous-traitant, de leur représentant et du DPO ; • Catégories de traitements pour chaque responsable de traitement ; • Les transferts vers des pays tiers ; et • La description générale des mesures de sécurité si possible.

Source : Cabinet SAMMAN

S'agissant des délais de conservation des données, on notera que le règlement parle de délai d'effacement. Cette question est cependant plutôt abordée sous l'angle du délai de conservation. La durée de conservation s'inscrit dans le principe de privacy by default, et doit être envisagée au regard des finalités pour lesquelles les données personnelles sont traitées. Ainsi, si une durée ne peut être a priori déterminée, il convient néanmoins de renseigner les modalités de détermination de cette durée de conservation.

Par ailleurs, le responsable du traitement est tenu de documenter toute violation de données à caractère personnel, en indiquant les faits concernant la violation des données à caractère personnel, ses effets et les mesures prises pour y remédier. La documentation ainsi constituée permet à l'autorité de contrôle de vérifier le respect des dispositions du GDPR.

Le responsable de traitement pourra utilement faire figurer dans cette documentation l'ensemble des informations que son sous-traitant lui aura transmis.

Dans ses récentes lignes directrices soumises à consultation, le G29 suggère également aux responsables de traitement de documenter les actions prises à la suite d'une violation de données personnelles et notamment de documenter les raisons qui ont conduit à considérer que la violation ne représentait pas un risque ou un risque élevé ou pourquoi la communication de la violation n'était pas nécessaire en application des dispositions de l'article 34 (3) du GDPR.

De même, le responsable de traitement devrait documenter les raisons pour lesquelles une notification à l'autorité de contrôle a été retardée au-delà du délai de 72h. Enfin, le responsable de traitement, afin de remplir ses obligations en matière d'*accountability* et de compliance, devrait se doter des moyens lui permettant de rapporter la preuve d'une notification auprès des personnes concernées.

Afin d'accompagner les entreprises, la CNIL propose un modèle de registre disponible à l'adresse suivante : https://www.cnil.fr/sites/default/files/atoms/files/registre-reglement-publie.xlsx

S'agissant de l'identification du responsable de traitement, afin d'éviter les confusions, il convient de se reporter aux contrats conclus pour le traitement des données. En effet, un sous-traitant opérant pour plusieurs filiales/ responsables de traitement d'une même société mère peut facilement être amené à considérer, à tort, que le responsable de traitement est la société mère et non sa filiale.

La documentation de la conformité passe également par l'enregistrement et la conservation des éléments suivants :

- Les analyses d'impact sur la protection des données ;
- Les outils de transferts de données en dehors de l'UE ;
- Les informations données aux personnes concernées ;
- Le recueil du consentement des personnes concernées ;
- Les procédures d'exercice des droits des personnes concernées et de notifications ; et
- Le recueil des contrats avec les responsables de traitement et sous-traitants.

Ces registres et documentation doivent être tenus en ayant en tête qu'ils devront être communiqués, à tout moment, aux autorités de contrôle qui en feront la demande. Il conviendra d'être vigilant sur la clarté et lisibilité des informations y figurant.

Marc DREVON
Avocat
Cabinet SAMMAN

> *Le registre ne doit pas être appréhendé comme une contrainte administrative mais plutôt comme un outil dynamique de cartographie des traitements et des flux de données. Si l'objet premier du registre est de faciliter les contrôles opérés par l'autorité de protection des données personnelles, le registre a également pour vocation de servir de repères aux sous-traitants et responsables de traitement pour s'assurer de la conformité de leurs traitements au GDPR. Le registre est ainsi particulièrement utile pour réaliser une évaluation des traitements qui ne sont pas soumis à analyse d'impact (voir ci-après).*

Analyse d'impact relative à la protection des données (ou « PIA »)

Le GDPR impose la réalisation d'une analyse d'impact relative à la protection des données (ou DPIA pour Data Protection Impact Assessment) pour les traitements présentant un risque important pour la protection des données personnelles et leurs impacts sur les droits et libertés des personnes concernées par ces traitements.

a) Qu'est-ce qu'une analyse d'impact ?

L'analyse d'impact est un outil introduit par le GDPR conçu pour décrire un traitement de données à caractère personnel, évaluer la nécessité et la proportionnalité du traitement et aider à identifier les risques résultant de ce traitement ainsi que les mesures pour y remédier.

Réalisé par le responsable de traitement en amont de tout projet dans le respect de l'approche Privacy by Design, l'analyse d'impact est un outil dynamique et efficace s'inscrivant à la fois dans une logique d'accountability et dans une logique de gestion des risques.

En effet, cet outil permet en premier lieu de bâtir sa conformité et de la démontrer. Même dans les cas où l'analyse d'impact n'est pas strictement exigée par la règlementation (cf. ci-dessous), elle sera très utile aux prestataires de services souhaitant proposer des produits respectueux

de la vie privée. Ceux-ci sont d'ailleurs vivement encouragés par les autorités de contrôle à communiquer au public leur analyse d'impact afin de créer une relation de confiance.

L'analyse d'impact permet également une gestion efficace du risque puisqu'une telle analyse demande au responsable d'évaluer, en particulier, l'origine, la nature, la portée, le contexte, la particularité et la gravité du risque engendré par le traitement de données à caractère personnel et de prendre des mesures pour supprimer ou limiter ces risques. Le risque résiduel sera soit accepté par le responsable de traitement soit assuré.

Pour effectuer cette analyse d'impact, le responsable de traitement pourra s'appuyer sur différents acteurs internes tels que le DPO, les métiers, le RSSI, qui seront dans la plupart des cas à l'initiative de l'analyse d'impact et définiront la méthodologie appropriée à l'entreprise (cf. ci-dessous), ainsi que sur des acteurs externes, sans oublier les sous-traitants eux-mêmes dans le cadre du devoir d'assistance envers le responsable de traitement pesant sur eux aux termes de la règlementation.

b) Quand réaliser une analyse d'impact ?

Au titre de l'Article 35 du GDPR, les responsables de traitement ont l'obligation d'effectuer une analyse d'impact dans certains cas limitativement énumérés et principalement lorsque le traitement ou le produit qui sera déployé est « *susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques concernées* ».

Par ailleurs, dans le cas où l'analyse d'impact révèlerait un risque résiduel important, le responsable de traitement devra également consulter l'autorité de contrôle afin d'obtenir son autorisation préalable.

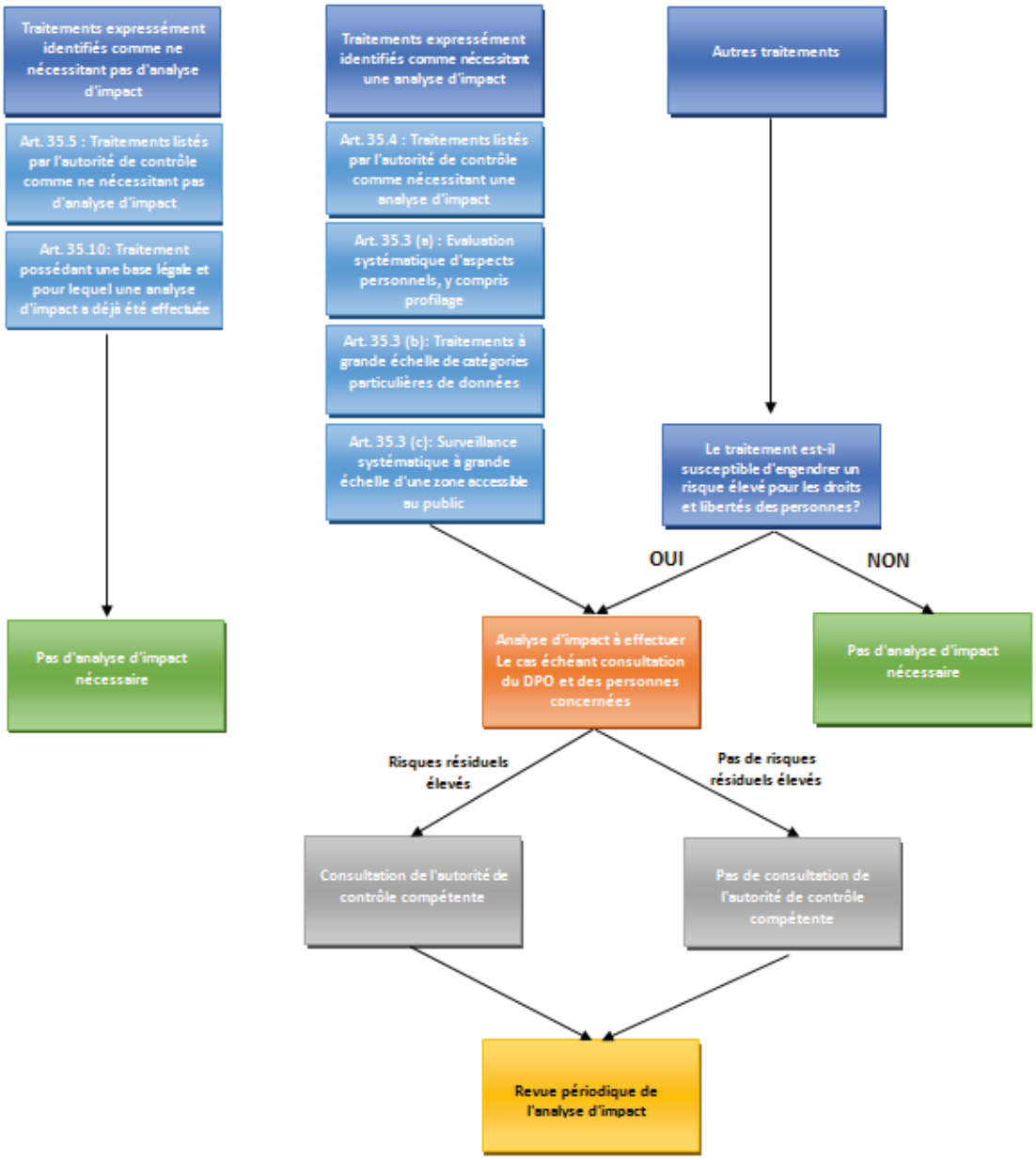
Afin de faciliter la mise en œuvre de cet article 35, le Groupe de l'Article 29 ("G29") a publié des lignes directrices publiées le 4 avril 2017[14].

[14] Groupe de l'Article 29," Lignes directrices sur l'analyse d'impact relative à la vie privée et sur la détermination du traitement "susceptible d'engendrer un risque élevé" dans le cadre du Règlement 2016/679", 4 avril 2017 (disponible en ligne en anglais uniquement :

http://ec.europa.eu/newsroom/document.cfm?doc_id=44137). Ces lignes directrices viennent d'être finalisées le 4 octobre 2017, https://www.cnil.fr/sites/default/files/atoms/files/20171013_wp248_rev01_enpdf.pdf

Dans la continuité de ces lignes directrice et afin d'aider les responsables de traitement dans la détermination de la nécessité d'une analyse d'impact et d'une consultation de l'autorité de contrôle nous avons élaboré l'arbre de décision suivant :

Arbre de décision – Analyse d'impact



Source : Osborne Clarke

c) Comment réaliser une analyse d'impact ?

Le GDPR n'impose pas de méthodologie particulière pour la conduite de l'analyse d'impact mais prévoit néanmoins ce que le rapport d'analyse devra contenir a minima :

- une description systématique des opérations de traitement et de ses finalités ;
- une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités ;
- une évaluation des risques pour les droits et les libertés des personnes concernées;
- les mesures envisagées pour faire face à ces risques.

Chaque responsable de traitement aura par conséquent la liberté soit de choisir une méthodologie existante (cf. liste de méthodologies publiée par le G29[15]), soit de créer sa propre méthodologie en fonction de son activité et de ses règles de fonctionnement interne.

Lise BRETEAU
Associée
Osborne Clarke

> *Dans une logique de mutualisation des coûts, on ne peut qu'encourager les responsables de traitement d'un même secteur d'activité à se réunir pour développer leur propre méthodologie sectorielle afin de disposer d'un outil le plus adapté possible.*

Le DPO, acteur indispensable de la conformité

Les autorités de régulation en Europe s'accordent pour dire que le DPO est la pierre angulaire de l'accountability. Le DPO va accompagner l'entreprise pour qu'elle soit en conformité avec les dispositions applicables en matière de protection des données à caractère personnel. Il a également pour mission d'être l'intermédiaire entre la CNIL et les entreprises afin que ces dernières puissent adapter en temps réel leurs traitements aux exigences du GDPR.

[15] Groupe de l'Article 29," Lignes directrices sur l'analyse d'impact relative à la vie privée et sur la détermination du traitement "susceptible d'engendrer un risque élevé" dans le cadre du Règlement 2016/679", 4 avril 2017 (disponible en ligne en anglais uniquement : http://ec.europa.eu/newsroom/document.cfm?doc_id=44137)

Elena GILOTTA,
Directrice de la conformité de la zone EMEA
BOX

GDPR, le point de vue de BOX

La gestion de données est centrale à l'activité de BOX, qui fournit des services de stockage, de partage et de gestions de données. BOX est donc très sensible à la question des données personnelles et applique depuis plusieurs années des principes similaires à ceux du GDPR, y compris le principe d'accountability.

BOX a déjà nommé un responsable de la protection des données personnelles aux Etats-Unis et a pour projet de nommer un DPO (Data Protection Officer, délégué à la protection des données) au niveau européen pour permettre une relation facilitée avec les autorités locales européennes. L'entreprise a choisi de ne pas placer le DPO au sein du département juridique pour éviter les conflits d'intérêts (le general counsel étant en charge des contentieux de données personnelles).

La stratégie de BOX en matière de données personnelles est d'étudier les règles des pays où l'entreprise a des activités en Europe (principalement Royaume-Uni, France et Allemagne) et d'appliquer les plus strictes (« the bar has to be high »).

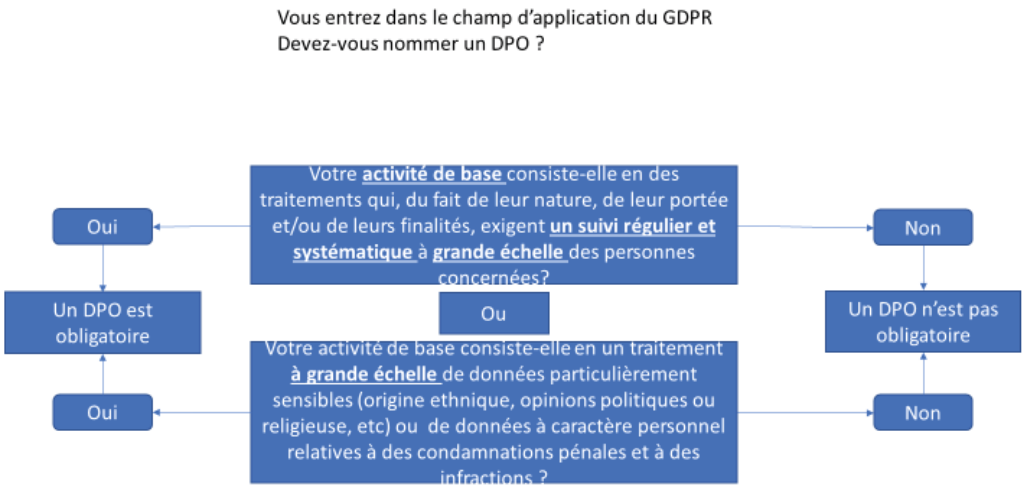
En matière de BCR (Binding Coroporate Rules, Règles contraignantes d'entreprise), les travaux de BOX ont commencé il y a trois ans ; l'entreprise a obtenu – en deux ans environ – les BCR Responsable de Traitement ainsi que les BCR Sous-Traitant ; ces dernières sont les plus intéressantes, bien que moins connues, car elles facilitent les transferts de données hors groupe.

La nécessité de cartographier les traitements de données est une des grosses difficultés du GDPR, complexifiée par la diversité des systèmes utilisés. BOX propose ainsi à ses clients de centraliser leurs données dans un système unique (même s'il ne s'agit pas d'un stockage géographique unique).

Pour permettre une meilleure sécurité des données, BOX offre également à ses clients de travailler avec un consultant externe afin que celui-ci propose des mesures de sécurité adaptée en fonction du type de données stockées chez BOX.

a) Les critères déterminant l'obligation de se doter d'un DPO

Le caractère obligatoire du DPO repose sur trois critères : l'activité de base, le suivi régulier et systématique, le traitement à grand échelle.



Source : Cabinet SAMMAN

1/ Activités de base : Les activités visées par le GDPR sont les activités d'un responsable du traitement qui ont trait à ses activités principales et ne concernent pas le traitement des données à caractère personnel en tant qu'activité auxiliaire.

Selon le G29, cette notion englobe les opérations nécessaires au responsable de traitement ou au sous-traitant pour accomplir ses missions. Cette interprétation exclurait donc des activités de base les activités de traitement des fonctions supports telles que les ressources humaines ou les services informatiques.

Cependant, dès lors que l'activité de traitement est inhérente à la mission du responsable de traitement ou du sous-traitant, celle-ci devrait être prise en compte pour la désignation d'un DPO.

2/ Traitement à grande échelle : Cette notion n'est pas définie par le GDPR et le G29 n'a pas souhaité donner une définition définitive estimant que cette notion devra être précisée par la pratique. Néanmoins, l'appréciation du traitement à grande échelle peut se fonder sur :

- Le nombre de personnes concernées soit en valeur absolue soit en pourcentage de la catégorie de personnes visées ;
- Le volume ou la diversité des données traitées ;
- La durée du traitement ;
- L'étendue géographique du traitement.

3/ Suivi régulier et systématique : ces termes ne sont pas définis par le GDPR. Le G29 interprète le terme « régulier » comme comprenant les significations suivantes :

- Intervenant à des intervalles réguliers pour une période donnée ;
- Répété à des moments déterminés ;
- Ayant lieu de façon périodique ou constante.

Le terme « systématique » devrait être compris comme :

- Réalisé selon un système ;
- Arrangé, organisé ou méthodique ;
- Accompli dans le cadre d'un plan plus général de collecte de données ;
- Effectué dans le cadre d'une stratégie.

Il convient de noter que le droit de l'Union et le droit national des Etats membres pourront prévoir des cas supplémentaires pour lesquels la désignation d'un DPO sera obligatoire.

Ainsi, par exemple, l'Allemagne a étendu la désignation obligatoire d'un DPO aux cas suivants :

- Si le responsable de traitement ou le sous-traitant emploie au moins 10 personnes pour le traitement automatisé de données personnelles ;
- Si le responsable de traitement ou le sous-traitant est soumis à une analyse d'impact sur la protection des données en application de l'article 35 du GDPR ;
- Si le responsable de traitement ou le sous-traitant traitent des données à des fins commerciales avec pour finalités leur transfert, le cas échéant sous forme anonymisée, le marché ou des enquêtes d'opinion.

Par ailleurs, la nomination volontaire d'un DPO oblige l'entreprise à respecter l'ensemble des critères relatifs au DPO.

Dans l'hypothèse où une entreprise ferait le choix de ne pas nommer un DPO, il semble primordial de documenter cette décision et de la justifier au regard des critères susmentionnés.

b) Le choix du DPO

Le DPO peut être un salarié de l'entreprise ou remplir sa mission en tant que collaborateur extérieur.

Le DPO doit être accessible

Le DPO doit être accessible, c'est-à-dire que son accès doit être aisé tant pour les personnes concernées que pour l'autorité de protection des données à caractère personnel. Cela suppose que le DPO puisse répondre dans une langue généralement utilisée par les personnes concernées et l'autorité de contrôle, que les coordonnées du DPO soient facilement accessibles tant vis-à-vis de l'extérieur qu'en interne. S'il est possible de nommer un unique DPO pour un groupe d'entreprises, il conviendra de veiller à que cela soit sans préjudice de son accessibilité.

Les compétences du DPO

Le DPO doit être désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir ses missions. Le niveau d'expertise doit être apprécié en fonction de la taille de l'entreprise et des traitements réalisés notamment de l'existence de traitements de données sensibles ou des transferts internationaux de données.

Il convient de s'assurer que le DPO dispose également d'une bonne connaissance du secteur d'activité de l'entreprise concernée. Il est important que le DPO puisse avoir accès aux formations proposées par la CNIL.

Les qualités du DPO

Le DPO doit être en mesure d'accomplir ses missions. En plus des compétences, le DPO doit disposer des moyens techniques et humains nécessaires. L'entreprise doit donc, le cas échéant, établir un budget et une équipe. Elle devra également permettre au DPO de suivre des formations.

Le profil et la place du DPO dans l'organisation doit lui permettre de disposer de l'autorité nécessaire et de l'accès aux dirigeants. Sur la base d'un état des lieux des traitements mis en œuvre, l'entreprise pourrait formaliser les éléments suivants :

- Évaluation de la charge de travail ;
- Évaluation du budget
- Composition de l'équipe mis à la disposition du DPO et modalités de désignation ;
- Nombre d'heures de formations dont bénéficie le DPO ou son équipe ;
- Engagements de faire participer le DPO aux réunions des dirigeants ;
- Engagement de consulter le DPO sur toutes questions relatives à la protection des données ; et
- Engagement d'informer le DPO de tout incident relatif à la protection des données à caractère personnel.

Il convient de veiller à ce que les mesures prises dans ces domaines ne viennent pas empiéter sur les missions du DPO. Il appartient également à l'entreprise de mettre en place la communication nécessaire pour asseoir l'autorité du DPO.

Sur la base de ces éléments, le DPO devrait pouvoir déterminer :

- Les modalités de reporting auprès des dirigeants ;
- Les modalités d'accès aux données, aux opérations de traitement ;
- Les modalités d'intervention en cas de data breach, etc.

Le DPO doit être indépendant. Si le DPO n'est pas un salarié protégé au sens du droit du travail, le GDPR précise que le DPO ne peut faire l'objet de sanctions ni ne recevoir d'instruction pour l'exercice de ses missions. Ces dispositions devraient être reprises dans le contrat entre le DPO et l'entreprise. On notera que le DPO peut être sanctionné pour des motifs extérieurs à sa mission. Dans une telle hypothèse, il conviendra de prévoir une procédure renforcée afin qu'il n'y ait pas de possible équivoque sur les raisons de ces sanctions.

Le DPO ne doit pas présenter de conflits d'intérêts. Les fonctions de DPO ne sont pas exclusives d'autres fonctions au sein de l'entreprise. Cependant, il convient de veiller à ce que ces autres fonctions ne conduisent pas à un risque de conflits d'intérêts. Tout particulièrement, le DPO ne doit pas exercer de missions le conduisant à définir les finalités et les moyens du traitement de données à caractère personnel. Ainsi, certains postes semblent par nature présenter des risques de conflits d'intérêts : directeur juridique, directeur du marketing,

directeur IT, etc. Les entreprises devraient réaliser une évaluation leur permettant de déterminer :

- Les postes qui ne peuvent être cumulés avec les fonctions de DPO ;
- Les règles permettant d'éviter les conflits d'intérêts ;
- Les stipulations contractuelles relatives aux conflits d'intérêts à prévoir dans le contrat avec le DPO ;
- Les modalités de déclaration d'absence de conflits d'intérêts afin d'attirer l'attention du DPO sur cette question.

c) Les missions du DPO

Le DPO est un poste de gestion de risques qui débouche sur des préconisations et des recommandations en vue de la conformité avec le GDPR.

Ainsi, l'article 39 du GDPR prévoit que le DPO a pour mission :

- D'informer et conseiller le responsable du traitement ou le sous-traitant sur les obligations qui leur incombent en vertu du GDPR et des autres dispositions relatives à la protection des données. Les entreprises devraient permettre au DPO de définir les modalités de cette mission d'information.

- Contrôler le respect du GDPR, des autres dispositions en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant. Notamment, le DPO devrait :
  - Recenser les traitements de données à caractère personnel ;
  - Analyser et vérifier leur conformité au GDPR ;
  - Informer et conseiller l'entreprise sur les mesures à prendre.

- Dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données. Les entreprises devraient prévoir les modalités selon lesquelles elles consultent leur DPO en matière d'analyse d'impact notamment sur les questions suivantes :
  - La nécessité ou non de réaliser une analyse d'impact ;
  - La méthodologie de cette analyse d'impact ;
  - Les garde-fous à mettre pour circonscrire les risques d'atteintes aux droits des personnes concernées ;
  - La vérification du bon déroulé de l'analyse d'impact et l'appréciation quant au respect du GDPR.

- Coopérer avec l'autorité de contrôle. Le DPO, dans le respect de son obligation de confidentialité, doit servir de relais entre l'entreprise et la CNIL. Il est important qu'il puisse demander conseil auprès de l'autorité de contrôle.

- Faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, notamment pour la consultation préalable des traitements dont l'analyse d'impact relève un risque fort pour les droits des personnes concernées.

Le DPO doit adopter une approche axée sur les risques. C'est le risque qui doit déterminer la conduite du DPO et l'aider à prioriser ses missions.

A noter : les entreprises devraient également prévoir de documenter les raisons pour lesquelles elles décident de ne pas suivre une recommandation du DPO.

Le GDPR ne se focalise pas seulement sur les objectifs de la protection des données, il définit aussi les moyens de cette protection et encourage l'adoption de différents outils permettant aux entreprises de communiquer publiquement sur leur conformité. Ainsi, codes de conduite, certification et règles contraignantes d'entreprise, font l'objet d'un focus et d'une reconnaissance marqués de la part du GDPR. Autant d'outils visant à créer la confiance.

Outils	Objet	Périmètre prévu au GDPR
Codes de conduite	Outil de conformité	Réservé à un secteur identifié [à confirmer]
Certifications	Outil de conformité	Non réservé à un secteur particulier
Règles d'entreprise contraignantes	Outil d'encadrement des transferts intragroupe de données à caractère personnel	Groupe d'entreprises

Source : Osborne Clarke

Stanislas DE RÉMUR
Cofondateur et CEO
Oodrive

GDPR, le point de vue d'Oodrive

La mise en conformité avec le GDPR est un passage obligé pour toutes les entreprises européennes. Et Oodrive ne fait pas exception, bien sûr. Compte tenu de notre secteur d'activité et de nos métiers, la question de la protection des données personnelles est essentielle. En effet, nous gérons à travers nos solutions – de partage, de sauvegarde et de signature électronique – une quantité considérable de données.

Ce nouveau texte européen est donc une étape importante pour nous

En tant que fournisseur de solutions traitant des données professionnelles et personnelles, nous occupons une place clé dans la chaîne de conformité et nous sommes amenés à interagir avec différents acteurs.

Nous sommes parfois en relation contractuelle directe avec le Responsable de Traitement, et parfois avec son sous-traitant (un éditeur SaaS sous contrat avec un hébergeur par exemple). Notre conformité au GDPR est donc un élément primordial. Mais elle n'est pas suffisante : chaque maillon devra être en capacité de démontrer sa conformité. Il est nécessaire de garantir que les prestataires, aussi bien en amont qu'en aval de la chaîne de sous-traitance, répondent aux exigences.

Nous travaillons à la fois sur la conformité de nos solutions (Privacy by Design), ainsi qu'à la fourniture des services requis par le règlement. Les données collectées via nos solutions de sauvegarde sont chiffrées de bout en bout par défaut avec une possibilité de choisir la clé de chiffrement. Cela nous permet d'être en accord avec certaines exigences du GDPR en matière de sécurité.

Une certification, notamment dans le domaine de la sécurité, peut également jouer un rôle très important. C'est non seulement une vraie reconnaissance de notre travail, mais c'est aussi un gage de confiance pour un client. Certaines sont pratiquement incontournables, comme la norme ISO 27001

La sécurité étant la pierre angulaire de nos métiers, nous nous sommes impliqués ces dernières années dans un certain nombre de démarches qui nous permettent aujourd'hui d'être déjà bien engagés sur la voie de la conformité au RGPD.

En 2014, nous avons par exemple participé à l'élaboration d'une certification sous la bannière Cloud Confidence. Le label Cloud Confidence, actuellement en cours de révision pour être en accord avec le RGPD, nous permet aujourd'hui de garantir à nos clients et aux utilisateurs de nos solutions un cadre de transparence sur la protection des données.

Les principaux outils de confiance vis-à-vis des tiers et la présomption de conformité

Instruments encore méconnus de la pratique, les codes de conduite, certifications, labels et marques ou encore règles contraignantes d'entreprise, pourraient se révéler être des outils précieux pour guider les organisations dans leurs efforts de conformité, en leur fournissant un cadre de conformité plus adapté et personnalisé que les règles génériques du GDPR.

Les codes de conduite

La notion de "code de conduite" introduite par le GDPR constitue une nouveauté par rapport à la loi française de 1978, même si certaines actions de la CNIL ces dernières années s'inscrivaient déjà dans une démarche proche (cf. ci-dessous). Dans une acception large, un code de conduite pour une entreprise est un ensemble d'engagements unilatéraux sur des principes, des actions, des pratiques, bref, sur une conduite que cette entreprise s'engage à adopter et respecter, le tout formalisé au sein d'un document rendu public. Ainsi le code de conduite n'est pas imposé par une loi ou une réglementation. Sa valeur contraignante ne vient donc pas de la sanction prévue par la loi, mais du caractère public de l'engagement unilatéral pris par l'entreprise qui, en cas de non-respect de cet engagement se retrouve publiquement exposée et décrédibilisée. Popularisé par les stratégies et plans de responsabilité sociétale et environnementale des entreprises, cet outil parfois conçu et perçu comme un simple instrument de communication et de marketing est le plus souvent un véritable instrument normatif pour les entreprises dans un contexte de "soft law", à savoir d'autorégulation, de plus en plus prégnant et encouragé par le législateur national et européen lui-même.

Ainsi au plan de l'Union Européenne, le concept de code de conduite fait son introduction dès la directive 2005/29/CE relative aux pratiques commerciales déloyales des entreprises vis-à-vis des consommateurs dans le marché intérieur qui le définit comme : « *un accord ou un ensemble de règles non imposés par les dispositions législatives, réglementaires ou administratives d'un État membre, qui définissent le comportement des professionnels qui s'engagent à être liés par lui sur une ou plusieurs pratiques commerciales ou un ou plusieurs secteurs d'activité.* »[16]

Il n'est dès lors pas surprenant que le GDPR reprenne cette notion en matière de protection des données à caractère personnel, son Article 40 §1 l'évoquant non pas à l'échelle d'une entreprise mais d'un secteur d'activité donné, secteur qui se doterait d'un ensemble de règles destinées à « *contribuer à la bonne application du [GDPR], compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises* »[17].

C'est donc un code de conduite "sectoriel" que vise le GDPR, sans pour autant définir ce terme, ce qui ouvre la voie à une approche de la conformité non pas limitée à une entreprise ou un groupe d'entreprises mais à l'ensemble des entreprises relevant du secteur concerné. Si les intérêts d'une telle approche sont multiples (a), il convient de s'attarder sur les conditions de mise en œuvre de ce nouvel outil de conformité (b).

---

[16] Article 40 § 1 du GDPR

[17] Voir notamment le considérant (77) et les articles 24, 28, et 32 du GDPR

a) Les intérêts liés au code de conduite sectoriel

Les codes de conduite font l'objet de deux articles dédiés dans le GDPR, les articles 40 et 41, auxquels s'ajoutent de nombreuses références tout au long du texte. Les codes de conduite sont présentés comme un outil de conformité des traitements de données et s'inscrivent dans la même logique d'accountability introduite par le GDPR que les certifications.

Concrètement, l'intérêt pour les responsables de traitement ou sous-traitants de pouvoir adhérer à un code de conduite sectoriel est de plusieurs ordres.

En premier lieu, il s'agit d'un outil de preuve de la conformité, aussi bien pour les responsables du traitement[18] que pour les sous-traitants[19]. L'adhésion à un code de conduite est d'ailleurs prise en compte dans les analyses d'impact[20] en ce qu'elle permet de minimiser les risques liés aux traitements réalisés.

Par ailleurs, l'adhésion à un code de conduite par un responsable du traitement ou un sous-traitant est inclue parmi les « *circonstances atténuantes* » devant être prises en compte par les autorités de contrôle en cas de décision de sanction administrative[21]. Ainsi, le montant d'une telle sanction administrative pourra être diminué si l'entreprise concernée démontre qu'elle respecte un code de conduite approuvé.

Enfin, l'adhésion à un code de conduite (comme c'est le cas en ce qui concerne les certifications) permet à des prestataires étrangers de fournir des « *garanties appropriées* » dans le cadre d'un transfert de données, sous réserve d'un engagement juridiquement contraignant sur ces garanties[22]. C'est une option intéressante qui peut être proposée à des partenaires hors UE (tels que des prestataires américains).

Plus généralement, **l'intérêt d'un code de conduite sectoriel est de préciser et d'adapter les règles générales de protection des données aux différents secteurs d'activité et aux contraintes propres aux petites et moyennes entreprises**. L'idée ici est clairement celle de croiser la prise en compte des spécificités d'un secteur avec le souci de permettre aux petites et moyennes entreprises l'accès à des outils de conformité, similaires à une certification, adaptés à leur activité et potentiellement plus favorable économiquement. En effet, si un secteur déterminé s'organise pour développer et faire valider un code de conduite, dont l'adhésion sera ensuite proposée aux entreprises concernées dans les conditions permettant le plein effet juridique du code de conduite sectoriel, ces entreprises pourraient bénéficier des économies d'échelle générées par une telle démarche collective.

Pour le législateur, c'est le moyen de permettre au plus grand nombre d'entreprises d'accéder aux outils de conformité, mais aussi de pouvoir dialoguer directement avec les instances représentatives des secteurs qui auront adopté un code de conduite, réduisant ainsi le nombre d'interlocuteurs directs.

Les codes de conduite sectoriels, pour produire leur plein effet, doivent avoir suivi une procédure d'approbation précise visant à garantir leur conformité à la réglementation européenne.

---

[18] Article 24 du GDPR

[19] Article 28 du GDPR

[20] Article 35 du GDPR

[21] Considérant (148) et article 83 du GDPR

[22] Article 46 du GDPR

b) Les conditions de validité et d'approbation d'un code de conduite sectoriel au sens du GDPR

Concernant la rédaction d'un code de conduite sectoriel, le GDPR fournit les indications suivantes sur son contenu qui devra aborder les thèmes suivants :

> *« a) le traitement loyal et transparent ;*
>
> *b) les intérêts légitimes poursuivis par les responsables du traitement dans des contextes spécifiques ;*
>
> *c) la collecte des données à caractère personnel ;*
>
> *d) la pseudonymisation des données à caractère personnel ;*
>
> *e) les informations communiquées au public et aux personnes concernées ;*
>
> *f) l'exercice des droits des personnes concernées ;*
>
> *g) les informations communiquées aux enfants et la protection dont bénéficient les enfants et la manière d'obtenir le consentement des titulaires de la responsabilité parentale à l'égard de l'enfant ;*
>
> *h) les mesures et les procédures visées aux articles 24 et 25 [concernant la responsabilité du responsable du traitement, la protection dès la conception et la protection par défaut] et les mesures visant à assurer la sécurité du traitement visées à l'article 32 [obligations relatives à la sécurité du traitement] ;*
>
> *i) la notification aux autorités de contrôle des violations de données à caractère personnel et la communication de ces violations aux personnes concernées ;*
>
> *j) le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales ; ou*
>
> *k) les procédures extrajudiciaires et autres procédures de règlement des litiges permettant de résoudre les litiges entre les responsables du traitement et les personnes concernées en ce qui concerne le traitement, sans préjudice des droits des personnes concernées au titre des articles 77 et 79 [réclamations auprès d'une autorité de contrôle et recours juridictionnels]. »*

En outre, le code de conduite doit prévoir un mécanisme permettant le contrôle de l'application de ce code par un organisme de contrôle agréé par l'autorité de contrôle[23].

Malgré ces indications, force est de constater que le contenu d'un code de conduite est encore incertain. Il parait raisonnable de s'inspirer, pour rédiger un code de conduite, du format et contenu des BCR, sous une forme à la fois plus générale (à savoir dépassant une seule entreprise) et adaptée au secteur concerné, tout en permettant de prendre en compte les différentes situations de ses signataires (par exemple selon la taille des entreprises).

[23] Article 40 § 4 du GDPR

Certaines associations et fédérations ont commencé à réfléchir sur l'élaboration d'un code de conduite et l'on peut citer l'exemple du code de conduite du CISPE (Cloud Infrastructure Services Providers in Europe)[24].

Cette rédaction pourra faire l'objet d'échanges avec l'autorité de contrôle compétente, puisqu'en tout état de cause tous les projets de code de conduite, ainsi que toutes les modifications ou prorogations ultérieures de tels codes, sont soumis à l'autorité de contrôle compétente, qui émet un avis.

En cas d'avis positif, si le projet ne concerne qu'un Etat membre (c'est-à-dire porte sur des traitements dans un seul Etat membre), l'autorité enregistre et publie le code de conduite. Si le projet concerne plusieurs Etats membres (s'il porte sur des traitements dans plusieurs Etats membres, ce qui sera probablement très souvent le cas), l'autorité soumet le projet au comité européen de la protection des données (CEPD), qui lui-même le consigne, le publie et le soumet à la Commission s'il estime que le projet est conforme au GDPR. Après une procédure d'examen, la Commission peut alors décider que le code de conduite est d'application générale au sein de l'UE. Cet aspect est important : potentiellement, un code de conduite peut devenir un instrument normatif général, ce qui plaide en faveur de cet outil et invite également à la prudence dans son élaboration.

Le contrôle du respect des codes de conduite sera effectué par un « contrôleur » agréé par les autorités de contrôle. Ce « contrôleur » doit être un « organisme qui dispose d'un niveau d'expertise approprié »[25], et qui pourra être une organisation privée.

Béatrice Delmas-Linel
Associée gérante
Osborne Clarke

> *Les modalités d'agrément d'un « contrôleur » par les autorités de contrôle ne sont pas connues à ce stade. La question se pose de savoir si l'association ou la fédération professionnelle ayant conduit l'élaboration d'un code de conduite sectoriel, et l'adhésion à celui-ci par ses membres, pourrait être agréée en tant qu'organisme de contrôle. Ce point devra être précisé, et il est probable que tout agrément exige d'un tel organisme de garantir son indépendance, sa neutralité et la gestion d'éventuels conflits d'intérêts. Ces questions sont d'autant plus importantes que l'organisme de contrôle aura le devoir et le pouvoir d'informer l'autorité de contrôle en cas de violation du code de conduite par un responsable du traitement ou sous-traitant et de décider des « mesures appropriées », incluant la suspension ou l'exclusion de l'application du code pour l'entreprise concernée.*

[24] Code de conduite élaboré par le CISPE (*Cloud Infrastructure Services Providers in Europe*) disponible en ligne : https://cispe.net/wp-content/uploads/pdf/CISPE-CodeOfConduct-160926.pdf

[25] Article 41 § 1 du GDPR

Sylvain FOUREY
RSSI Groupe
Cegid

GDPR, le point de vue de Cegid

Cegid au même titre que toutes les entreprises européennes est soumis au nouveau règlement général sur la protection des données 'RGPD' ou GDPR en anglais. Plus qu'une évolution réglementaire, il faut voir cette obligation comme une opportunité d'apporter plus de transparence et donc de confiance aux personnes avec qui nous sommes tous en relation.

En attendant les labels, certifications, outils et autres process qui permettront de démontrer la conformité d'une organisation sur le sujet de la gestion des données personnelles, nous pensons qu'il est nécessaire de faire un focus sur quelques notions.

Le point le plus important est la mise en place d'une gouvernance transverse sur la gestion des données. En effet la mise en place d'un projet GDPR se traduit par des modifications dans les usages des collaborateurs, les moyens mis à disposition et donc doit s'inscrire dans un changement plus global de la culture de l'entreprise. Les données doivent devenir des actifs à part entière du système d'information.

Afin de suivre et guider cette transformation, la fonction DPO (Data Privacy Officer) aura un rôle central. Ses domaines de compétences devant couvrir un périmètre allant du juridique à l'opérationnel en passant par la sécurité des systèmes d'information et la connaissance des métiers de l'entreprise, les réflexions portant sur la nomination de plusieurs DPO ayant chacun sa spécialité ne doit pas être écartée.

Un autre sujet sur lequel il est essentiel de s'attarder est la documentation à produire. Cette documentation obligatoire sera demandée lors d'un contrôle mais il faut aussi la voir comme un élément de confiance. En effet, pourquoi ne pas capitaliser sur le travail effectué pour en tirer des éléments de communication avec lesquels nous pourrions alimenter la confiance de toutes les personnes avec qui nous travaillons.

Enfin, le mode de distribution de certains produits comme les notre va revêtir une importance supplémentaire. Au moment où les organisations évaluent leurs risques et commencent à se mettre en ordre de bataille, les éditeurs de logiciel ont un rôle évident à jouer dans l'accompagnement -ou non !- de leurs clients. Dans cette perspective, le mode SaaS apparait comme un outil d'autant plus puissant et rassurant pour de nombreux clients et prospects ; ceux qui ont déjà opté pour ce choix stratégique sont d'autant mieux placés pour se préparer.

La sécurité des données et la confiance dans les acteurs numériques sont les piliers qui vont construire les échanges digitaux de demain, faisons-en sorte de tous contribuer à ce but.

En France, il est intéressant de signaler que la loi informatique et libertés française permet déjà à la CNIL de donner un avis sur la conformité aux dispositions de la loi du 6 janvier 1978 des projets de **règles professionnelles** tendant à la protection des personnes à l'égard du traitement de données à caractère personnel. Ces règles professionnelles, peu répandues jusqu'ici, préfigurent la notion de code de conduite. On peut citer comme exemple de code de conduite reconnu conforme par la CNIL, le code relatif à l'utilisation de coordonnées électroniques à des fins de prospection directe établi par l'Union Française du Marketing Direct[26], ainsi que le code de déontologie de la communication directe électronique établi par Syndicat National de la Communication Directe[27].

Enfin, la CNIL a élaboré plusieurs **packs de conformité**[28] en concertation avec les acteurs de certains secteurs d'activité. Ces packs de conformité définissent des bonnes pratiques pour un secteur et peuvent contenir des mesures de simplification des formalités, des guides pratiques et pédagogiques, des tests de vérification de conformité à la loi. Ils illustrent la volonté de la CNIL de développer de nouveaux outils de régulation. Si ces packs s'appuient sur divers instruments juridiques aujourd'hui remis en cause par le GDPR (normes simplifiées, autorisations uniques, recommandations notamment), il est probable que la CNIL s'inspire de cette approche dans la future procédure d'adoption des codes de conduite : même si la CNIL et les autres autorités de contrôle agiront formellement par « délégation », il ne fait pas de doute que les codes de conduite seront des outils soumis à un encadrement strict de la part de ces autorités.

Les certifications, labels et marques

La Directive 95/46/CE ne prévoyait pas de mécanisme de certification. Cependant, au niveau national, la CNIL peut délivrer des labels à des produits ou procédures tendant à la protection des personnes à l'égard du traitement de leurs données à caractère personnel. Le GDPR consacre les mécanismes de certification, labels et marques et, les Etats membres, les DPA, le comité européen de la protection des données et la Commission sont invités à encourager la mise en place de ces mécanismes[29]. La certification ainsi que les labels et marques doivent permettre d'attester de la conformité au GDPR des traitements poursuivis par les responsables de traitement ou les sous-traitants. Ces mécanismes peuvent également être utilisés pour démontrer l'existence de garanties appropriées pour les responsables de traitement ou sous-traitants n'entrant pas dans le champ d'application du GDPR ou dans le cadre de transfert de données vers des Etats tiers en l'absence de décision d'adéquation.

---

26 Code relatif à l'utilisation de coordonnées électroniques à des fins de prospection directe, Union Française du Marketing Direct (disponible en ligne : http://www.ufmd.org/file/125350/) déclaré conforme à la loi Informatique et Libertés par la CNIL dans une délibération n°2005-051 du 30 mars 2005.

27 Code de déontologie de la communication directe électronique, Syndicat National de la Communication Directe (disponible en ligne : http://www.sncd.org/deontologie/code-de-deontologie-electronique-du-sncd/) déclaré conforme à la loi Informatique et Libertés par la CNIL dans une délibération n°2005-047 du 22 mars 2005.

28 Pack de conformité compteurs communicants (disponible en ligne :

https://www.cnil.fr/sites/default/files/typo/document/Pack_de_Conformite_COMPTEURS_COMMUNICANTS.pdf), pack de conformité logement social (disponible en ligne:

https://www.cnil.fr/sites/default/files/typo/document/PackConf_LOGEMENT_SOCIAL_web.pdf) et pack de conformité assurance (disponible en ligne: https://www.cnil.fr/sites/default/files/typo/document/PACK_ASSURANCE_complet.pdf); pack de conformité véhicules connectés publié le 17 octobre 2017 (disponible en ligne: https://www.cnil.fr/sites/default/files/atoms/files/pack_de_conformite_vehicule_connecte.pdf).

[29] Articles 42 et 43 du GDPR

Thaima Samman
Associée fondatrice
Cabinet SAMMAN

Les certifications et les labels ont vocation à jouer un rôle de premier ordre dans la mise en œuvre du GDPR car ils présentent de réels avantages pour toutes les parties prenantes : les entreprises certifiées mais également les autorités de contrôle et, plus important encore, les individus. Les mécanismes de certification, comme les codes de conduite, sont également une illustration de la transformation de la protection des données personnelles vers des mécanismes d'auto-régulation.

Ces outils ont pour vocation non seulement d'aider les entreprises à se conformer au GDPR mais également à démontrer leur conformité à ce règlement que ce soit pour certains ou pour l'ensemble de leurs services, produits ou activités. Par ailleurs, les certifications devraient être adaptées à toute taille d'entreprises, de la PME à l'entreprise multinationale. Bien que le GDPR ne le prévoit pas expressément (contrairement à ce qui existe pour les codes de conduite), l'implication des entreprises concernées dans l'élaboration des certifications et labels, au côté du régulateur, en France la CNIL, semble indispensable au succès et à l'effectivité de ces dernières.

Si certains de ces outils d'auto-régulation n'existeront qu'au niveau national, ils ont, par ailleurs, tous vocation à être harmonisés et/ou reconnu au niveau européen avec pour objectif la création d'interopérabilité avec les outils de conformité existants dans d'autres régions du monde.

L'adhésion à un mécanisme de certification est volontaire et transparente. Elle ne diminue pas la responsabilité du responsable de traitement ou du sous-traitant mais elle peut être prise en compte par l'autorité de contrôle en cas de sanctions : c'est-à-dire que la certification aura vraisemblablement un effet atténuant sur les sanctions dans la mesure où le responsable du traitement ou le sous-traitant aura respecté les prescriptions de la certification. C'est aussi un gage de confiance pour les responsables de traitement devant choisir des sous-traitants présentant des garanties suffisantes de protection des données.

La certification constitue un outil efficace de :

- Conformité au GDPR ;
- Démonstration du respect des obligations du GDPR ;
- Déclinaison opérationnelle du GDPR ;
- Facilitation des relations contractuelles : la certification offre un cadre fiable et vérifiable pour les opérations de traitement des données, particulièrement pertinent pour les opérations de cloud computing où un audit individuel ne serait pas possible ;
- Communication avec les tiers, les personnes concernées et les DPA. La certification permet de construire une relation de confiance ;

- Transfert : les certifications constituent des garanties appropriées pour les transferts hors de l'UE sous réserve de l'engagement contraignant et exécutoire d'appliquer ces garanties appropriées, y compris en ce qui concerne les droits des personnes concernées. Notamment, une telle certification ne nécessite pas une autorisation préalable au transfert.

La certification peut être délivrée, pour une période maximale de trois ans, par un organisme spécialement agréé par l'autorité de contrôle (l'organisme national d'accréditation (COFRAC) pourrait potentiellement jouer ce rôle) voire le comité de protection des données. Le comité européen de la protection des données centralisera dans un registre à disposition du public tous les mécanismes de certification et les marques. La Commission quant à elle peut, par voie d'acte délégué, préciser les critères et exigences à prendre en considération lors de l'élaboration des mécanismes de certification. Elle peut, par voie d'acte d'exécution, fixer des normes techniques pour les mécanismes de certification, ainsi que des marques et labels. La CNIL souhaite ainsi être en amont dans la production de référentiel, et tout à fait en aval au moment du contrôle du respect des certifications, labels ou marques. Plusieurs organismes comme l'AFNOR ou Bureau Veritas ont exprimé leur intérêt à devenir organisme de certification.

Il n'existe pas encore de certification GDPR. Cependant, la CNIL propose plusieurs labels, dont le label « Gouvernance Informatique et Libertés », le label « Formation » ou encore le label « coffre-fort numérique »[30].

La CNIL a publié en septembre une mise à jour des labels formation et gouvernance pour prendre en compte les exigences du GDPR et pour permettre aux organismes labellisés d'adapter dès que possible leurs procédures et produits labellisés. La mise à jour des référentiels en matière de procédure d'audit et de coffre-fort numérique est prévue pour fin 2017.

Le label « Gouvernance Informatique et Libertés » a vocation à aider les organismes privés et publics à mettre en œuvre la protection des données et à rendre compte de l'action qu'ils mènent en matière de gouvernance des données à caractère personnel. Cette gouvernance est définie comme l'ensemble des mesures, des règles et des bonnes pratiques qui permettent l'application des lois et règlements pour la gestion de ces données, et qui permettent de préciser les responsabilités qui interviennent dans cette gestion. Fondé sur les normes ISO/IEC 27001 :2013 sur les systèmes de management de la sécurité de l'information et ISO/IEC 29190 :2014 sur la maturité dans le domaine de la protection de la vie privée, le label a été élaboré en prenant en compte le projet de règlement européen relatif à la protection des données à caractère personnel.

Il constitue donc un outil intéressant pour se préparer à la transition vers le GDPR.

Le « label coffre-fort numérique » adopté par la CNIL par une délibération du 23 janvier 2014 valide les services de coffre-fort numérique qui répondent à l'objectif de conversation sécurisée et de protection des données à caractère personnel contenues dans un coffre-fort de telle sorte que ces dernières ne soient accessibles qu'à leur utilisateur et aux personnes physiques spécialement mandatées par ce dernier. L'adhésion à un tel label peut permettre également de se préparer au GDPR.

---

[30] CNIL, délibération n° 2014-500 du 11 décembre 2014 portant adoption d'un référentiel pour la délivrance de labels en matière de procédures de gouvernance Informatique et libertés.

Particulièrement adapté aux fournisseurs de services de cloud computing, le label EuroPriSe, auquel la CNIL a contribué, a fait l'objet d'une mise à jour pour prendre en compte les nouvelles obligations issues du GDPR.

Les conditions du succès des certifications

Les certifications, labels et marques devraient :

- Comprendre des incitations pour accélérer leur adoption par les entreprises ;
- Etre harmonisés au niveau européen : il faut éviter la multiplication des types de certification sous peine de diminuer leur lisibilité et leur efficacité auprès des personnes concernées. Les éventuelles certifications nationales devraient être des déclinaisons de certifications de niveau européen.
- Prendre en compte les autres certifications ou standards existants comme les certifications ISO ou les règles pour les transferts internationaux de données de l'APEC.
- Prévoir une coordination avec les BCR : l'adoption de BCR devraient faciliter l'obtention d'une certification et réciproquement ;
- Pouvoir être adaptés en fonction de la taille de l'entreprise et de son activité.

Les règles d'entreprise contraignantes (ou "BCR")

Les BCR sont des règles contraignantes qui s'imposent à l'ensemble des entités concernées d'un groupe et confèrent aux personnes concernées des droits opposables en matière de protection de leurs données à caractère personnel. Elles sont approuvées par les autorités de contrôle dans le cadre d'un processus très encadré. Elles constituent un investissement pour faciliter les flux de données au niveau mondial au sein d'un groupe.

Cependant**, les BCR ne doivent pas être vues comme étant simplement un mécanisme de transfert, il s'agit d'un véritable outil de conformité au GDPR de façon harmonisée au niveau du groupe.**

Les BCR peuvent être considérées comme une véritable certification de l'entreprise bénéficiaire. Outil de communication, les BCR permettent de gagner la confiance des clients et d'assurer les personnes concernées du bon niveau de protection des données à caractère personnel par l'entreprise.

Le G29 d'ailleurs travaille sur l'actualisation des référentiels en matière de BCR afin qu'ils puissent aller au-delà des questions de garantie offertes en matière de transfert.

Nathalie LANERET
Responsable de la protection des données
Capgemini

GDPR, le point de vue de Capgemini

Comment le Groupe Capgemini a-t-il abordé sa mise en conformité avec le GDPR ?

Le Groupe Capgemini a intégré la problématique de la protection des données personnelles et donc de la mise en conformité au GDPR au sein de son programme de cybersécurité. La sécurité est en effet la pierre angulaire de tout programme de protection des données personnelles.

Dans ce cadre, Capgemini a établi un socle 64 règles minimales de sécurité qui doivent être appliquées par toutes les entités du groupe dans tous les pays et qui sont répercutées sur les cocontractants.

Capgemini met en place le GDPR en s'appuyant sur ses BCR controller et processor, ce qui lui permet de mutualiser les efforts. Grâce aux BCR, Capgemini a mis en place une gouvernance interne qui comporte notamment la nomination d'un DPO au niveau du Groupe ainsi que la tenue de réunions de suivi régulières sur le niveau d'avancement de la mise en conformité.

De façon générale, de par leurs prérequis organisationnels et leur approche transversale, les BCR permettent d'établir les bases du programme de conformité interne de l'entreprise en matière de protection des données personnelles, lequel est rendu nécessaire dans le cadre de la mise en œuvre du principe d'accountability au titre du GDPR.

A ce titre, il importe que les BCR soient considérées comme un outil d'accountability privilégié au titre de la mise en œuvre du règlement.

Pour réussir la mise en œuvre du GDPR, il convient d'adopter une approche dynamique et non statique de la compliance, tout comme c'est le cas en matière de sécurité.

Focus transferts internationaux de données

Les transferts internationaux de données sont encadrés par le GDPR. Celui-ci prévoit 5 modalités principales de transferts :

- Une décision d'adéquation de la Commission ;
- La fourniture de garanties appropriées qui peuvent être :
    - Des clauses types de protection des données adoptées ou approuvées par la Commission,
    - Un code de conduite ou une certification assortie de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant d'appliquer les garanties appropriées, notamment en ce qui concerne les droits des personnes concernées ; ou
    - Des clauses contractuelles entre le responsable du traitement ou le sous-traitant et le responsable du traitement, le sous-traitant ou le destinataire des données à caractère personnel dans le pays tiers sous réserve d'une autorisation ;
    - Les règles d'entreprises contraignantes ou Binding Corporate Rules ("BCR").

A défaut de décisions d'adéquation ou de garanties appropriées, les transferts demeurent possibles pour certaines situations particulières. Ces dérogations sont strictement encadrées et reposent sur des conditions qui peuvent être difficiles à remplir ou à démontrer :

- Le consentement explicite de la personne concernée qui a été préalablement informée des risques liés au transfert ;
- Transfert nécessaire à la conclusion ou à l'exécution d'un contrat bénéficiant à la personne concernée ;
- Motifs d'intérêt public ;
- Constatation ou exercice d'un droit en justice ;
- Transfert nécessaire pour des motifs d'intérêts vitaux de la personne concernée ou d'autres personnes si la personne concernée ne peut donner son consentement ;
- Transfert à partir d'un registre destiné à donner des informations au public sous certaines conditions ;
- Dérogation pour les transferts non répétitifs sous les conditions suivantes :
    - Ne concernent qu'un nombre limité de personnes ;
    - Nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement ;
    - À conditions que les intérêts ou les droits et libertés de la personne concernée ne prévalent pas sur ces derniers
    - Le responsable du traitement a évalué toutes les circonstances entourant le transfert de donnée
    - Le responsable de traitement a adopté en conséquence des garanties appropriées ;
    - Le responsable de traitement informe l'autorité de contrôle et la personne concernée.

Attention !

Une décision de justice ou une décision administrative d'un pays tiers ne peut contraindre un responsable de traitement ou un sous-traitant à divulguer des données à caractère personnel sauf accord entre les Etats ou l'Etat et l'UE.

Contenu des BCR

Le contenu des BCR est largement précisé par le règlement. Ainsi, les BCR doivent au moins comprendre :

- La structure et les coordonnées du groupe ;
- Les transferts de données, y compris les catégories de données à caractère personnel, le type de traitement et ses finalités, le type de personnes concernées et les pays tiers concernés ;
- Leur caractère contraignant tant en interne que vis-à-vis de l'extérieur ;
- L'application des principes généraux relatifs à la protection des données (notamment limitation de la finalité, minimisation des données, limitation des durées de conservation des données, privacy by default, privacy by design, etc.) ;
- Les droits des personnes concernées et les moyens d'exercer ces droits ;
- L'acceptation, par le responsable du traitement ou le sous-traitant de l'engagement de sa responsabilité pour toute violation des règles d'entreprise contraignantes par toute entité concernée non établie dans l'Union ;
- La manière dont les informations sur les règles d'entreprise contraignantes, sont fournies aux personnes concernées ;
- Les missions du DPO ou de toute autre entité chargée de la surveillance du respect des BCR et du suivi de la formation et du traitement des réclamations ;
- Les procédures de réclamation ;
- Les procédures de contrôle du respect des BCR au sein du groupe (mise en place d'audits et de reporting) ;
- Les mécanismes mis en place pour communiquer notamment à l'autorité de contrôle les modifications apportées aux règles et les consigner ;
- Les mécanismes de coopération avec l'autorité de contrôle s'agissant de la mise en œuvre des BCR ;
- Les mécanismes de communication à l'autorité de contrôle de toute modification d'ordre juridique venant d'un pays tiers et susceptible d'avoir un effet négatif sur les BCR ;
- La formation en matière de protection des données du personnel.

Conclusion sur les outils de confiance

Le GDPR modifie les obligations et responsabilités des différents acteurs et encadre beaucoup plus strictement les contrats devant être conclus entre eux. Cela suppose ainsi de procéder à une revue des contrats en cours comportant des traitements de données à caractère personnel d'ici le 25 mai 2018 et, le cas échéant d'envisager leur renégociation, voire de négocier un contrat spécifique pour le traitement des données, ce qui contraste avec la pratique actuelle où, bien souvent, des mentions assez générales ou des clauses de styles figurent dans les contrats de services, dont les contrats cloud.

Avant de pouvoir rédiger toute clause de protection des données à caractère personnel dans un contrat, il faudra déjà s'assurer que l'on est bien en présence d'un traitement de données à caractère personnel soumis au GDPR (voir Focus GDPR supra). Il faudra ensuite comprendre et analyser le type de relation en cause : responsable de traitement à responsable de traitement ? Responsable de traitement à sous-traitant ? Responsabilité conjointe ? En effet la rédaction des clauses diffère selon le type de relation.

Christian LITAUDON
Marketing Produits et Services
SAGE

GDPR, le point de vue Sage

La protection des données personnelles est un sujet déjà actuel et adressé par la CNIL. Le nouveau Règlement Général sur la Protection des Données applicable en Mai 2018, représente un enjeu de taille pour toutes les entreprises. Il vise à renforcer les obligations relatives aux traitements des données personnelles des résidents de l'UE et accroit les exigences en matière de collecte / traitement / conservation/ sécurité. Aujourd'hui, Sage a d'ores et déjà cerné l'ampleur des bouleversements portés par ce nouveau texte et enclenché les premières étapes du processus de mise en conformité.

Il résulte du GDPR de nouvelles obligations pour les entreprises qui devront être en mesure de justifier quelles données elles exploitent, à quelles fins et avec quels processus d'encadrement et de contrôle.

De nombreux outils d'accompagnement à la prise en compte du GDPR sont disponibles auprès des institutions, fédérations, syndicats professionnels, éditeurs et intégrateurs, etc. qui recommandent tous une gestion en mode projet de la transformation (depuis la désignation d'un pilote (Délégué à Protection des Données / DPO), jusqu'à la cartographie des données, l'adressage des risques, l'organisation des processus internes et la documentation associée).

Ce nouveau dispositif marque la reconnaissance de la valeur de la « data », les contre effets et risques de leurs manipulations à des fins non délimitées, mais aussi une volonté de sensibiliser (et contraindre) les entreprises à une gestion de cet actif afin d'instaurer un climat de « confiance » entre les individus et les acteurs économiques

Pour autant chacun en aura-t-il les moyens ? Comment les plus petites entreprises vont-elles pouvoir appréhender ce changement de paradigme ? L'inversion de la charge de la preuve est-elle « tenable » pour tous- hier déclaration préalable, demain démonstration de la conformité à tout moment jusqu'à des amendes de 2 à 4% du CA ? Enfin tous les domaines ont-ils la même exposition ? (Comptabilité-Finance / Paie-RH /…)

Autant de questions sur lesquelles notre entreprise porte sa réflexion. De manière plus globale, Sage examine et évalue les problématiques posées par la mise en conformité avec le GDPR et vulgarise le dispositif auprès de ses partenaires et clients pour proposer des outils et services qui favoriseront et soutiendront la démarche de conformité menée par ses utilisateurs.

Les outils contractuels et les responsabilités

Le GDPR revoit en profondeur l'équilibre des relations entre responsables et sous-traitants. En premier lieu, il enrichit les statuts par l'introduction de la notion de responsables "conjoints" d'un traitement, à côté des notions classiques de responsable de traitement et sous-traitant. En second lieu, il renforce les responsabilités de l'ensemble des acteurs et contraint à clarifier les rôles et obligations de chacun dans les contrats, par l'inclusion de clauses obligatoires.

L'ambition de fournir un cadre contractuel adapté à l'économie contemporaine de la donnée

En dehors des personnes dont les données sont traitées, les parties peuvent agir en tant que responsable de traitement, sous-traitant ou, nouveauté du GDPR, en tant que responsables conjoints de traitement.

Ces notions doivent être interprétées de manière à la fois autonome, en ce sens que leur interprétation relève principalement de la loi et non du choix des parties, et fonctionnelle, car la qualification vise à attribuer les responsabilités aux personnes selon leur rôle de fait et repose par conséquent sur une analyse factuelle. Le risque est de "mal" qualifier une partie. Ceci pourra être le cas lorsque le régime de responsabilité retenu pour encadrer son intervention ne sera pas celui retenu ni appliqué par les autorités. Ces dernières pourraient alors statuer sur la responsabilité de l'intervenant a posteriori sur la seule base des textes et de la jurisprudence, en décalage complet avec ce que les parties auront prévu, créant ainsi une insécurité juridique rendant vains les efforts des parties à encadrer leur relation par le contrat.

a) La nouvelle typologie des statuts dans le GDPR

- **Les statuts classiques de responsable et sous-traitant**

Le GDPR[31] reprend la définition fonctionnelle classique de responsable du traitement, à savoir « *la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. (…)* ». C'est donc schématiquement l'entité qui détermine le « pourquoi » et le « comment » de tout traitement. Le sous-traitant est toujours la personne physique ou morale qui « *traite des données pour le compte du responsable de traitement* » et sur ses instructions.

Si les définitions paraissent simples, la mise en pratique est plus délicate face à des scénarios divers, dans lesquels des responsables du traitement et des sous-traitants interviennent à des degrés d'autonomie et de responsabilité variés.

Lorsqu'une société fait appel à une société tierce pour prendre en charge un traitement de données, on a tendance à considérer, par réflexe, cette dernière comme sous-traitant. Mais en pratique les situations ne sont pas aussi binaires. L'émergence du cloud et de services techniquement complexes ont vu apparaître des offres en ligne, standardisées et non négociables, ou encore requérant la maîtrise de technologies particulières, qui ont modifié l'équilibre des rôles. Le client peut être un simple bénéficiaire de services dont il n'a pas la maîtrise et n'est pas nécessairement en position de donner des directives à son prestataire ou d'exercer un contrôle sur le service rendu. De son côté, le prestataire peut être contraint de

[31] Article 4, 7 du GDPR

fortement standardiser son offre pour pérenniser un modèle économique requérant expertise, souplesse et puissance opérationnelle.

Le G29 a publié un long avis en février 2010 « sur les notions de responsable de traitement et de sous-traitant »[32] selon lequel le responsable de traitement est l'organisme qui exerce une influence de fait sur les finalités poursuivies par le traitement de données et un contrôle réel sur ses modalités de mise en œuvre : « *la détermination de la finalité du traitement est réservée au « responsable du traitement ». Toute personne qui prend cette décision est donc un responsable du traitement (de fait)* ».

En revanche, la détermination de certains « moyens » du traitement peut être déléguée par le responsable du traitement, pour autant qu'elle concerne des questions techniques ou d'organisation et dès lors qu'il s'agit de questions secondaires (choix du matériel informatique utilisé, logiciel proposé etc.). Il convient donc de distinguer clairement ces questions secondaires des questions sensibles fondamentales pour la licéité du traitement (durée de conservation des données, personnes ayant accès aux données, etc.) qui restent réservées au responsable du traitement.

La qualification de sous-traitant devra être attribuée à toute entité juridique distincte du responsable du traitement qui traite des données à caractère personnel pour le compte de ce dernier. De plus, pour une même opération, une entité pourra agir à la fois comme responsable de traitement et comme sous-traitant en fonction des finalités en cause.

La CNIL a développé un faisceau d'indices[33] pouvant servir à la qualification des parties :

Indices	Le prestataire pourra être qualifié de sous-traitant	Le prestataire pourra être qualifié de responsable de traitement
Niveau d'instruction : Le niveau d'instruction donné par le client indique le degré d'autonomie laissé au prestataire. Par conséquent il permet d'apprécier s'il est plus qu'un simple sous-traitant.	Le contrat de prestation et les directives données au cours de son exécution sont très précis dans les instructions et le niveau de qualité demandé.	Le contrat de prestation et les directives données au cours de son exécution sont très généraux en termes d'instructions et laissent une grande autonomie au prestataire.
Niveau de contrôle : Le degré de contrôle du client sur les prestations et sur les données révèle également la liberté dont peut disposer le prestataire.	La société audite son prestataire et lui demande des comptes régulièrement.	La société laisse le prestataire réaliser ses prestations et le laisse libre d'utiliser les données comme bon lui semble.
Transparence : Le prestataire se présente-t-il sous son nom propre ou sous le nom de son client ? Peut-il réutiliser les données à des fins qui lui sont propres ?	L'employé du prestataire se présente sous le nom du client et ne réutilise pas les données pour son propre compte.	Le prestataire se présente sous son propre nom et réutilise les données à des fins qui lui sont propres.

[32] Avis WP 169 du 16 février 2010 disponible à l'adresse : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fr.pdf

[33] Guide transferts de données à caractère personnel hors Union européenne publié en novembre 2012, disponible à : https://www.cnil.fr/sites/default/files/typo/document/GUIDE-transferts-integral.pdf

Expertise : Un prestataire qui dispose d'une expertise peut décider des moyens à mettre en place dans le cadre de la réalisation des prestations.	Le prestataire utilise l'infrastructure technique du client pour réaliser sa prestation.	Le prestataire expert dans son domaine impose des outils au client qui n'a pas de pouvoir de négociation, ne peut les modifier parce qu'il n'a pas les compétences, ou parce que l'outil est un outil qui ne fait pas l'objet d'un développement spécifique.

Source : CNIL

En plus d'influer sur la responsabilité des acteurs, la qualification des parties permet de ventiler les obligations pesant sur chacune d'elles.

Loïc Rivière
Délégué général
TECH IN France

Doit-on distinguer les acteurs B2B et les acteurs B2C ?

Tous peuvent être concernés par le GDPR, les contrats B2B n'échappant pas de ce seul fait à la réglementation de protection des données personnelles. Le périmètre d'application peut néanmoins différer. En B2B, il pourrait être nécessaire de mettre l'accent sur les relations entre intervenants (partage des responsabilités) et les questions techniques (qualité de service, sécurité et confidentialité, gestion des risques de violations de données, etc.). Cependant, même en présence d'une pure relation B2B, il s'avérera le plus souvent nécessaire de clarifier les rôles des parties vis-à-vis des personnes dont les données sont traitées : qui centralise et répond aux demandes d'exercice des droits, qui les met en œuvre, documente et rapporte à l'autre partie, etc.

Doit-on distinguer les acteurs du cloud/hors cloud ?

Même hors cloud (i.e., un éditeur de logiciel qui ne traite pas de données, mais se limite à livrer un logiciel à un client), le sujet des données personnelles ne doit pas être ignoré. Même si le prestataire n'intervient en rien dans les traitements effectués par son client, l'obligation d'information, de conseil et d'alerte peut néanmoins s'appliquer si le logiciel permet d'effectuer ou d'interagir avec des traitements de données à caractère personnel effectués par ailleurs. Il pourrait être nécessaire de permettre au client de traiter les données de manière conforme au GDPR, le cas échéant par application du principe de privacy by design (par exemple, un logiciel CRM doit contenir un dispositif de gestion des durées de conservation et de gestion des consentements), ou encore de l'informer des exigences de conformité, selon les circonstances. du règlement.

Pour réussir la mise en œuvre du GDPR, il convient d'adopter une approche dynamique et non statique de la compliance, tout comme c'est le cas en matière de sécurité.

- **L'introduction d'un régime de responsables conjoints d'un traitement**

Si la notion de responsables conjoints d'un traitement n'est pas fondamentalement nouvelle, le simple fait qu'elle figure expressément dans la loi lui donnera une impulsion nouvelle et en amplifiera l'usage, pour développer des partenariats d'analyse et d'exploitation de données, incluant des données personnelles.

Une notion nouvelle

La notion de responsables conjoints d'un traitement ne figure pas dans la loi Informatique et Libertés, bien qu'elle apparaisse dans la directive européenne de 1995 et qu'elle ait été utilisée par la CNIL.[34]

Elle n'est pas explicitée ou illustrée dans le GDPR, qui se contente de poser que "lorsque deux responsables du traitement ou plus déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement" et qu'ils doivent préciser leur relation par voie d'accord.[35]

La structuration de leur relation est donc libre, sous réserve d'un repère majeur : la transparence vis-à-vis des personnes concernées. Le GDPR leur impose en effet de définir "de manière transparente leurs obligations respectives aux fins d'assurer le respect des exigences du présent règlement", notamment en ce qui concerne l'information et les droits des personnes concernées.

Béatrice Delmas-Linel
Associée gérante
Osborne Clarke

> *Le GDPR ouvre la voie à une nouvelle façon d'envisager les partenariats pour l'analyse et l'exploitation de données qui ne se limitent pas à une relation responsable à sous-traitant, parfois artificielle. Cette ouverture se double d'une grande liberté sur l'économie contractuelle à mettre en place, dès lors que les droits des personnes concernées sont assurés.*
>
> .

Un cadre contractuel à inventer

On peut imaginer que ces relations contractuelles se construiront sur la base de l'existant, à savoir les relations entre responsable et sous-traitant, et en faisant varier les responsabilités de chacun en fonction de leur implication fonctionnelle ou technique dans un projet. Par exemple, en présence d'un contrat d'adhésion pour des services cloud (software as a service, platform as a service, etc.) pour lesquels le client n'a aucune marge de négociation ni les compétences et moyens pour exercer une quelconque influence sur les services, y compris sur des questions fondamentales comme la sécurité des données, il ne peut être exclu que le

---

34 Délibération n°SAN – 2017-006 du 27 avril 2017 dans laquelle la CNIL qualifie les sociétés Facebook Inc. Et Facebook Ireland de responsables conjoints de traitement.

35 Art. 26.

prestataire soit considéré comme responsable conjoint de traitement, comme le confirme la CNIL dans ses recommandations pour les entreprises qui envisagent de souscrire à des services de cloud computing (précité). Cette qualification ne correspond pas nécessairement à la pratique contractuelle dominante. Un travail de sensibilisation et de refonte des contrats est donc nécessaire.

Pour ouvrir à davantage de configurations que les seuls services en nuage, des situations de coresponsabilité pourraient être mises en œuvre en intragroupe, lorsqu'une entité commune gère des projets globaux à forte dimension technique ou stratégique au bénéfice de l'ensemble des entités du groupe. Il pourrait encore s'agir de contrats conclus entre sociétés non liées, permettant de démarrer des projets communs d'analyse et d'exploitation de données -- avant de consolider la relation dans le cadre d'une joint venture.

Par ailleurs, il convient de noter que les situations de coresponsabilité doivent être détectées suffisamment en amont pour pouvoir les organiser par contrat.

Or, c'est une analyse relativement nouvelle en droit français, et qui n'a sans doute pas été envisagée dans les contrats en cours ou dans les projets en discussion actuellement. Il convient donc par précaution, dans les partenariats étroits où le rôle du sous-traitant est plus large qu'une simple exécution d'instructions – ou pourrait évoluer en ce sens – d'être vigilant sur une telle évolution afin d'adapter le cadre contractuel en tant que de besoin, voire de prévoir dans le contrat même des clauses de revoyure ou de réévaluation périodique des rôles et responsabilités.

Enfin et pour finir, le GDPR prévoit que le droit national puisse qualifier les droits et obligations des responsables conjoints, disposition qui pourrait permettre aux autorités nationales de prévoir des règles spécifiques à certains secteurs ou certains contrats, comme la CNIL l'avait fait pour le cloud par le passé. Il conviendra donc de suivre les législations nationales à cet égard.

b) Les nouvelles obligations pesant sur les acteurs

Le GDPR contraint ainsi à reprendre les contrats comportant des traitements de données personnelles et à les réévaluer au regard des nouvelles règles, afin d'en adapter les termes aux nouvelles obligations, voire à redistribuer les rôles en présence d'une situation de responsabilité conjointe.

- **Contrats de sous-traitance**

Sous l'empire de la loi informatique et libertés, la relation entre responsable de traitement et sous-traitant est relativement peu encadrée. Au plus, la loi Informatique et Libertés impose aux responsables de traitement de choisir un sous-traitant qui présente « *des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité (...)* »[36]. Cette exigence est naturellement maintenue avec le GDPR, mais le contenu de cette relation est beaucoup plus détaillé et les contrats les liant doivent prévoir de très nombreuses clauses impératives.

[36] Article 35 de la loi Informatique et Libertés.

Avant l'entrée en vigueur du règlement :

Sous l'empire de la loi du 6 janvier 1978 (article 35 alinéa 4), le contrat entre responsable de traitement et sous-traitant doit préciser les obligations du sous-traitant en matière de :

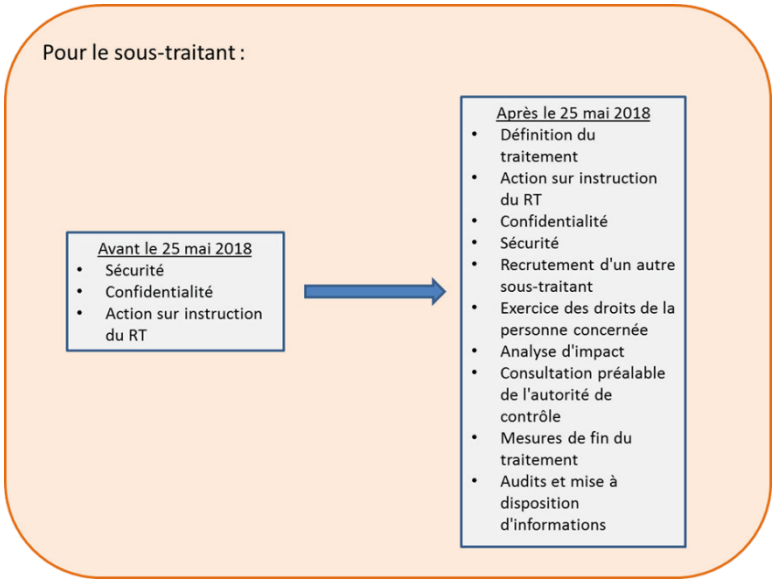
- Sécurité des données traitées,
- Confidentialité des données,
- Le fait que le sous-traitant ne puisse agir que sur instruction du responsable de traitement.

Pour les contrats cloud, la CNIL a publié fin 2012 un guide détaillé dans lequel la Commission recommande l'insertion de nombreuses clauses dans les contrats liant entreprises clients aux prestataires cloud, au titre desquelles figurent les informations relatives aux traitements, la remontée des plaintes et failles de sécurité, le recours à la sous-traitance, les procédures permettant de respecter les droits des personnes concernées, la durée de conservation des données, l'audit du prestataire par le client, etc.

De plus, la CNIL n'hésite pas à imposer des obligations détaillées à cette relation sur le fondement des obligations générales précitées, en sanctionnant les violations de données dès avant l'entrée en vigueur du GDPR, les sanctions ayant été renforcées en la matière par la loi République Numérique du 7 octobre 2016.[37]

Après l'entrée en vigueur du règlement :

Les obligations du sous-traitant sont substantiellement accrues.



Source : Osborne Clarke

[37] Délibération n° SAN-2017-010 du 18 juillet 2017 prononçant une sanction pécuniaire à l'encontre de la société HERTZ France ; délibération n°SAN-2017-011 du 20 juillet 2017 prononçant un avertissement public à l'encontre de la société Ouicar.

Le contrat conclu entre le responsable et le sous-traitant doit définir les modalités du traitement[38] :

- L'objet du traitement,
- La durée du traitement,
- La nature du traitement,
- La finalité du traitement,
- Le type de données à caractère personnel traitées,
- Les catégories de personnes concernées.

En plus de ce descriptif, qui oblige à lui seul à un travail de recensement détaillé qui n'était pas requis auparavant, le GDPR prévoit une liste novatrice de clauses obligatoires[39].

Doivent ainsi être prévues contractuellement les obligations suivantes à la charge du sous-traitant :

- n'être autorisé à traiter les données que sur instruction documentée du responsable de traitement, sauf en cas d'obligation légale, auquel cas il doit en informer au préalable le responsable ;

- veiller à ce que les personnes autorisées à traiter les données soient engagées, contractuellement ou légalement, à une obligation de sécurité ;

- prendre toutes mesures requises pour assurer la sécurité du traitement ;

- respecter les dispositions du règlement concernant le recrutement d'un autre sous-traitant (autorisation du RT, transmission des obligations aux sous-traitant subséquents, etc.) ;

- aider le responsable du traitement, dans toute la mesure du possible, pour que celui-ci puisse donner suite aux demandes d'exercice de leurs droits par les personnes concernées (accès, rectification, suppression, portabilité, etc.) ;

- aider le responsable du traitement à remplir ses obligations en matière de sécurité des données et de réalisation des analyses d'impact ;

- aider le responsable du traitement à remplir ses obligations en matière de consultation préalable de l'autorité de contrôle en cas de risque élevé ;

- respecter les exigences du responsable du traitement à l'issue de la prestation de services de traitement (suppression ou restitution des données) et détruire - sauf obligation légale - les copies existantes des données traitées ;

- mettre à la disposition du responsable du traitement les informations nécessaires au contrôle du respect de ses obligations, permettre la réalisation d'audits par le responsable du traitement et informer immédiatement le responsable du traitement lorsqu'une instruction constitue une non-conformité.

---

[38] Article 28 § 3 du GDPR

[39] Article 28 § 3 du GDPR

Lise BRETEAU
Associée
Osborne Clarke

> *Vu le nombre, la nature et la complexité des clauses à négocier, il pourra se révéler nécessaire de prévoir, en plus du contrat de service, un document spécifique séparé consacré aux traitements des données à caractère personnel: avenant à un contrat en cours et, pour les nouveaux contrats, annexe au contrat principal, voire contrat séparé.*

- **Contrats de responsabilité conjointe**

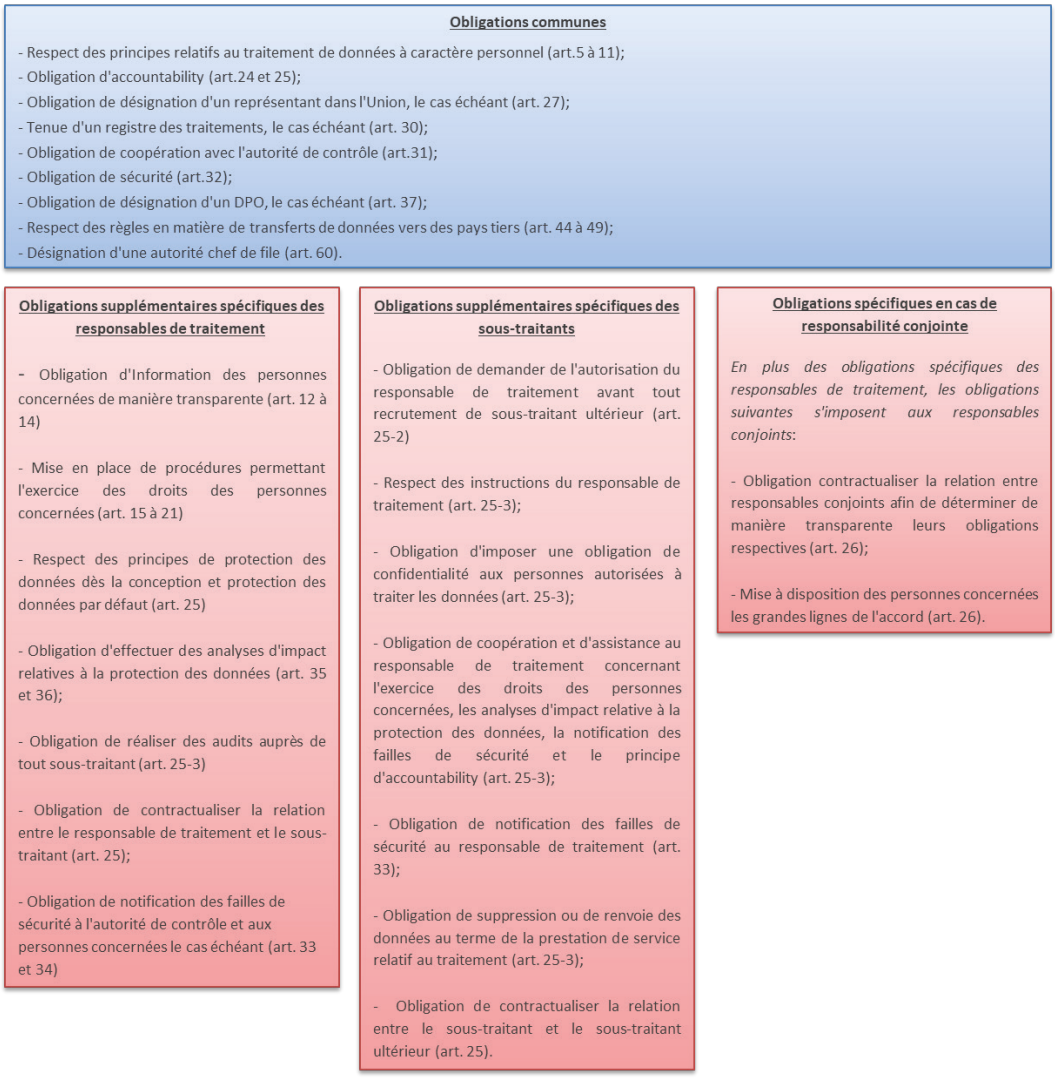
Les contrats organisant les relations entre responsables conjoints devront aborder l'ensemble des sujets soulevés dans les contrats de sous-traitance : application des principes de privacy by design et by default, études d'impact, audits, notification des violations, recours à des sous-traitants, instructions, confidentialité, coopération et assistance à la conformité, etc. Chacun de ces sujets devra toutefois être résolu de manière spécifique, les parties ne pouvant ici se reposer sur la logique des contrats de sous-traitance "contrôle vs. instructions".

En outre, un élément est plus particulièrement ciblé par le GDPR et devra recevoir une réponse claire dans les accords de coresponsabilité, à savoir l'information et l'exercice des droits des personnes concernées. C'est le point fondamental de la conformité de ces contrats.

Les parties doivent clairement organiser entre elles le "circuit" de l'exercice des droits par les personnes concernées. Ils doivent mettre à leur disposition "les grandes lignes" de leur accord. Ils peuvent enfin désigner un point de contact commun pour elles, sans que cela empêche les personnes d'exercer leurs droits "à l'égard de et contre" chacun d'eux.[40]

[40] Art. 26.

Les obligations pesant sur les acteurs



Source : Osborne Clarke

- **Les questions en suspens**

Quelle sanction si les contrats ne sont pas conformes ?

La question de la sanction en cas de non-inclusion ou de non-respect de ces clauses se pose. En l'absence de précision dans le règlement, on peut supposer que l'absence d'une clause obligatoire est sanctionnée par une amende administrative mais reste sans effet sur le contrat lui-même, ces clauses n'étant pas présentées comme des conditions de validité du contrat. Cependant, il convient d'être prudent car un traitement non conforme a déjà pu entraîner l'annulation d'une cession de fichier par le passé.[41]

La question de la personne qui encourt la sanction n'est pas non plus traitée par le texte du règlement. En l'absence de précision, il paraît prudent de considérer que le responsable de

[41] Civ. Com. 25 juin 2013, Bulletin 2013, IV, n° 108 : "tout fichier informatisé contenant des données à caractère personnel doit faire l'objet d'une déclaration auprès de la CNIL et (...) la vente par la société X d'un tel fichier qui, n'ayant pas été déclaré, n'était pas dans le commerce, avait un objet illicite."

traitement et le sous-traitant pourraient être sanctionnés aussi bien l'un et l'autre en l'absence d'une clause faisant porter la responsabilité sur l'une d'entre elles.

Le sujet de la mise en conformité des contrats en cours est, à cet égard, épineux.

En principe, tous les contrats doivent être conformes le 25 mai 2018. Il convient, dans ce contexte, de rédiger des avenants à circulariser auprès de l'ensemble des partenaires commerciaux, avec lesquels l'organisme est en contrat, afin de mettre en conformité les clauses en matière de données personnelles avec la nouvelle réglementation.

A minima, il convient de procéder avec ces contrats de la même manière que dans les efforts actuels de mise en conformité des traitements et des processus, à savoir auditer les contrats, cartographier et prioriser les efforts sur les relations les plus stratégiques et/ou risquées et mettre en place des étapes de mise en conformité, qu'il convient toujours de documenter et de tracer, dans la perspective de l'obligation d'*accountability*.

Quelle est la portée des obligations du sous-traitant dans son "assistance" à la conformité du responsable de traitement ?

Certaines clauses imposées par le GDPR font peser un certain nombre d'obligations assez vagues sur le sous-traitant (par exemple, « aider au respect des obligations du responsable de traitement en matière d'analyse d'impact », « aider au respect des obligations du responsable de traitement en matière de consultation préalable des autorités de contrôle », etc.). Il pourra être tentant, pour le sous-traitant, d'encadrer strictement ses obligations et d'en limiter au maximum le périmètre et, pour le responsable, de les formuler de la manière la plus large possible. Reste à savoir comment des clauses générales seront interprétées par les autorités. La sécurité des parties sera mieux assurée si elles parviennent à mettre en œuvre ces principes par des obligations précises, identifiées et mesurables.

Une autre question est de savoir si le sous-traitant est en droit de faire payer cette assistance. A notre sens, rien ne s'y oppose, dès lors qu'il ne s'agit pas pour le sous-traitant de se soustraire à ses obligations ni d'exiger une rémunération disproportionnée pour ses services.

De plus, de quels recours et quelle protection dispose le sous-traitant qui conseillerait au client de mettre en place ou d'opter pour certaines mesures de sécurité ou procédures si jamais le client s'y refusait ? Pour limiter ses risques en termes de responsabilité, le sous-traitant devra veiller à bien documenter ses échanges avec le client.

Jawaher ALLALA
CEO
Systnaps

GDPR, le point de vue de Systnaps

L'impact de ces obligations va bien plus loin que la simple protection des données à caractère personnel détenues au sein des Systèmes d'Informations d'entreprises. Elles touchent toutes les strates du SI de toute organisation : stratégiques, métiers, fonctionnels, applicatives, techniques et infrastructures obligeant les acteurs de cette transformation à revoir leurs politiques de données, leurs communications, leurs processus, leurs procédures et les mesures de sécurité misent en œuvre aussi bien techniques qu'organisationnelles afin d'assurer une protection adaptée à la criticité de détention des DCP qu'ils manipulent.

Notre lecture du GDPR avec notre prisme de spécialiste de la gouvernance de la donnée depuis 10 ans, nous a conforté dans l'idée que les autorités compétentes souhaitaient que les entreprises reprennent de façon loyale et transparente, le contrôle des données à caractère personnel qu'elles détiennent afin de mieux répondre aux droits fondamentaux du citoyen européen.

Ce n'est pas un exercice facile, dans la mesure où les acteurs internes et externes impactés sont nombreux (responsable de traitement, DPO, directeur des systèmes d'information, sous-traitant) et au vu du nombre d'applications hétéroclites détenues au sein de l'organisation.

Acteur dans la gestion du cycle de vie de la donnée, c'est tout naturellement que nous avons impliqué l'ensemble de nos collaborateurs et fournisseurs dans une démarche de conformité au RGPD en 2016 en choisissant de se faire labélisé CNIL - Gouvernance de la donnée /GDPR.

Quoi de plus évident pour répondre aux exigences d'une autorité de contrôle que de se confronter au référentiel d'une labélisation et en même temps, faire reconnaitre la qualité de nos procédures, et proposer en totale conformité méthodologies et solutions à nos clients.

Une mise en conformité n'est pas un projet ponctuel mais une obligation permanente qui doit s'inscrire naturellement dans un processus plus large qu'est celui de la gouvernance de la donnée devenue incontournable dans toutes organisations.

Contrainte pour certains, opportunités pour d'autres, ce règlement n'est rien de moins qu'un tremplin vers un niveau d'exigence plus élevé de protection face aux nouvelles menaces et à la cybersécurité.

Cas pratiques et exemples de clauses

a) Je suis responsable de traitement

L'entreprise A traite des données à caractère personnel de ses clients pour les besoins de la relation commerciale. Sa solution de CRM lui est fournie par un prestataire B, en mode SaaS, depuis 2010.

Dans un tel scénario, il est probable que l'entreprise A soit qualifiée de responsable de traitement et que le prestataire B soit qualifié de sous-traitant. En vertu de l'article 28 du GDPR, sa relation avec le prestataire B doit être contractualisée.

Un exemple de clauses devant être incluses dans un contrat conclu entre un responsable de traitement et un sous-traitant est proposée en exemple 1. Ces clauses sont rédigées pour favoriser le responsable du traitement.

b) Je suis sous-traitant

Le prestataire B, fournisseur de solution de gestion commerciale clients, souhaite revoir ses conditions générales de services afin de les mettre en conformité avec le GDPR.

Un exemple de clauses "données personnelles" qui pourrait être incluses dans des conditions générales d'un prestataire sous-traitant est proposée en exemple 2. Cette proposition est le miroir de l'exemple 1, mais dans une approche qui se veut plus favorable au sous-traitant.

c) Nous sommes responsables conjoints

L'entreprise C exploite une place de marché en ligne ouverte à des vendeurs tiers et leurs acheteurs. L'entreprise C souhaite analyser les données des internautes et visiteurs de sa plateforme, pour vendre à ses vendeurs D ces résultats d'analyse marketing, et leur proposer de cibler plus finement leur clientèle en envoyant des publicités et offres promotionnelles personnalisées. Pour ce projet, elle travaille avec un prestataire E qui développe un outil d'analyse de données (data analytics).

Selon les rôles et responsabilités des différents intervenants, il peut y avoir une coresponsabilité sur les traitements entre l'entreprise C opérant la place de marché et les vendeurs D, voire avec le prestataire E, selon son degré d'implication.

Comment rédiger la clause de données à caractère personnel dans le contrat entre la place de marché C et ses partenaires D et E ?

Un exemple de clauses pouvant être incluses dans un contrat conclu entre des responsables conjoints est proposé en exemple 3.

EXEMPLE 1 : "Je suis responsable de traitement"

(© Osborne Clarke)

Ces clauses sont proposées à titre purement indicatif et ne sont qu'une illustration de ce qu'il serait possible de rédiger. Elles devront être adaptées à chaque situation en fonction de la réalité des données collectées et des traitements. Elles devront en outre être articulées avec les autres clauses du contrat principal, notamment objet, obligations, responsabilité, etc.

1. Statut du prestataire

Les parties reconnaissent que le prestataire, afin d'exécuter ses obligations aux termes du présent contrat, aura accès et traitera des données à caractère personnel du client figurant aux présentes en qualité de sous-traitant au sens de la réglementation.

2. Description du traitement

[Commentaire : cette description pourra être complétée au jour de la signature ou en cours d'exécution du contrat ou si les parties ne connaissent pas à l'avance les traitements de données à caractère personnel qui seront effectués durant la durée du contrat.]

2.1. Description des activités de traitement

[Commentaire : décrire l'objet, la durée, la nature et la finalité des traitements effectués.]

2.2. Types de données à caractère personnel du client traitées

[Commentaire : lister les types de données à caractère personnel traitées. Exemple : noms, prénoms, adresse, téléphone des salariés du client ; noms, prénoms, adresse e-mail, adresse IP, produits achetés par les clients du client.]

2.3. Catégories de personnes concernées

[Commentaire : lister les catégories de personnes concernées, par exemple salariés du client ; clients et prospects ; fournisseurs du client ; etc.]

3. Obligations générales du prestataire

Le prestataire s'engage à :

(i) respecter la réglementation dans le cadre du présent contrat, et notamment à ne traiter les données à caractère personnel du client que sur instruction documentée du client afin de fournir les services et remplir ses obligations au titre du contrat ;

(ii) s'abstenir d'agir d'une manière qui constituerait ou entrainerait une violation de la réglementation par le client et alerte le client sans délai en cas de détection par le prestataire d'une conformité ou d'un risque de non-conformité ;

(iii) garantir et indemniser le client en cas d'action, réclamation, demande de toute tierce partie résultant de son manquement ou de sa défaillance à l'égard de la réglementation dans le cadre du présent contrat ;

(iv) tenir un registre de toutes les catégories d'activités de traitement effectuées pour le compte du client. Ce registre contient au moins les informations obligatoires requises par le GDPR. Le prestataire met ce registre à la disposition de toute autorité de contrôle qui en fait la demande ;

(v) mettre en œuvre les ressources humaines, techniques et organisationnelles suffisantes pour opérer les traitements en conformité avec la réglementation, telles que et sans que cette liste

soit limitative : former son personnel, nommer un DPO, le cas échéant, appliquer les principes de privacy by design et by default, etc.

4. Responsabilité

Le prestataire indemnise pleinement le client en cas de condamnation de celui-ci. Le client indemnise pleinement le prestataire en cas de condamnation de ce dernier pour manquement à la réglementation résultant d'un défaut d'alerte, mise en garde et conseil sur la conformité de son usage des services à la réglementation.

4. Coopération et assistance

Le prestataire assiste le client et coopère activement avec ce dernier pour lui permettre d'assurer la conformité du traitement à la réglementation, en particulier pour ce qui est des demandes d'exercice des droits des personnes concernées. [Commentaire : Décrire dans cette clause, de manière non limitative afin de sécuriser le responsable de traitement, les obligations en matière de coopération et d'assistance, notamment en ce qui concerne :

- les notifications de violations,

- les analyses d'impact,

- les formalités applicables,

- les demandes d'exercice des droits des personnes concernées : conditions de gestion des demandes, rôle respectif des parties,

- les documents et informations nécessaires à la satisfaction par le responsable de ses obligations d'accountability].

5. Sécurité et confidentialité

Le prestataire met en œuvre les mesures de sécurité et de confidentialité nécessaires à la conformité du traitement à la réglementation, dans les conditions précisées ci-après. [Commentaire : Décrire dans cette clause les obligations du sous-traitant en matière de sécurité :

- Mesures organisationnelles et techniques de sécurité et de confidentialité : mesures techniques, pseudonymisation, chiffrement, application par le personnel, etc. ;

- Plus spécifiquement, décrire le processus de gestion des violations de données : mesures de prévention, plan de recouvrement, procédure de notification de violation de données, délai, etc.]

6. Sous-traitance ultérieure

La désignation par le prestataire de tout sous-traitant ultérieur est soumise à l'obtention préalable de l'autorisation expresse et écrite du client. En cas d'autorisation du client, le prestataire conclut un contrat écrit avec le dit sous-traitant ultérieur contenant les mêmes obligations que celles fixées aux présentes, notamment :

- imposer au sous-traitant ultérieur de ne traiter les données à caractère personnel que conformément aux instructions écrites du prestataire ou du client ;

- prévoir la faculté pour le client d'auditer ce sous-traitant ultérieur dans les conditions prévues au 7 ci-après afin de s'assurer de son respect des obligations prévues aux présentes.

Le prestataire communique au client, dans les meilleurs délais, une copie du contrat conclu avec le sous-traitant ultérieur.

Nonobstant la désignation d'un sous-traitant ultérieur, le prestataire demeure pleinement responsable à l'égard du client pour tout traitement effectué par le sous-traitant ultérieur en violation des obligations des présentes.

Le prestataire s'assure que le sous-traitant ultérieur ne peut pas lui-même confier ses prestations à un sous-traitant sans l'autorisation écrite préalable et expresse du prestataire et/ou du client.

7. Audits

Le prestataire s'engage à se conformer aux demandes du client ou des auditeurs qu'il aurait mandaté de :

- accéder à ou d'inspecter (i) les locaux, (ii) les systèmes d'information, (iii) les registres ainsi que (iv) tout documents et informations, et
- interroger le personnel du prestataire,

et ce afin de permettre au client d'auditer et de vérifier que le prestataire et ses sous-traitants ultérieurs respectent pleinement les dispositions des présentes.

Les frais de l'audit sont à la charge du client. Par exception à ce qui précède, si l'audit révèle des manquements du prestataire, le prestataire rembourse le client les frais de l'audit, sans préjudice de toute indemnisation qui pourrait être réclamée par le client.

Le prestataire s'assure que le contrat conclu avec tout sous-traitant ultérieur permet au client de procéder ou faire procéder aux audits prévus au présent article, chez ce sous-traitant ultérieur et ses propres sous-traitants.

8. Localisation et transferts des données

[Commentaire : décrire dans cette clause les transferts de données et les garanties apportées pour les protéger, par exemple : clauses contractuelles types, Privacy Shield, règles d'entreprise contraignantes.]

9. Renvoi ou destruction de données à caractère personnel

[Commentaire : décrire dans cette clause les conditions de renvoi ou de destruction des données à caractère personnel au terme ou à la résiliation du contrat, ou à l'arrêt d'un traitement.]

EXEMPLE 2 : "Je suis sous-traitant"

(© Osborne Clarke)

Ces clauses sont proposées à titre purement indicatif et ne sont qu'une illustration de ce qu'il serait possible de rédiger. Elles devront être adaptées à chaque situation en fonction de la réalité des données collectées et des traitements. Elles devront en outre être articulées avec les autres clauses du contrat principal, notamment objet, obligations, responsabilité, etc.

1. Statut du prestataire

Les parties reconnaissent que le prestataire, afin d'exécuter ses obligations aux termes du présent contrat, aura accès et traitera les données à caractère personnel fournies par le client en qualité de sous-traitant au sens de la réglementation. Le client s'engage à alerter sans délai le prestataire en cas d'évolution des services demandés par le client, entraînant ou risquant d'entraîner un changement de statut du prestataire au regard de la réglementation.

2. Description du traitement

[Commentaire : cette description pourra être complétée au jour de la signature ou en cours d'exécution du contrat si les Parties ne connaissent pas à l'avance les traitements de données qui seront effectués durant la durée du contrat.]

Si le client utilise les services pour traiter d'autres données ou catégories de données à caractère personnel ou pour d'autres traitements ou finalités que listées ci-avant, le client le fait à ses risques et périls et le prestataire ne peut être tenu pour responsable en cas de manquement à la réglementation.

2.1. Description des activités de traitement

[Commentaire : décrire l'objet, la durée, la nature et la finalité des traitements effectués.]

2.2. Types de Données à Caractère Personnel du Client traitées

[Commentaire : lister les types de données à caractère personnel traitées. Exemple : noms, prénoms, adresse, téléphone des salariés du Client ; noms, prénoms, adresse email, adresse IP, produits achetés par les clients du Client.]

2.3. Catégories de personnes concernées

[Commentaire : lister les catégories de personnes concernées, par exemple salariés du client ; clients et prospects ; fournisseurs du client; etc.]

3. Obligations des Parties

Chacune des parties s'engage à respecter la réglementation dans le cadre du présent contrat.

Le client reconnaît que les ressources mises en œuvre dans le cadre du présent contrat par le prestataire constituent des garanties suffisantes de la conformité du prestataire et de ses services à la réglementation.

Le prestataire s'engage à traiter les données à caractère personnel listées aux présentes pour les seules finalités et dans les conditions convenues dans ce contrat afin de fournir les services et remplir ses obligations au titre du présent contrat. Le client reconnaît notamment que le prestataire se limite à suivre les instructions documentées du client en matière de traitements, sous réserve d'alerter le client en cas d'instructions données non conformes à la réglementation. Toute demande du client excédant ou modifiant les instructions de

traitement font l'objet d'un devis séparé. Toute instruction non documentée par écrit ou non conforme à la réglementation n'est pas prise en compte.

Chacune des parties tient un registre de toutes les opérations de traitement effectuées par elle. Ce registre contient au moins les informations obligatoires requises par la réglementation. Les parties mettent ce registre à la disposition de toute autorité de contrôle qui en fait la demande.

4. Responsabilité

Le Client indemnise pleinement le prestataire en cas de condamnation de ce dernier pour manquement à la réglementation résultant d'une utilisation des services non conforme au présent contrat. Le client indemnise pleinement le prestataire en cas de condamnation de ce dernier pour manquement à la réglementation, résultant de la poursuite de la fourniture des services conformément aux instructions du client, pour lesquelles le prestataire aura informé le client du caractère potentiellement non-conforme à la réglementation.

En cas de mise en cause de sa responsabilité, la responsabilité du prestataire est limitée à [préciser des limites de responsabilité, le cas échéant.]

5. Coopération et assistance

Le client reconnaît que les diligences suivantes satisfont à l'obligation de coopération et d'assistance du prestataire à l'égard du client pour lui permettre d'assurer la conformité du traitement à la réglementation :

[Commentaire : Décrire dans cette clause les diligences du prestataire s'agissant notamment :

- des notifications de violations,

- des analyses d'impact,

- des formalités applicables,

- des demandes d'exercice des droits des personnes concernées : conditions de gestion des demandes, rôle respectif des parties,

- des documents et informations nécessaires à la satisfaction par le responsable de ses obligations d'accountability].

En cas de nécessité de mettre en œuvre des diligences additionnelles, les parties conviennent de se réunir et discuter de bonne foi des conditions de ces diligences additionnelles, qui feront l'objet d'un avenant aux présentes.

6. Sécurité et confidentialité

Le client reconnaît que les diligences suivantes satisfont à l'obligation de sécurité et de confidentialité nécessaires à la conformité du traitement à la réglementation :

[Commentaire : Décrire dans cette clause les obligations du sous-traitant en matière de sécurité :

- Mesures organisationnelles et techniques de sécurité et de confidentialité : mesures techniques, pseudonymisation, chiffrement, application par le personnel, etc.;

- Plus spécifiquement, décrire le processus de gestion des violations de données : mesures de prévention, plan de recouvrement, procédure de notification de violation de données, délai, etc.]

En cas de nécessité de mettre en œuvre des diligences additionnelles, les parties conviennent de se réunir et discuter de bonne foi des conditions de ces diligences additionnelles, qui feront l'objet d'un avenant aux présentes.

7. Sous-traitance ultérieure

Le client accepte que le prestataire puisse faire appel à des sous-traitants ultérieurs agissant en son nom et pour son compte afin de l'assister dans les opérations de traitement des données à caractère personnel du client. Le prestataire informe le client de tout changement prévu concernant l'ajout ou le remplacement d'un sous-traitant ultérieur.

Le prestataire conclut un contrat écrit avec tout sous-traitant ultérieur contenant les mêmes obligations que celles fixées aux présentes, notamment en imposant au sous-traitant ultérieur de ne traiter les données à caractère personnel du client que conformément aux instructions écrites du prestataire ou du client. Nonobstant la désignation d'un sous-traitant ultérieur, le prestataire demeure pleinement responsable à l'égard du client pour tout traitement effectué par le sous-traitant ultérieur en violation des obligations des présentes.

Le client peut s'opposer à un tel ajout ou remplacement en notifiant le prestataire par écrit dans les dix (10) jours suivant la réception de l'avis d'ajout ou de remplacement envoyé par le prestataire. Dans le cas où le Client s'oppose à la désignation d'un sous-traitant ultérieur, le prestataire peut résilier le contrat.

8. Audits

A la demande du client, le prestataire met à disposition du client les rapports d'audit effectués par des organismes d'audit indépendants tiers et toutes informations pertinentes fournies par ces organismes.

A défaut pour le prestataire de fournir au client une preuve de sa conformité aux dispositions des présentes via les rapports susmentionnées et/ou si le Client estime raisonnablement nécessaire d'effectuer un audit complémentaire conformément à la réglementation, pour pleinement vérifier la conformité des services fournis à la réglementation et au contrat, le prestataire accepte de se soumettre à un audit effectué par un auditeur indépendant réputé, ne concurrençant pas les activités commerciales du prestataire, dans la limite d'un audit par an. Cet auditeur indépendant est choisi par le client et accepté par le prestataire. Il possède les qualifications professionnelles requises et est soumis à un accord de confidentialité. Les parties reconnaissent que tous rapports et information obtenues dans le cadre de cet audit sont des informations confidentielles.

La date de début de l'audit, la durée et le périmètre de l'audit sont définis d'un commun accord par les parties avec un préavis minimum de 15 jours ouvrés. L'audit ne peut être effectué que durant les heures d'ouverture du prestataire et d'une façon qui ne perturbe pas l'activité du prestataire. L'audit ne comporte pas d'accès à tous systèmes, information, données non liées aux traitements effectués en vertu de ce contrat ni d'accès physique aux serveurs sur lesquels est sauvegardée la solution.

Le client prend à sa charge tous les frais occasionnés par l'audit, incluant de manière non limitative les honoraires de l'auditeur et rembourse au prestataire toutes les dépenses et frais occasionnés par cet audit, y compris le temps consacré à l'audit en fonction du taux horaire moyen du personnel du prestataire ayant collaboré à l'audit.

9. Localisation et transferts des données

[Commentaire : décrire dans cette clause les transferts de données et les garanties apportées pour les protéger, par exemple : clauses contractuelles types, Privacy Shield, règles d'entreprise contraignantes.]

10. Renvoi ou destruction de données à caractère personnel

[Commentaire : décrire dans cette clause les conditions de renvoi ou de destruction des données à caractère personnel au terme ou à la résiliation du contrat, ou à l'arrêt d'un traitement.]

EXEMPLE 3 : "Nous sommes responsables conjoints"

(© Osborne Clarke)

Ces clauses sont proposées à titre purement indicatif et ne sont qu'une illustration de ce qu'il serait possible de rédiger. Elles devront être adaptées à chaque situation en fonction de la réalité des données collectées et des traitements. Elles devront en outre être articulées avec les autres clauses du contrat principal, notamment objet, obligations, responsabilité, etc.

1. Statut des parties

Les parties reconnaissent traiter les données à caractère personnel en qualité de Responsables Conjoints au sens de la réglementation, dans les conditions définies aux présentes. Chacune des parties s'engage à respecter la réglementation dans le cadre du contrat.

2. Description du traitement

Les parties s'engagent à traiter uniquement les Données à Caractère Personnel listées et pour les finalités décrites ci-après.

2.1. Description des activités de traitement de chaque Responsable Conjoint

[Commentaire : décrire l'objet, la durée, la nature et la finalité des traitements effectués par chaque Responsable Conjoint.]

2.2. Types de Données à Caractère personnel traitées par chaque Responsable Conjoint

[Commentaire : lister les types de données à caractère personnel traitées par chaque Responsable Conjoint. Exemple : noms, prénoms, adresse, téléphone des salariés ; noms, prénoms, adresse email, adresse IP, produits achetés par les clients.]

2.3. Catégories de personnes Concernées

[Commentaire : lister les catégories de personnes concernées, par exemple salariés ; clients et prospects; fournisseurs; etc.]

3. Obligations des parties

[Commentaire : Décrire ici les obligations respectives des parties sur les opérations effectuées dans le cadre du traitement, en particulier:

- qui intervient dans quelles opérations : collecte, analyse, croisement, sécurisation, hébergement, effacement, etc.;

- dans quelles conditions: prise en main de la conformité de tel type d'opérations à la réglementation, obtention d'une autorisation préalable de l'autre partie ou simple information, mécanismes de reporting, doucmentation, alerte;

- quel partage des rôles dans les obligations de conformité et d'accountability : qui tient le ou les registres des traitements, qui met en œuvre l'accountability/les études d'impact/les formalités/etc., l'autre partie lui apportant aide et assistance, comment les parties s'alertent sur les risques de non-conformité, qui nomme un DPO, etc. ;

- quelles relations avec les autorités de contrôle ; etc.]

4. Information et exercice des droits des personnes concernées

4.1. Information des personnes concernées

Le Responsable Conjoint qui collecte les données à caractère personnel auprès des personnes concernées a l'obligation d'informer celles-ci des traitements effectués par les Responsables Conjoints dans le respect des dispositions de l'Article 13 du GDPR.

4.2. Gestion de l'exercice des droits des personnes concernées et point de contact

[Commentaire : Décrire dans cette clause les obligations en matière de coopération et d'assistance en ce qui concerne les demandes des personnes concernées].

Le Responsable Conjoint qui collecte les données à caractère personnel est la personne désignée comme point de contact auprès de celles-ci pour l'exercice de leurs droits, notamment dans toute politique de confidentialité et sera le gestionnaire des demandes des personnes concernées.

A réception par le gestionnaire précité d'une demande concernant des données traitées par l'autre Responsable Conjoint, le gestionnaire informe l'autre Responsable Conjoint dans un délai de 3 jours. Ce dernier apportera dans les meilleurs délais toute son assistance pour permettre au gestionnaire de répondre à la demande.

Le gestionnaire des demandes répond à la personne concernée dans un délai maximum de [x] jours, sous réserve de la bonne exécution de ses obligations par l'autre Responsable Conjoint.

4.3. Mise à disposition des grandes lignes de la présente annexe aux personnes concernées

[Commentaire : Décrire dans cette clause les modalités de mise à disposition des grandes lignes de la présente annexe aux personnes concernées : article ou annexe dans des conditions générales de service, privacy policy, choix du wording validé en annexe aux présentes, etc.]

5. Sécurité et confidentialité

Les parties mettent en œuvre les mesures de sécurité et de confidentialité nécessaires à la conformité du traitement à la réglementation, dans les conditions précisées ci-après. [Commentaire : Décrire dans cette clause les obligations en matière de sécurité :

- Mesures organisationnelles et techniques de sécurité et de confidentialité : mesures techniques, pseudonymisation, chiffrement, application par le personnel, etc. ;

- Plus spécifiquement, décrire le processus de gestion des violations de données : mesures de prévention, plan de recouvrement, procédure de notification de violation de données, délai, etc.]

Chaque Responsable Conjoint assure la sécurité des traitements effectués par lui. En cas de manquement du Responsable Conjoint à son obligation de sécurité entrainant une violation de données personnelles, celui-ci est seul tenu responsable des conséquences de cette violation auprès des personnes concernées, des autorités de contrôle et de tout tiers et en garantit intégralement l'autre partie.

Le Responsable Conjoint ayant identifié une violation de données notifie l'autre partie dans un délai de 3 jours calendaires. Les correspondants de chaque Responsable Conjoint se rencontrent dans les meilleurs délais afin de déterminer d'un commun accord s'il convient de notifier cette violation à l'autorité de contrôle compétente et le cas échéant aux personnes concernées.

6. Localisation des donnés et transferts hors UE

[Commentaire : Décrire dans cette clause le lieu où seront traitées les données et les éventuels transferts en dehors de l'UE, ainsi que les mesures de conformité prises à cet égard et, le cas échéant, préciser les rôles respectifs de chaque partie.]

7. Recours à des sous-traitants

[Commentaire : Décrire dans cette clause les possibilités pour chacune des parties d'avoir recours à des sous-traitants ou non et les obligations et responsabilités des parties en découlant]

8. Correspondants

Les parties désignent chacune un correspondant qui les représente et prend toutes les décisions nécessaires à la bonne exécution des présentes à l'égard des personnes concernées. Les correspondants de chaque partie doivent être investis d'une autorité suffisante pour prendre des décisions au jour le jour.

L'identité et les coordonnées des correspondants figurent en annexe.

9. Sort des données en fin de contrat

[Commentaire : décrire dans cette clause le sort des données à caractère personnel au terme ou à la résiliation du contrat.]

CONCLUSION

L'annonce de l'entrée en vigueur du GDPR, qui était en discussion au sein des instances européennes depuis de longs mois, a suscité **inquiétudes, questionnements et volonté d'action** au sein des entreprises et notamment au sein des directions juridiques, des responsables de la sécurité des SI, des responsables de la conformité, et des directions de l'audit interne.

Depuis, ces acteurs se sont employés à **sensibiliser leurs directions générales** afin de fédérer l'ensemble de l'entreprise autour des problématiques liées à la protection des données à caractère personnel. En effet, avec le GDPR, la protection des données à caractère personnel doit désormais être **un sujet traité par l'ensemble des parties prenantes de l'entreprise** et non plus seulement par le Correspondant Informatique et Libertés (CIL) ou par la direction juridique.

La mise en conformité au GDPR implique des changements de taille au sein des entreprises.

Même si la plupart des concepts du GDPR ne sont pas nouveaux et se trouvaient déjà dans la réglementation existante, les entreprises s'étaient principalement concentrées sur les aspects « déclaratifs » de la loi Informatique et Libertés (déclarations CNIL, autorisations CNIL, etc.) ainsi que sur la prise en compte des droits des personnes concernées ; elles n'avaient en revanche généralement pas mis en place de dispositifs élaborés de management des données permettant ainsi une exploitation et une valorisation optimisées de leur patrimoine informationnel.

Avec le GDPR, les entreprises doivent élaborer un dispositif complet de protection des données, dont les principales caractéristiques sont :

- **Une gouvernance forte** avec un rattachement du Data Protection Officer (DPO) au plus haut niveau de l'entreprise ;
- **La tenue d'un registre des activités de traitement des données à caractère personnel** ;
- **La formalisation de politiques** explicitant les détails de la mise en œuvre de ce dispositif de protection des données ;
- **La prise en compte des problématiques relatives à la protection des données au sein des différents processus opérationnels de l'entreprise** (développement de nouveaux produits ou nouveaux traitements, exploitation des systèmes d'information ou solutions numériques, dispositifs de cybersécurité, gestion des incidents de violation de données à caractère personnel, gestion des sous-traitants et des tiers, …)
- **La mise en place d'un programme d'audit régulier** visant à s'assurer de l'efficacité de ce dispositif.

L'initiative DPSI lancée par l'AFAI, le CIGREF et TECH IN France vise à permettre aux entreprises d'accélérer leurs projets de mise en conformité avec le GDPR au travers de :

- **La compréhension des dispositifs et mesures** à mettre en place pour les DSI, les responsables métiers mais aussi les « *Data Protection Officers* » dont un certain nombre n'aura pas toujours une grande expérience du sujet ;

- **La mise à disposition d'une check-list pratique** à destination des acteurs de l'entreprise susceptibles de traiter ou d'être impliqués dans le traitement de données à caractère personnel ;

- **La fourniture d'un catalogue de mesures pratiques** permettant de répondre aux risques sur la sécurité des SI, sur la sécurité des données, sur les droits des personnes concernées.

Une fois que le cadre de gestion de la protection des données à caractère personnel aura été mis en place, il sera nécessaire d'outiller la démarche pour pouvoir assurer la pérennité des mesures prises et leur mise à jour de manière efficace.

ANNEXES

- SG1 - Check-list du Règlement Général sur la Protection des Données
- SG2 – Mesures techniques à mettre en place pour être conforme au GDPR

SG1 - Check-list du Règlement Général sur la Protection des Données (GDPR)

Gouvernance : Direction générale, Direction des risques ou conformité ou Secrétariat général (service juridique)
Métiers : Direction Marketing, Direction des ressources humaines (DRH),
Informatique : Directeur des systèmes d'information (DSI) et cybersécurité

Thème	Sous thème	#	Question	Commentaires / Exemples
Gouvernance	DPO (délégué à la protection des données personnelles)	1	Avez-vous nommé un délégué à la protection des données personnelles (DPO) ? Si non, avez-vous vérifié et documenté que vous n'êtes pas soumis à cette exigence ?	D'après l'article 37 §1, la nomination d'un DPO est notamment obligatoire dans le cas où vos activités de base consistent des opérations de traitement à grande échelle impliquant un suivi systématique des personnes concernées, ou des données sensibles au sens des articles 9 et 10.
		2	Le rattachement hiérarchique du délégué à la protection des données personnelles (DPO) garantit-il son indépendance ?	
	Périmètre d'application	3	Avez-vous déterminé le périmètre des entités / Business Unit concernées par le plan de mise en conformité ?	
		4	Avez-vous établi un registre des traitements dont vous êtes responsable, co-responsable ou sous-traitant ?	Le registre comporte le nom et les coordonnées du responsable du traitement, les finalités du traitement, les catégories de destinataires et des personnes concernées, etc.
		5	Avez-vous identifié les transferts de données personnelles hors Union Européenne ? Si oui, avez-vous formalisé les garanties mises en œuvre ou à l'étude ?	Garanties cf. chapitre V du GDPR : soit niveau de protection adéquate du pays tiers (art. 44) soit mécanisme de sauvegarde visé à l'art 46 (p ex Binding Corporate Rules)
		6	Avez-vous réalisé un état des lieux des processus métiers traitant des données personnelles ?	
		7	Avez-vous identifié les sous-traitants traitant vos données personnelles ? Si oui, vous assurez vous que les sous-traitants existants et futurs sont conformes aux exigences du	

			GDPR contractuellement et par le biais de contrôles ?	
	Mise en conformité	8	Avez-vous mis en place une organisation projet pour la mise en conformité au GDPR ?	Une organisation projet couvre généralement le(s) sponsor(s), l'équipe projet, les tâches, jalons et livrables
		9	Avez-vous établi une feuille de route pour la mise en conformité au GDPR ?	Une feuille de route propose généralement les projets, le recensement des moyens, la cible à atteindre, la priorité des tâches, ainsi qu'un calendrier pour atteindre ces buts.
		10	Existe-t-il un reporting périodique au Board/Comex pour s'assurer de l'avancement du plan d'actions et décider d'actions correctrices ?	
		11	Le plan d'audit intègre-t-il des missions de contrôle de la mise en conformité au GDPR ?	
	Politiques et procédures	12	Avez-vous intégré les éléments de conformité au GDPR dans vos politiques et procédures ?	Les politiques précisent les durées de conservation des données personnelles, la sécurité des données, la suppression des données, la notification en cas de violation des données personnelles, la validation périodique de la pertinence du dispositif en place, etc.
	Veille juridique	13	Une veille juridique a-t-elle été mise en place pour suivre les évolutions réglementaires ?	Exemple = guidelines émises par le G29 (WP29)
	Formation	14	Les politiques et procédures en lien avec le GDPR sont-elles diffusées aux collaborateurs de votre entreprise ?	Exemple = code de conduite
		15	Avez-vous intégré le GDPR à votre programme de formation RH ?	Le programme de formation inclut des dispositifs comme du E-learning, des formations régulières (Manager, SI, métiers), des actions de communication, etc
	Assurance	16	Avez-vous revu la couverture d'assurance de votre entreprise pour tenir en compte du GDPR ?	
Métiers	**Licéité des traitements**	17	Avez-vous identifié pour vos traitements : les finalités, les personnes concernées, les catégories de données traitées ?	Ces éléments sont un préalable nécessaire à l'établissement du registre de traitements exigé par le GDPR pour chaque responsable de traitement et sous-traitant.
		18	Avez-vous vérifié la proportionnalité des données collectées aux finalités des traitements ?	Limiter par défaut le traitement de données à caractère personnel à ce qui est strictement nécessaire, en ce qui concerne la quantité de données traitées, leur accessibilité et leur période de conservation

		19	Pouvez-vous justifier la base légale de chacun de vos traitements ?	Le traitement doit être fondé sur une base légale prévue à l'article 6 du règlement (licéité), qui peut être : une obligation légale, l'intérêt légitime du responsable de traitement, l'exécution d'un contrat, le consentement exprimé par la personne concernée, la protection des intérêts vitaux d'une personne concernée, une mission d'intérêt ou de service public
		20	Lorsque la base légale du traitement est le consentement, avez-vous mis en place des mécanismes de gestion de ces consentements ?	Gestion = recueil, modification, enregistrement, révocation, etc
		21	Pour les traitements impliquant le croisement entre plusieurs catégories de données (interconnexion de fichiers), la réutilisation de données collectées lors d'un autre traitement ou l'enrichissement des données, avez-vous consulté le DPO et vérifié la conformité au GDPR ?	Si vous - effectuez des croisements entre plusieurs catégories de données collectées séparément, ou - réutilisez des données collectées pour un autre traitement, ou - utilisez des données fournies par une tierce partie, vous devez vérifier que votre traitement est conforme aux finalités pour lesquelles les données ont été collectées ou, le cas échéant, aux consentements donnés par les personnes concernées
		22	Des durées de conservation sont-elles définies pour les données traitées ? Si oui, les durées sont-elles communiquées aux personnes concernées ?	
	Types de traitements	23	Pour les traitements entrant dans le cadre du profilage, avez-vous consulté le DPO et vérifié la conformité au GDPR ?	Profilage = toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique
		24	Pour les traitements soumis à des hauts risques potentiels sur la vie privée, avez-vous consulté le DPO et vérifié le respect des conditions spécifiques ?	Exemples de traitement : vidéosurveillance, géolocalisation, whistleblowing, écoute sur le lieu de travail, contrôle d'accès aux locaux, biométrie, etc...
	Catégories des données collectées	25	Si vous collectez des catégories particulières de données (données sensibles), avez-vous vérifié la licéité de leur collecte et de leur traitement ?	Cf. articles 9 et 10 du GDPR
	Droits des personnes	26	Les personnes concernées bénéficient-elles d'une information claire et compréhensible lors de la collecte des données ?	
		27	Avez-vous une procédure validée et testée pour répondre aux demandes d'exercice des droits prévus par le GDPR ? En particulier droits d'accès, de rectification, de suppression des	Y compris la notification des demandes de rectification ou de suppression aux sous-traitants ou autres tierces parties destinataires des données

			données de droit à l'oubli, de droit à la portabilité ou de limitation de traitement ?	
		28	Les personnes concernées peuvent-elles modifier leurs consentements ?	Exemple : Self service
	Contractualisation avec les sous-traitants	29	Avez-vous défini contractuellement avec vos sous-traitants des exigences en termes de protection des données ?	
	Transferts de données en dehors de l'Espace Economique Européen	30	Si vous effectuez des transferts de données personnelles à des entreprises situées hors de l'Union Européenne, vous êtes-vous rapprochés de votre DPO ou de votre service juridique pour vérifier que les transferts effectués soient couverts par des garanties appropriées ?	
	Sécurité des données personnelles	31	Avez-vous exprimé des exigences de protection des données personnelles vis à vis de votre service informatique ?	Exemple d'exigences de sécurité : pseudonymisation, chiffrement, stockage et transferts sécurisés, règles de purge ou d'archivage, etc...
		32	Etes-vous associé au processus de détection, de traitement et de notification des violations de données personnelles ?	
	Etude d'impact sur la vie privée (DPIA)	33	Avez-vous défini des critères de décision pour déterminer si une Etude d'impact sur la vie privée (DPIA) était nécessaire ?	
		34	Si la criticité du traitement implique une étude d'impact sur la vie privée (DPIA), avez-vous effectué cette étude en coordination avec DPO ?	
Systèmes d'Information et cybersécurité	**Cartographie des systèmes d'informations (SI)**	35	Avez-vous une cartographie exhaustive des données personnelles traitées dans votre système d'information ?	Dictionnaire de données, accès (utilisateurs, interfaces), applications, bases de données, serveurs, Datacenter, services cloud, localisation, ...
	Sécurité des donné	36	Avez-vous intégré les éléments de conformité au GDPR dans votre politique de sécurité des systèmes d'information ?	

		37	Utilisez-vous des standards ou des guides de bonnes pratiques Security by design ?	Exemples de référentiels de sécurité = ISO27001, NIST, guide d'hygiène ANSSI, CIS critical security controls, …
		38	Avez-vous défini et mis en place des procédures de gestion des accès aux systèmes contenant de données personnelles ?	Conception des habilitations, ajout/suppression des droits, revues régulières des droits d'accès)
		39	Avez-vous défini et mis en place des mesures de sécurisation des accès administrateurs privilégiés ?	Bastion, enregistrement de sessions des comptes à privilèges sur les serveurs, …)
		40	Avez-vous mis en place des mécanismes de protection des données personnelles (notamment chiffrement ou de pseudonymisation) ?	Données stockées sur les serveurs (Data at Rest) et pour le transport de ces données sur le réseau (Data in transit), (exemples : outils de tokenisation, …)
	Protection de la vie privée dès la conception (« privacy by design »)	41	Avez-vous mis en place des mécanismes d'archivage et de suppression des données personnelles ?	
		42	Ces mécanismes sont-ils alignés sur la politique de conservation (notamment avec les durées légales ou contractuelles de rétention des données) ?	
		43	Avez-vous mis en place des mécanismes permettant d'isoler les environnements de production et de non production ?	Segmentation réseau, pare feux, anonymisation éventuelle des données personnelles en environnements de non production
	Transparence, information	44	Avez-vous mis en place des mécanismes de traçabilité et de détection d'accès aux données personnelles ? (Notamment déplacement ou copies de données non autorisées déclenchant des alertes aux équipes sécurité)	Accès des utilisateurs/interfaces, déplacements et copies en masse des données à personnelles, etc.
	Dispositif de détection et de notification	45	Avez-vous établi la procédure de détection, de traitement et de notification des violations de données personnelles ?	Procédure détaillant la détection, la réponse à incident et la communication en cellule de crise, puis l'autorité dans les 72 heures
	Contractualisation avec les sous-traitants	46	Avez-vous défini contractuellement des exigences en termes de protection des données avec vos sous-traitants informatiques (prestataires ou fournisseurs) ?	Exemples = questionnaire de sécurité, clauses contractuelles liées à la protection des données, clause d'audit de sécurité, suppression des données à la fin de la prestation, etc.

	Codes de conduite et Certification	47	Effectuez-vous régulièrement des contrôles / audit de sécurité de vos sous-traitants informatiques (prestataires ou fournisseurs) ?	Exemples : vérification de la mise en place des clauses de sécurité, audit technique de sécurité, tests d'intrusion, etc.
	Etude d'impact sur la vie privée (DPIA)	48	Avez-vous défini des critères de décision pour déterminer si une Etude d'impact sur la vie privée (DPIA) était nécessaire ?	
		49	Avez-vous défini une méthode d'étude d'impact vie privée (DPIA / EIVP) en coordination avec le DPO ?	Exemples : Etude d'impacts sur la vie privée : la méthode de la CNIL -
	Gestion de l'exercice des droit s des personnes	50	Avez-vous défini et mis en œuvre une ou des solutions pour répondre aux demandes d'accès, de rectification, de suppression des données, de droit à l'oubli, de droit à la portabilité, de limitation des traitements dans vos applications ?	Sauf exception, le GDPR impose un délai maximum d'un mois pour répondre aux demandes d'exercice de leurs droits par les personnes concernées (Art. 12.3).

SG2 Mesures techniques à mettre en place pour être conforme au GDPR

ONGLET 1 : Types de Risques par Composants SI

Types de Risques	Réseau	Datacenter	Cloud	Workplace	Données source	Video-IoT	Application	Database	DWH	Big Data	GED-Archivage	Fichiers Partagés	Messagerie	Données sortie	Réseaux Sociaux
Sécurité du SI															
Intrusion physique dans le datacenter ou dans les locaux	1	1	1												
Perte ou vol d'un équipement		1	1	1				1							
Destruction d'un équipement physique, d'un composant software ou de		1	1					1							
Intrusion extérieure dans le réseau	1														
Inaccessibilité d'un service	1	1	1				1								
Infiltration via malware	1	1	1	1		1	1	1	1	1	1	1	1	1	1
Gestion défaillante des droits d'accès	1	1	1	1	1		1	1	1	1	1	1	1	1	1
Usurpation d'identité d'un compte utilisateur					1		1	1	1	1	1	1			
Usurpation d'un compte administrateur				1			1	1	1	1	1		1	1	1
Exfiltration de données		1		1											
Interception d'échanges	1		1	1		1	1	1	1	1	1		1	1	1
Défaut d'application des mises à jour de sécurité	1	1	1	1		1	1						1		1
Non détection de vulnérabilités	1	1	1	1		1	1	1	1	1	1	1			1
Incapacité à tracer un incident ou des accès	1	1	1	1	1		1	1	1	1	1	1	1	1	
Incapacité à détecter une atteinte aux données			1												
Défaut de pilotage d'un sous-traitant / fournisseur (IoT)	1	1	1	1			1	1	1	1			1		1
Négligence d'un sous-traitant / fournisseur (IoT)	1	1	1	1			1	1	1	1			1		1
Intervention frauduleuse d'un sous-traitant	1	1	1	1			1	1	1	1	1		1		1
Protection des données															
Défaut de cartographie (actualisée) des données et des traitements (défaut															
Localisation non autorisée de données personnelles							1								
Non respect des réglementations locales (ex. égalité des chances aux US, ...)		1	1		1		1	1	1	1	1	1	1	1	
Absence de cloisonnement des données personnelles					1		1	1	1	1	1	1	1	1	
Non respect des règles de rétention des données (durée de conservation)		1			1		1	1	1	1	1	1	1	1	
Non respect des formalités préalables applicables au traitement		1			1		1	1	1	1	1	1	1	1	
Transfert non sécurisé de données personnelles			1		1		1	1	1	1	1	1	1	1	
Transferts non encadrés de données hors UE			1		1		1	1	1	1	1	1	1	1	
Accès non conforme ou non encadré aux données personnelles			1		1		1	1	1	1	1	1	1	1	
Propagation malveillante de données personnelles			1		1		1	1	1	1	1	1	1	1	
Divulgation de données personnelles par inadvertance			1		1		1	1	1	1	1	1	1	1	
Vol de données			1		1		1	1	1	1	1	1	1	1	
Perte d'intégrité des données	1	1	1					1					1		
Détention ou utilisation abusive de données personnelles							1	1	1	1	1	1	1	1	
Détournement de finalité de traitements de données personnelles du fait							1	1	1	1	1	1	1	1	
Reconstitution de l'identité d'une personne et enrichissement de son profil							1	1	1	1	1	1	1	1	
Défaut de PIA							1	1	1	1					
Défaut de privacy by design (absence de règles sur la minimisation des			1		1		1	1	1	1	1	1	1	1	
Défaut de notification d'une atteinte aux données			1		1		1	1	1	1	1	1	1	1	
Droits de la personne															
Incapacité à répondre aux droits des personnes (exécution des droits)															
Information							1	1	1	1	1	1	1	1	
Transparence du traitement															
Preuve du consentement															
Retrait du consentement (opposition ou suppression)															
Respect de la limite du traitement															
Accès															
Rectification															
Effacement															
Portabilité															
Profilage															
Données des mineurs															

SG2 Mesures et recommandations potentiellement applicables pour être conforme au GDPR

ONGLET 2 : Mesures par types de risques

Types de Risques	Mesures techniques possibles	
Sécurité du SI	Sécurité du SI	#
Intrusion physique dans le datacenter ou dans les locaux	Système de contrôle des accès physiques : badge, contrôle identité (scanner biométriques, etc...), accès renforcé pour certains espaces sensibles (salles serveurs fermées, etc...), caméras video-surveillance, alarmes, etc...	1
	Exigences contractuelles (contrats hébergement, partenaires intervenant dans les locaux)	2
	Chiffrement wifi et accès contrôlé par mot de passe	3
	Blocage des ports sur les équipements	4
	Network Access Control	5
Perte ou vol d'un équipement	Authentification forte (2-factor, tentatives limitées,mots de passe bios et windows...)	6
	Chiffrement des postes et des mobiles (bitlocker, mobileiron, etc...)	7
	Usage limité/contrôlé du BYOD	8
	Blocage des ports usb	9
	Effacement à distance des disques des mobiles	10
	Interdiction de stockage sur disque dur	11
	Sauvegardes réseau	12
	Gestion centralisée des configurations	13
	Procédure de décommissionnement des équipements (serveurs, PC's, mobiles...)	14
	Chiffrement des disques du SAN pour les serveurs	15
Destruction d'un équipement physique, d'un composant software ou de données	Contrat de maintenance fournisseur (accès à un équipement similaire, restoration, réversibilité, etc...)	16
	Sauvegardes adaptées (cycle de vie...)	17
	Chiffrement de surface	18
	Sauvegarde des configurations et des procédures de Maintien en Conditions Opérationnelles (MCO)	19
Intrusion extérieure dans le réseau	Protection type filtrage internet (BlueCoat, etc...)	20
	Protection WAF, firewall, reverse proxy	21
	Limitation des flux	22
	Segmentation réseau VLAN	23
	Sécurisation des points d'accès (wifi WPA)	24
	Filtrage de port des VPN des partenaires externes	25
	url et contrôle d'accès nominatif	26
	IPS	27
	Blocage des ports	28
	Utilisation du chiffrement par défaut des communications	29
	Sauvegarde des logs réseaux	30
	Mise en place d'un SOC (Security Operation Center)	31
	Network Access Control	32
Inaccessibilité d'un service	Plan de Continuité d'Activité	33
	Dual data center (actif/actif)	34
	Haute disponibilité	35
Infiltration via malware	Politique de veille éditeurs (système + middleware)	36
	Patch management	37
	Anti-malware (et anti-virus)	38
	Filtrage url et ports	39
	Passerelles SMTP (ProofPoint)	40
	Blocage webmail	41
	Protection contre les menaces réseau avancées (ATP, Advanced Threat Protection)	42
	Sauvegardes et restorations	43
	Sensibilisation des utilisateurs	44
	Procédure d'alerte en cas d'urgence	45
	SOC de 3ème génération incluant une analyse d'écart comportemental	46
Gestion défaillante des droits d'accès	Outillage d'identification, de classification et de revue des accès	47
	Attribution automatique des accès (GDI/GDA), et workflow associés	48
	Security entitlement	49
	Audit régulier des droits d'accès	50
	Politique de changement de mots de passe	51
	Gestion centralisée des logs (SIEM, Security Information Event Management)	52
	Mise en place d'un SOC	53
	Mise en place de scénarios d'attaque métier dans les règles du moteur de corrélation (SIEM)	54
Usurpation d'identité d'un compte utilisateur	Politique de mots de passe (complexité, changement régulier...)	55
	Sensibilisation utilisateur	56
	Norme de flux https/sftp	57
	Norme sur les cookies et les identifications	58
	Gestion centralisée des logs (SIEM, Security Information Event Management) (par exemple, détection d'un même compte accédant à plusieurs postes)	59
	Authentification forte à 2 facteurs	60
Usurpation d'un compte administrateur	Comptes "administrateur" (privilèges forts) séparés des comptes "utilisateur" (usage bureautique)	61
	Contrôle d'accès renforcé	62
	Politique de mots de passe renforcée	63
	Outil de gestion des accès et renouvellement automatique sur des comptes génériques (type CyberArk)	64
	Notification automatique des accès IP suspects	65
	Gestion nominative des accès administrateurs	66
	Limitation des administrateurs de domaines au strict minimum, et séparation complète de leurs environnements de travail et de leur environnement d'administration de l'Active Directory	67
	Utilisation de connexion centralisée et tracée des comptes administrateurs (Bastion type Wallix, Centrify...)	68
	Revue des comptes administrateurs (et de leur droits)	69
	Politique sur les droits et devoirs en matière de sortie des données	70
	Chiffrement, anonymisation et pseudonymisation	71
	Anonymisation persistante	72

SG2 Mesures et recommandations potentiellement applicables pour être conforme au GDPR

ONGLET 2 : Mesures par types de risques

Types de Risques	Mesures techniques possibles	
Sécurité du SI	**Sécurité du SI**	**#**
Exfiltration de données	Encadrement contractuel avec le partenaire (NDA, clause de confidentialité, clause de suppression des données…)	73
	Gestion centralisée des logs (SIEM, Security Information Event Management), et synchronisation des équipements	74
	EDRM, Enterprise Digital Right Management (protection bureautique avec chiffrement, ou watermarking, qui consiste à cacher un copyright dans un fichier…)	75
	Limitation des accès internet	76
	Blocage des ports usb pour le transfert de données (clés usb, disques durs externes, téléphones portables, graveurs de CD/DVD/Blueray exernes, etc...)	77
	Blocage de sites de transferts (type wetransfer, dropbox…)	78
	Détection de téléchargements/transferts de fichiers importants	79
	Intégration de données pièges pour traçabilité de la source de l'exfiltration	80
	Mise en place d'une politique de DLP (Data Leakage Prevention) et des outils associés	81
Interception d'échanges	Protection via des flux sécurisés (TLS/SSL, https, sftp...)	82
	Traçabilité des flux (garantie arrivée), chiffrement datacentrique	83
	Installation clé WPA sur le réseau wifi	84
	Chiffrement au niveau applicatif (chiffrement de signature)	85
	Chiffrement datacentrique	86
	Politique de mots de passe	87
Défaut d'application des mises à jour de sécurité	Politique de gestion des patchs	88
	Outil de contrôle de mise à niveau applicatif, intégrant des scans de vulnérabilité périodiques	89
	Tests de pénétration avec rapport et plan de remédiation	90
	Projet de normalisation et gestion de l'obsolescence	91
	Patchs virtuels (ex. pour simuler les patchs au niveau réseau). IPS (Intrusion Prevention System)	92
	Déploiement d'un IDS (Intrusion Detection System)	93
	Automatisation du patching des équipements auprès du fournisseur	94
	Sensibilisation des équipes techniques	95
	Dispositifs de contrôle interne (contrôle ad hoc dans le cadre de contrôle interne de l'entité)	96
	Solution de conteneurisation des applicatifs	97
Non détection de vulnérabilités	Test intrusion et scans de vulnérabilité réguliers	98
	Politique de patching	99
	Host Intrusion Prevention System (HIPS) pour permettre le patching virtuel des vulnérabilités	100
	Analyse de qualité de code, et respect standard & normes sécurité (type Fortify)	101
	Production de normes & standards : master, code, configuration middleware, etc...	102
	Procédure d'alerte et d'application urgente de patch	103
	Inventaire ponctuel qui permet de détecter des non conformités et vulnérabilités potentielles	104
	Veille vulnérabilités	105
	Sensibilisation utilisateur	106
Incapacité à tracer un incident ou des accès	Remontée centralisée des logs et moteurs de corrélation (SIEM)	107
	SOC	108
	Service forensic (équipe dédiée pour réponse aux incidents et à la veille)	109
	Procédure de gestion de crise (pour être efficiente, doit être testée périodiquement, dans son ensemble)	110
Incapacité à détecter une atteinte aux données	SIEM : qualification des incidents, contrôle d'intégrité (signature cryptographique, hash, CRC), logs sur les accès aux données	111
	Audit de sécurité	112
	Tests d'intrusion	113
	Sensibilisation à la remontée d'incidents/doutes de compromission	114
	Veille sur internet pour recherche de traces de compromission ou de revente des données	115
Défaut de pilotage d'un sous-traitant / fournisseur (IoT)	Encadrement contractuel (clauses contractuelles types approuvées par la Commission et/ou la CNIL, BCR)	116
	NDA	117
	SLA	118
	Reporting	119
	Audit physique et logique	120
	Obtention d'un rapport d'audit d'un tiers de confiance, i.e. un auditeur indépendant attestant la bonne exécution des services (ISAE 3402, SSAE16...)	121
	Validation des procédures de backup	122
	Vérification de la bonne gestion/corrélation des logs	123
	Mise en concurrence	124
	Bilan de conformité annuel	125
Négligence d'un sous-traitant / fournisseur (IoT)	Contrôles préalables à la contractualisation (clauses contractuelles types approuvées par la Commission et/ou la CNIL, BCR)	126
	Intégration de clauses contractuelles de rupture en cas de négligence	127
	Revue opérationnelle régulière avec le sous-traitant	128
	Utilisation de la stéganographie (dissimulation de données dans d'autres données) ou de données pièges pour identifier la source du problème	129
	Gestion des incidents et notification à l'autorité de contrôle et/ou aux personnes concernées	130
	Audit régulier sur sous-traitant	131
Intervention frauduleuse d'un sous-traitant	Service de fraude avec contrôle et surveillance	132
	Vérifications de précaution sur la santé financière du sous-traitant	133
	Encadrement contractuel (clauses contractuelles types approuvées par la Commission et/ou par la CNIL, BCR)	134
	Contrôle des accès	135
	VPN partenaire	136
	Gestion des incidents et notification à l'autorité de contrôle et/ou aux personnes concernées	137
	Utilisation de la stéganographie, ou insertion de données pièges, pour identifier la source du problème	138
	Audit régulier du sous-traitant	139
Protection des données	**Protection des données**	
Défaut de cartographie (actualisée) des données et des traitements (défaut de tenue d'un registre des traitements et/ou des violations de données personnelles)	Procédure de cartographie/inventaire des données métiers (catégories de données, finalités, destinataires, durée de conservation, types de support, etc…), régulièrement tenu à jour et analysé	140
	Registre du CIL/DPO (obligatoire)	141

SG2 Mesures et recommandations potentiellement applicables pour être conforme au GDPR

ONGLET 2 : Mesures par types de risques

Types de Risques	Mesures techniques possibles	
Sécurité du SI	Sécurité du SI	#
et/ou des violations de données personnelles)	Dictionnaire de données (catégories de données: données courantes, données perçues comme sensibles, données sensibles)	142
Localisation non autorisée de données personnelles	Information/sensibilisation sur les contraintes de localisation des données dans les pays concernés	143
	Maîtrise des données et traitements des services concernés	144
	Déploiement d'une solution de data management	145
	Revue des contrats des sous-traitants	146
	Insertion de clauses spécifiques	147
Non respect des réglementations locales (ex. égalité des chances aux US, …)	Implication de juristes locaux	148
	Sensibilisation/Formation des équipes métiers et IT	149
	Gestion des droits d'accès	150
	Cartographie des données et des réglementations applicables localement	151
	Déclaration simplifiée/normale, et autorisation préalable	152
	Data masking (anonymisation dynamique/ non persistante)	153
	Non respect des formalités préalables applicables au traitement en France (déclaration simplifiée, déclaration normale, autorisation préalable de la CNIL exigible jusqu'au 28 mai 2018).	154
Absence de cloisonnement des données personnelles	Cloisonnement fonctionnel (logique) et infra dédiée (physique) si nécessaire	155
	Sensibilisation/Formation des équipes métiers et IT	156
	Gestion des droits d'accès	157
	Gouvernance de la donnée interne	158
	Chiffrement des bases de données	159
Non respect des règles de rétention (durée de conservation) des données	Politique de rétention/conservation des données	160
	Mise en place d'une gouvernance de la donnée en interne	161
	Sensibilisation/Formation des équipes métiers et IT	162
	Gestion des droits d'accès	163
	Mise en place de traitements automatisés de purge	164
	Gestion des logs	165
	Audits outillés	166
	Utilisation de dispositifs de Privacy by Design ou de Privacy by Re-Design	167
	Intégration de marqueurs des données	168
Transfert non sécurisé de données personnelles	Intégrer les contraintes dès la phase de design (privacy-by-design)	169
	Politique sur les droits et devoirs en matière de transfert interne/externe des données	170
	Chiffrement et anonymisation	171
	Encadrement contractuel avec le partenaire (NDA, clause de confidentialité, clause de suppression des données…)	172
	Contrôle des accès	173
	Gestion centralisée des logs (SIEM, Security Information Event Management)	174
	EDRM, Enterprise Digital Right Management (protection bureautique avec chiffrement, ou watermarking qui consiste à cacher un copyright dans un fichier…)	175
	Mise en place d'outils de DLP	176
	Limitation des accès webmail	177
	Interdiction de clés usb (dans certains pays)	178
	Blocage de sites de transferts (type wetransfer, dropbox…)	179
	Détection de téléchargements/transferts de fichiers importants	180
	Intégration de données pièges (stéganographie)	181
	Audit	182
	Sensibilisation/Formation utilisateurs et IT	183
	Filtrage IP des applications multi-tiers (firewalls applicatifs)	184
	Mise en place d'une politique de DLP (Data Leakage Prevention) et des outils associés	185
	Gestion des incidents et notification à l'autorité de contrôle et/ou aux personnes concernées	186
Transferts non encadrés de données hors UE	Définition et validation officielle de règles contraignantes d'entreprise (ou Binding Corporate Rules - BCR)	187
	Clauses contractuelles types	188
	Accord explicite et éclairé des individus	189
	Marquage et traçabilité des données	190
	Contrôle des accès	191
Accès non conforme ou non encadré aux données personnelles	Politique de gestion des habilitations, de gestion des accès, et de gestion des identifications	192
	Sensibilisation utilisateur et IT	199
	Audits réguliers	200
	Cloisonnement des données	201
	Gestion des incidents et notification à l'autorité de contrôle et/ou aux personnes concernées	202
Propagation malveillante de données personnelles	Veille sur internet (web, réseaux sociaux, dark web ou black market)	203
	Chiffrement, pseudonymisation, anonymisation	204
	Intégration de données pièges (fingerprinting)	205
	Contrôle des accès	206
	Gestion des logs	207
	Audits	208
	Politiques et moyens de prévention, détection, alerte, data breach, et réaction	209
	Tests d'activation de la cellule de crise	210
	Gestion des incidents et notification à l'autorité de contrôle et/ou aux personnes concernées	211
Divulgation de données personnelles par inadvertance	Sensibilisation utilisateur et IT	212
	Politique d'utilisation des réseaux sociaux	213
	Contrôle des accès	214
	Gestion des logs	215
	Audit	216
	Filtrage IP des applications multi-tiers	217
	Notification immédiate (lorsque nécessaire) à l'autorité de contrôle et/ou aux personnes concernées	218
	Transmission sécurisée des données (flux chiffrés)	219

SG2 Mesures et recommandations potentiellement applicables pour être conforme au GDPR

ONGLET 2 : Mesures par types de risques

Types de Risques	Mesures techniques possibles	
Sécurité du SI	**Sécurité du SI**	**#**
Vol de données	Mesures de sécurité du SI	220
	Politique de gestion des demandes de rançon	221
	Politique de notification (dt formulaire CNIL de notification)	222
	Politique de gestion de crise	223
	Cloisonnement des équipements	224
	Contrôle des accès	225
	Chiffrement base de données	226
	Chiffrement disques	227
	Blocage des ports usb	228
	Blocage des sites de transfert	229
	Veille sur les marchés clandestins (Dark web / Black Market)	230
	Validation contractuelle	231
	EDRM	232
	Gestion et corrélation des logs (mise en place d'un SIEM)	233
	Filtrage IP des applications multi-tiers	234
	Gestion des incidents et notification à l'autorité de contrôle et/ou aux personnes concernées	235
	Politique de changement des mots de passe	236
	Procédure d'inforensic	237
Perte d'intégrité des données	Sauvegardes et tests réguliers des sauvegardes	238
	Gestion et corrélation des logs	239
	Système de détection précoce d'atteinte volumétrique (cryptolocker)	240
	Traçabilité des actions sur les services (logs applicatifs)	241
	Audits	242
	Contrôle d'intégrité (CRC, signature cryptographique…)	243
	Test du bon fonctionnement des applications	244
	Qualification des incidents utilisateurs	245
	Gestion des incidents et notification à l'autorité de contrôle et/ou aux personnes concernées	246
Détention ou utilisation abusive de données personnelles	Contrôle des accès (validation de la demande, séparatiion des tâches, revue des accès…)	247
	Sensibilisation/formation utilisateurs et IT	248
	Alignement entre données détenues et finalité du traitement	249
	Politique de rétention des données	250
	Gestion et corrélation des logs	251
	Encadrement contractuel	252
	Mesures de traçabilité, audit, notification	253
	Gestion des incidents et notification à l'autorité de contrôle et/ou aux personnes concernées	254
Détournement de finalité de traitements de données personnelles du fait d'une mauvaise anonymisation	Inventaire des traitements de données personnelles	255
	Intégration de la privacy-by-design dans la méthodologie projet	256
	Déclaration des traitements	257
	Minimisation des données (privacy by design)	258
	Implication du délégué à la protection des données (CIL/ DPO)	259
	Gestion des incidents et notification à l'autorité de contrôle et/ou aux personnes concernées	260
Reconstitution de l'identité d'une personne et enrichissement de son profil par corrélation entre plusieurs sources internes ou externes (big data)	Anonymisation permanente	261
	Audit de la robustesse de l'anonymisation (exemple de techniques d'anonymisation : évaluation k-anonymat, L-diversité, t-proximité)	262
	Utilisation de données agrégées ou généralisées	263
	Pas de données personnelles dans les traitements de big data	264
	Sensibilisation/Formation utilisateurs	265
	Limitation et contrôle des accès aux données personnelles	266
	Mise en place d'une charte éthique spécifique	267
	Traçabilité et audit	268
Défaut de PIA/ EIVP	Intégration de la PIA dans la méthodologie projet	269
	Méthodologie PIA/ EIVP (dont analyse de risque)	270
Défaut de privacy by design (absence de règles sur la minimisation des données à celles strictement nécessaires et/ou non application des règles sur la minimisation)	Politiques de sécurité et charte utilisateur du SI	271
	Intégration des équipes Sécurité dans les projets	272
	Formation des équipes	273
	Déploiement d'exigences de bonne pratique Privacy by Design (minimisation, accès strictement nécessaires…)	274
	Politique de minimisation des données (privacy by design)	275
	Vérification de la privacy-by-design dans les phases de recettes	276
	Intégration d'une procédure de "Privacy by Re-Design" (gestion des évolutions)	277
Défaut de notification d'une atteinte aux données	Procédure de qualification des incidents de sécurité	278
	Procédure de notification précisant notamment quand une notification est nécessaire et à qui (à l'autorité de contrôle, à la personne)	279
	Suivi et évaluation des conséquences	280
	Implication du délégué à la protection des données (CIL/ DPO)	281
	Formation des équipes	282
Droits de la personne	**Droits de la personne**	
Incapacité à répondre aux droits des personnes (exécution des droits)	L'exécution des droits de la personne impose avant tout de bien savoir authentifier le demandeur. L'entreprise a 2 mois pour répondre à la demande. Un registre centralisé des données personnelles doit être détenu/accessible par le DPO	283
	Intégration des obligations du droit des personnes dés la conception des nouveaux services (privacy-by-design). Prévoir aussi de le faire à l'occasion d'un privacy-by-re-design pour les services legacy sensibles (éventuellement via des procédures manuelles de contournement...)	284
	Politique pour les services existants dans lesquels la réponse aux droits des personnes n'a pas été prévue à l'origine	285
	CIL/DPO, point de contact unique, et instructions pour le contacter	286
	Accès libre service pour une partie des informations, possibilité de rectification	287
	Catégorisation des traitements	288
	Rationalisation du processus de recueil et mise à jour des consentements	289

SG2 Mesures et recommandations potentiellement applicables pour être conforme au GDPR

ONGLET 2 : Mesures par types de risques

Types de Risques	Mesures techniques possibles	
Sécurité du SI	Sécurité du SI	#
	Traçabilité des consentements	290
	Limitation du traitement	291
	Limitation de la durée de conservation	292
	Purges automatisées, ou alertes avant atteinte de la limite rétention	293
	Outil de text mining sémantique (détection des termes sensibles ou injurieux / champs commentaires)	
	Règles des possibilités de profilage	294
	Politique de non-référencement des mineurs (sauf consentement formel et tracé des parents)	295
Information (clarté sur les politiques de confidentialité, les objectifs de collecte, les conditions générales de vente, à valider via une case à cocher…)	Politique de confidentialité et de données à caractère personnel (comprenant les informations sur l'identité et les coordonnées du RP, les coordonnées du DPO, la nature des données collectées, les finalités, la durée de conservation, les destinataires, les éventuels transferts vers des pays tiers, etc.)	296
	Information par un message au moment de la collecte des données (nature des données collectées, finalités, destinataires, comment exercer ses droits d'accès, d'opposition et de modification des données, etc.):par exemple, sur internet: via un message facilement accessible sur le site; salarié: dans son contrat de travail, etc.	297
Transparence du traitement	Information de la personne concernée de la nature des données collectées et des finalités de traitement, identité du RP, etc.	298
Preuve du consentement	Vérifier si le traitement ne repose pas sur une autre base légale que le consentement (obligation légale, sauvegarde de la vie, mission de service public, contrat ou mesures prises avec la personne, intérêt légitime).	299
	S'assurer que le traitement ne puisse pas être mis en oeuvre sans consentement.	300
	S'assurer que le consentement sera obtenu de manière libre.	301
	S'assurer que le consentement sera obtenu de manière éclairée et transparente quant aux finalités du traitement.	302
	S'assurer que le consentement sera obtenu de manière spécifique à une finalité.	303
	En cas de sous-traitance, encadrer les obligations de chacun dans un document écrit, explicite et accepté des deux parties	304
	Pour un site internet: opt-in; cookies (avec un bandeau); email récapitulatif Pour un salarié ou un partenaire commercial: contrat signé	305
Retrait du consentement (opposition ou suppression)	Vérifier que le traitement ne fait pas l'objet d'une exception interdisant à la personne de s'opposer au traitement (obligation légale, exclusion dans l'acte portant création du traitement)	306
	Déterminer les moyens pratiques qui vont être mis en oeuvre pour permettre l'exercice du droit d'opposition. Ce droit doit pouvoir être exercé le plus rapidement possible, sans jamais excéder deux mois, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches à effectuer ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais. Ex: Pour un site internet, créer un formulaire, facilement accessible, avec des cases à décocher (dit « opt-out ») ou prévoir la possibilité de se désinscrire d'un service (suppression de compte).	307
	Vérifier que les demandes d'exercice du droit d'opposition faites par voie postale sont signées et accompagnées de la photocopie d'un titre d'identité (qui ne devrait pas être conservée sauf en cas de besoin de conserver une preuve) et qu'elles précisent l'adresse à laquelle doit parvenir la réponse. Vérifier que les demandes d'exercice du droit d'opposition faites par voie électronique (en utilisant un canal chiffré si la transmission se fait via Internet) sont accompagnées d'un titre d'identité numérisé (qui ne devrait pas être conservé sauf en cas de besoin de conservation d'une preuve, et ce, en noir et blanc, en faible définition et sous la forme d'un fichier chiffré).	308
	S'assurer que le motif légitime des personnes exerçant leur droit d'opposition est fourni et apprécié	309
	S'assurer que tous les destinataires du traitement seront informés des oppositions exercées par des personnes concernées	310
Respect de la limite du traitement	Vérifier que le ou les motifs pour lesquels l'effacement est demandé s'appliquent: - l'exactitude des données à caractère personnel est contestée par la personne concernée, pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel; - le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation; - le responsable du traitement n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice; - la personne concernée s'est opposée au traitement, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par le responsable du traitement prévalent sur ceux de la personne concernée.	311
	Déterminer les moyens pratiques qui vont être mis en oeuvre pour permettre l'exercice du droit de limitation. Ce droit doit pouvoir être exercé le plus rapidement possible, sans jamais excéder deux mois pour des données, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais excédant le coût de la reproduction.	312
Accès	Déterminer les moyens pratiques qui vont être mis en oeuvre pour permettre l'exercice du droit d'accès. Ce droit doit pouvoir être exercé le plus rapidement possible, sans jamais excéder deux mois pour des données, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais excédant le coût de la reproduction.	313
	Vérifier que les demandes d'exercice du droit d'accès faites sur place permettent de s'assurer de l'identité des demandeurs et des personnes qu'ils peuvent mandater.	314
	Vérifier que les demandes d'exercice du droit d'accès faites par voie postale sont signées et accompagnées de la photocopie d'un titre d'identité (qui ne devrait pas être conservée sauf en cas de besoin de conserver une preuve) et qu'elles précisent l'adresse à laquelle doit parvenir la réponse. Vérifier que les demandes d'exercice du droit d'accès faites par voie électronique (en utilisant un canal chiffré si la transmission se fait via Internet) sont accompagnées d'un titre d'identité numérisé (qui ne devrait pas être conservé sauf en cas de besoin de conservation d'une preuve, et ce, en noir et blanc, en faible définition et sous la forme d'un fichier chiffré).	315
	S'assurer de la possibilité de fournir toutes les informations qui peuvent être demandées par les personnes concernées, tout en protégeant les DCP des tiers.	316
	S'assurer que l'identité des demandeurs et que la légimitimité des limitations demandées seront vérifiées.	317
	S'assurer qu'une confirmation sera fournie aux demandeurs.	318
	S'assurer que les tiers à qui des données auraient été transmises seront informés des demandes de limitation.	319
Rectification	Vérifier que le traitement ne fait pas l'objet d'une exception (Ex: sûreté de l'État, défense ou sécurité publique).	320
	Déterminer les moyens pratiques qui vont être mis en oeuvre pour permettre l'exercice du droit de rectification. Ce droit doit pouvoir être exercé le plus rapidement possible, sans jamais excéder deux mois, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches à effectuer ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais.	321
	S'assurer que l'identité des demandeurs et que la véracité des rectifications demandées seront vérifiées.	322
	S'assurer qu'une confirmation sera fournie aux demandeurs.	323

SG2 Mesures et recommandations potentiellement applicables pour être conforme au GDPR		
ONGLET 2 : Mesures par types de risques		
Types de Risques	**Mesures techniques possibles**	
Sécurité du SI	**Sécurité du SI**	**#**
	S'assurer que les tiers à qui des données auraient été transmises seront informés des rectifications faites.	324
Effacement, droit à l'oubli	Vérifier que le ou les motifs pour lesquels l'effacement est demandé s'appliquent: - les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière; - la personne concernée retire le consentement sur lequel est fondé le traitement, et il n'existe pas d'autre fondement juridique au traitement; - la personne concernée s'oppose au traitement et il n'existe pas de motif légitime impérieux pour le traitement - les données à caractère personnel ont fait l'objet d'un traitement illicite - les données à caractère personnel doivent être effacées pour respecter une obligation légale, etc.	325
	Déterminer les moyens pratiques qui vont être mis en oeuvre pour permettre l'exercice du droit d'effacement. Ce droit doit pouvoir être exercé le plus rapidement possible, sans jamais excéder deux mois, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches à effectuer ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais.	326
	S'assurer que l'identité des demandeurs et que la légimitimité de l'effacement demandé seront vérifiées.	327
	S'assurer qu'une confirmation sera fournie aux demandeurs.	328
	S'assurer que les tiers à qui des données auraient été transmises seront informés des demandes d'effacement.	329
Portabilité	Vérifier que le traitement ne fait pas l'objet d'une exception (Ex: missions d'intérêt public ou relevant de l'exercice de l'autorité publique).	330
	Déterminer les moyens pratiques qui vont être mis en oeuvre pour permettre l'exercice du droit à la portabilité. Ce droit doit pouvoir être exercé le plus rapidement possible, sans jamais excéder deux mois, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches à effectuer ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais.	331
	S'assurer que l'identité des demandeurs et que la légimitimité de la portabilité demandée seront vérifiées.	332
	S'assurer qu'une confirmation sera fournie aux demandeurs.	333
	S'assurer que les tiers à qui des données auraient été transmises seront informés de la portabilité faite.	334
Profilage	Vérifier que le traitement ne fait pas l'objet d'une exception (Ex: le profilage est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement; consentement explicite, etc.).	335
	Déterminer les moyens pratiques qui vont être mis en oeuvre pour permettre l'exercice du droit à s'opposer au profilage. Ce droit doit pouvoir être exercé le plus rapidement possible, sans jamais excéder deux mois, dans une forme similaire à celle du traitement (voie postale et/ou voie électronique). En outre, les démarches à effectuer ne doivent pas décourager les personnes concernées et ne doivent pas leur occasionner de frais.	336
Données des mineurs	Vérifier l'âge du mineur (si + ou - de 16 ans). Si - de 16 ans, le traitement n'est licite que si, et dans la mesure où, le consentement est donné ou autorisé par le titulaire de la responsabilité parentale à l'égard de l'enfant	337

REMERCIEMENTS

Ce document est le fruit de l'initiative des trois organisations professionnelles AFAI, CIGREF, TECH IN France et des travaux des trois groupes de travail qu'elles ont co animés pendant un an avec le concours d'experts (cabinet August Debouzy, De Gaulle Fleurance & Associés, Osborne Clarke, SAMMAN) et des adhérents des associations qui ont bien voulu participer.

L'AFAI, le CIGREF et TECH IN France tiennent à remercier tout particulièrement les entreprises et les cabinets d'avocats qui se sont engagés dans l'initiative DPSI.

Éditeurs :

AFAI, association loi 1901 – Centre d'Affaires Alac Etoile, 3 rue du Colonel Moll, 75 017 PARIS – Tél : +33 1 40 08 47 81 – https://www.afai-isaca.fr

CIGREF, association loi 1901 – 21 avenue de Messine, 75008 PARIS – Tél. : +33 1 56 59 70 00 – http://www.cigref.fr/

TECH IN France, association loi 1901 - 13 Rue La Fayette, 75009 Paris - Tél. : +33 1 40 32 45 90 - http://www.techinfrance.fr/

Directeurs de publication : Pascal Antonini, AFAI ; Régis Delayat, CIGREF ; Loïc Rivière, TECH IN France.

Groupe de travail : Sous-groupe 1 présidé par Pascal Antonini (AFAI), coordonné par Bertrand Helfre (EY), avec le concours de Florence Chafiol et Stéphanie Lapeyre (August Debouzy) ; Sous-groupe 2 présidé par Régis Delayat (CIGREF), coordonné par Flora Fischer (CIGREF) et Sophie Bouteiller (SCOR), avec le concours de Jean-Sébastien Mariez et Marie-Mathilde Deldicque (De Gaulle Fleurance & Associés) ; Sous-groupe 3 présidé par Loïc Rivière (TECH IN France), coordonné par Camille Parra (TECH IN France) avec le concours de Thaima Samman et Marc Drevon (Cabinet Samman) et Béatrice Delmas-Linel et Lise Breteau (Osborne Clarke).

Coordination Éditoriale : Camille Parra (TECH IN France) et Flora Fischer (CIGREF)

Création graphique et réalisation : Juliette Bernard (TECH IN France) et Thibault Luret (CIGREF)

Relations Presse :

AFAI : Isabelle Mauriac - 06 27 70 71 60 - imauriac@imedia-conseil.fr - 3 rue du Colonel Moll 75017 PARIS - www.afai-isaca.fr

CIGREF : Thibault Luret - 06 45 49 93 75 - tluret@cigref.fr - 21, avenue de Messine, 75008 PARIS - www.cigref.fr

TECH IN France : Stéphanie Muthelet – 01 55 74 52 28 – 06 18 05 12 70– https://www.rumeurpublique.fr – 9 rue Alphonse de Neuville, 75017 PARIS

afai
Pour des systèmes d'information de confiance et créateurs de valeur

3 rue du Colonel Moll
75 017 PARIS

+33 (0)1 40 08 47 81

cigref
réussir le numérique

21 avenue de Messine
75008 PARIS

+33 (0)1 56 59 70 00

TECH'IN
FRANCE

13, rue La Fayette
75009 Paris

+33 (0)1 40 32 45 90