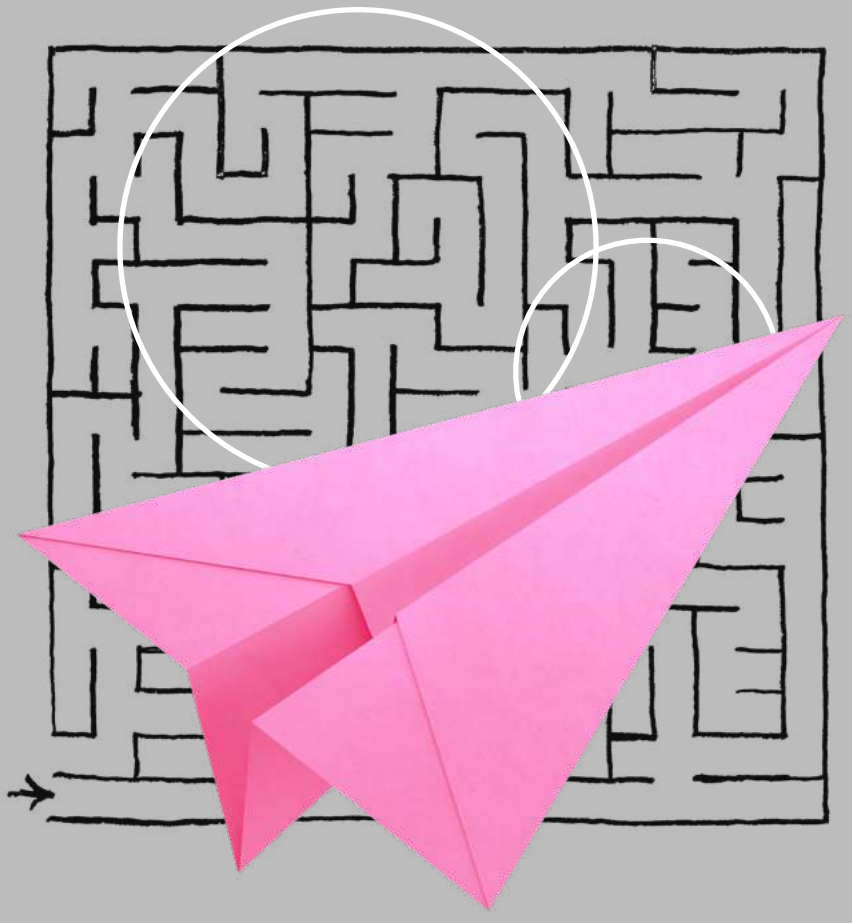
LIVRE BLANC



RGPD

BONNES PRATIQUES
ET NOUVELLES RESPONSABILITÉS

TECH'IN FRANCE

RGPD

BONNES PRATIQUES
ET NOUVELLES RESPONSABILITÉS

SOMMAIRE

EDITO

Protection des données à caractère personnel : Au-delà de la conformité, une opportunité !

La plupart des entreprises ont conduit des projets RGPD avec une approche purement conformité, le plus souvent sous la contrainte du risque de niveau élevé du montant des sanctions (le plus élevé de 4% du chiffre d'affaires mondial ou 20 M€). Avec le RGPD, la protection des données à caractère personnel est passée d'un modèle basé sur la déclaration des traitements aux autorités (la Cnil en France) et l'application de principes de protection de ces données, à un modèle basé sur « l'accountability » et la mise en œuvre de mesures spécifiques lors de la conception et par défaut (Privacy by Design et by Default). Par conséquent, dans ce nouveau paradigme, **les responsables de traitement se doivent de documenter leur cadre de gestion de la protection des données** conformément aux dispositions du RGPD.

Sur cet axe de conformité, la maturité des entreprises est aujourd'hui assez hétérogène selon leur secteur d'activité bien sûr, mais aussi en fonction de l'appétence des directions générales vis-à-vis du sujet. Les plus matures d'entre-elles ont mis en place des systèmes complets de management de la protection des données reposant sur une gouvernance forte ; elles ont lancé ou s'apprêtent à lancer des projets de déploiement de solutions technologiques permettant de faciliter et d'optimiser la gestion au jour le jour de cette conformité.

Plus rares sont celles qui ont profité de l'arrivée du RGPD pour aller au-delà de la conformité et faire de la protection des données à caractère personnel un axe majeur de renforcement de la confiance des clients, des collaborateurs, des partenaires et plus généralement du public. Pourtant, la protection des données personnelles constitue un des droits fondamentaux de l'Union Européenne et s'inscrit au chapitre des libertés individuelles. **Au-delà de la conformité, c'est le caractère éthique de l'utilisation des données** à caractère personnel qui doit être mis au centre des préoccupations des directions générales, cette notion d'éthique et de liberté individuelle étant à la base du RGPD.

L'accroissement des violations de données à caractère personnel liées à des cyberattaques, combiné au développement de la collecte de ces données rend le public de plus en plus sensible à leur protection. Les données que nous sommes susceptibles de confier à des entreprises, des administrations ou autres organisations sont le reflet de notre intimité et méritent, à ce titre, d'être considérées autrement que comme « l'or noir » de l'économie numérique. Les entreprises qui sauront se différencier en valorisant leurs pratiques de protection des données à caractère personnel avec un haut niveau de transparence obtiendront la confiance de leurs clients et du public en général alors même que dans un monde où l'incertitude est à un niveau rarement égalé, la recherche de confiance est forte.

A cet égard, l'opinion publique européenne est très sensible sur ces sujets. Outre l'amélioration et la structuration des traitements engendrées par le RGPD, il donne aux entreprises l'occasion d'afficher concrètement leurs convictions en matière d'éthique contribuant ainsi à leur bonne réputation.

Si l'on considère également diverses études réalisées depuis le milieu des années 2000 montrant que la performance des entreprises qui offrent un niveau de confiance élevé est accrue, cela renforce la nécessité de travailler sur cet axe.

Dans ce contexte, les directions générales doivent se saisir du sujet de la protection des données à caractère personnel et agir sur différents leviers (ils sont notamment mis en évidence dans le livre blanc de l'ISACA Privacy Beyond Compliance publié en septembre 2020) :

Développer la culture de protection des données à caractère personnel (privacy) ;

Clarifier les conditions dans lesquelles certains services sont offerts en échange de la collecte de données à caractère personnel en offrant la possibilité au consommateur d'exercer un véritable choix ;

S'assurer de la bonne mise en œuvre des concepts de « Security by design » et « Privacy by design » pour assurer la protection des données à caractère personnel des clients ;

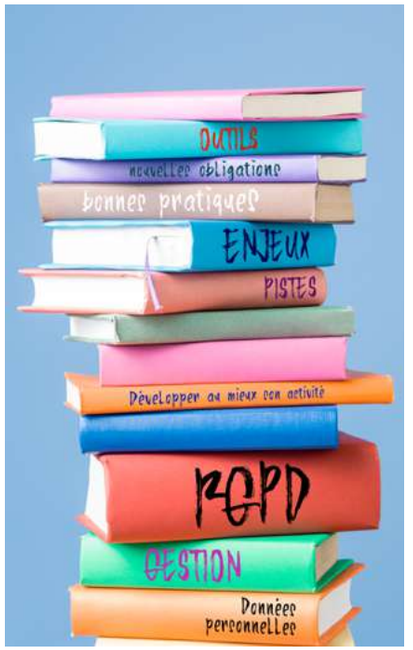
Donner de la transparence sur les algorithmes notamment dans le contexte de l'utilisation d'analytics, d'intelligence artificielle ou de « machine learning » dans le contexte de traitements de données à caractères personnel ;

Considérer les données à caractère personnel comme des données relatives à la vie réelle d'un individu et non pas comme un actif à valoriser.

La prise de conscience des comités de direction des immenses enjeux de ces différents sujets est aujourd'hui indispensable pour dépasser la stricte conformité et valoriser les données à caractère personnel. Mettre les droits et les libertés des personnes au cœur des préoccupations de l'entreprise lui permettra d'instaurer une relation de confiance vertueuse avec son environnement et ainsi contribuer largement à son développement.

Par Pascal Antonini, Associé EY Consulting, Vice-Président ISACA-AFAI

RGPD : Des évolutions permanentes qui nécessitent l'adoption de bonnes pratiques



Le RGPD a sans conteste rebattu les cartes de la gestion des données personnelles en entreprise. Depuis maintenant près de deux ans, le règlement général sur la protection des données renforce le rôle des éditeurs dans leur dimension d'accompagnement et de transformation numérique de l'écosystème. Une véritable fonction opérationnelle mais également prospective dans la mesure où les implications qu'emportent le texte évoluent du fait des mutations technologique, de la multiplication des usages ou des inflexions que prend la jurisprudence.

Le constat est donc évident. La donnée représente un actif stratégique pour n'importe quelle entité professionnelle. **Un véritable « or noir » dont chacun doit s'emparer afin de dégager de nouvelles opportunités de développement et d'actionner des leviers de croissance forts**. A condition toutefois de manier ces éléments comme il se doit et de respecter les règles normatives actuelles.

C'est dans cette optique que vient se nicher un impérieux besoin d'établir un cadre novateur en matière d'application du RGPD. Un ensemble de bonnes pratiques dont chaque professionnel peut s'emparer afin de développer au mieux son activité. Pour les éditeurs, ce recueil a ainsi vocation à dégager les moyens de mieux accompagner leurs clients dans l'observance des textes de lois dans leur dimension purement juridique mais également pratique. Ce livre blanc se fait fort de dégager des pistes d'anticipation de la règlementation et des usages afin d'adopter une posture prospective face aux enjeux à venir.

L'ambition est **de pouvoir bâtir des stratégies de gestion des règles régissant l'utilisation des données personnelles.** L'enjeu est de taille à l'heure où nombre d'utilisateurs des outils numériques s'arment de méfiance quant au cheminement de leurs propres informations. Une récente étude menée en mai 2019 par la Chaire Valeurs et Politiques des Informations Personnelles de l'Institut Mines-Télécom (dont Dassault Systèmes et la Cnil sont partenaires) se révèle instructive. En France, les internautes sont encore plus vigilants par rapport à il y a quelques années (ils étaient déjà 54% dans l'enquête de 2017). Parmi ceux-ci, 57% se sentent davantage surveillés par les entreprises privées proposant des services de type moteur de recherche, réseaux sociaux, sites de commerce électroniques... Or la confiance est un enjeu économique majeur : c'est elle qui, *in fine*, détermine l'adhésion ou non à un service. Une problématique forte aux mains des professionnels et des responsables de traitement, lesquels peuvent s'appuyer en confiance sur les éditeurs de logiciels.

La confiance constitue en effet un socle fort pour qui entend traiter données personnelles et identités et ainsi défendre une souveraineté numérique. Cette dernière contribue de facto à développer la confiance des entreprises et de leurs partenaires.

Dès lors, plus d'un an après l'entrée en vigueur du RGPD, qu'est ce qui a réellement changé ? Le règlement a apporté nombre de nouveautés d'un point de vue technologique mais également pratique. Le texte a en effet introduit des nouveaux mécanismes de responsabilité pour l'ensemble de la chaîne de valeur traitant des données. **Une « accountability » véritable dont il convient de tracer les contours et de délimiter correctement les effets.** Cette dernière échoit par nature au responsable du traitement des données personnelles. Toutefois, l'éditeur peut, dans une certaine mesure, être tenu responsable en cas de manquement grave.

__57%__ des internautes se sentent davantage surveillés par les entreprises proposant des moteurs de recherche, réseaux sociaux, sites de e-commerce...

C'est pourquoi ce document se propose d'aborder un volet juridique nécessaire à toute étude du sujet en présentant des positions d'experts. L'objectif étant de traiter des nouvelles obligations des professionnels en la matière tout en optimisant l'intégration et le suivi RGPD au sein de l'entreprise. Dans un second temps, des professionnels expliqueront comment implémenter au mieux la réglementation non seulement chez les clients mais également chez les partenaires. Puis, le document abordera les solutions technologiques pertinentes ainsi que les rôles de chacun dans ce suivi permanent qu'impose le texte.

Enfin, il ne serait de guide pertinent sans l'apport de retours d'expériences. Ce livre blanc propose ainsi de donner la parole à ceux qui manipulent les données au quotidien. Un guide de bonnes pratiques, afin de conduire les professionnels dans la direction la plus à même d'épouser les évolutions futures de la réglementation et des évolutions technologiques.

Les citations à connaître ...

> *Contrairement aux idées reçues, le RGPD ne fait pas référence à la conformité du logiciel. En réalité, le client - qui est très souvent un responsable de traitement - garde deux responsabilités importantes : le choix de son logiciel, d'une part, et l'utilisation qu'il en fait dans son contexte métier, d'autre part. C'est cet ensemble qui va l'engager vis-à-vis du RGPD.*

Chloé Rousselet,
Data Protection Officer Cegid,
page 36

> *Le fait que le RGPD impose une conformité du traitement dès la conception et par défaut change radicalement la donne : ces nouvelles exigences ont vocation à porter les obligations liées à la protection des données à caractère personnel au niveau de l'éditeur du logiciel.*

Sylvain Staub,
CEO de Data Legal Drive &
Avocat Associé DS Avocat
page 14

> *Le RGPD 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. 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.*

Béatrice Delmas-Linel,
Associée gérante Osborne
Clarke Paris

> *Le nombre de données produites sur le Web pour la seule année 2010 s'est élevé à 800 milliards de Gigabytes. Ce chiffre serait plus important que tout ce qui a été produit (écrits, films etc...) dans l'histoire de l'Humanité jusqu'à 2003.*

Eric Schmidt,
ex-PDG de Google

> *Les principaux risques qui peuvent affecter les données d'une organisation sont l'absence d'organisation et de compétences permettant d'aligner la connaissance des données, la stratégie et les opérations de l'entreprise. A ceci, il faut ajouter l'insuffisance du dispositif de contrôle interne permettant d'assurer la protection des données et le respect des réglementations.*

Jawaher Allala,
CEO de Systnaps, page 24

> *Le RGPD, par le fait des droits qu'il confère comme le droit à la portabilité, est un facteur d'innovation pour le déploiement de nouveaux services ou de nouveaux produits. Ce qui peut naturellement bousculer les dispositifs existants.*

Sophie Nerbonne,
Directrice chargée de co-régulation
économique, Cnil, page 31

> *Le RGPD met l'accent sur la finalité du traitement. Les marques doivent donc être sûres, et pouvoir prouver, que toutes les données récoltées ont une utilité.*

Solen Bienaise,
Consultante Data Scientist
Coheris

> *Le RGPD a été 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.*

Stanislas de Rémur,
Co-fondateur et CEO
d'Oodrive

... sur le RGPD

01

RGPD, DE NOUVELLES RESPONSABILITÉS POUR LES ÉDITEURS

Editeurs, à qui la responsabilité échoit-elle ?

Avis d'expert, Sylvain Staub, CEO, Data Legal Drive et Avocat Associé DS Avocats.

Faire rimer l'accumulation de données avec le RGPD.

Editeurs, à qui la responsabilité échoit-elle?

Selon un sondage IFOP réalisé en avril 2019 pour la Cnil, 70 % des Français se disent plus sensibles que ces dernières années quant à la protection de leurs données personnelles. Le sentiment est identique pour les professionnels. L"or noir numérique" devant être valorisé, la sécurisation et la protection des datas constituent à ce titre des attentions de tous les instants.

A grandes fonctions, grandes responsabilités. Les éditeurs disposent désormais d'un rôle majeur dans l'ensemble de la chaîne de valeur relative aux données personnelles. Le RGPD et ses jurisprudences rebattent en effet les cartes de la responsabilisation des acteurs en place. Editeurs et clients bâtissent des relations fortes au fil des services déployés qui inclut également un régime de responsabilité pour chacun quant au traitement de ces mêmes datas.

En France, la justice a défini un cadre général, mais des exceptions se sont progressivement insérées dans ce mécanisme. L'arrêt du 25 mai 2018 énonce que le responsable du traitement est, par défaut, responsable de toute situation pouvant survenir. Mais la responsabilité du sous-traitant peut, dans certains cas, être engagée. Ce dernier devant alors avoir fait preuve de manquements véritables. Face à cette nouvelle obligation portée par les éditeurs, il demeure donc crucial de pouvoir anticiper tout problème éventuel.

__70%__ des Français se disent plus sensibles que ces dernières années quant à la protection de leurs données personnelles.

C'est pourquoi de nouvelles questions sont soulevées chaque jour par les professionnels et experts du sujet. Le RGPD oblige les éditeurs de logiciels à livrer des produits conformes mais également à s'assurer que leur produit est technologiquement responsable. Face à cette extension du domaine de la responsabilité, une délimitation et un éclairage bienvenu doivent être apportés.

AVIS D'EXPERT

Sylvain Staub

CEO Data Legal Drive & Avocat Associé DS Avocats

Les éditeurs de logiciels confrontés aux principes de *privacy by design* et de *privacy by default*

Quels sont les principes de protection des données dès la conception et par défaut ?

Le Règlement général sur la protection des données[1] applicable dans l'ensemble des Etats membres de l'Union Européenne depuis le 25 mai 2018, a introduit de nouvelles obligations à l'égard des personnes qui traitent des données à caractère personnel. Au nombre des nouvelles obligations se trouvent **deux principes, particulièrement innovants, qui consistent à assurer la protection des données dès la conception et par défaut**[2].

A travers ces principes de **« protection dès la conception »** (*privacy by design*) et de **« protection par défaut »** (*privacy by default*) il s'agit d'assurer **le respect de la vie privée des personnes concernées et d'éviter la violation de leurs données à caractère personnel, par l'adoption de mesures protectrices en amont et sans action de la part de ces personnes.**

Ajoutons que ces principes doivent s'appliquer aux projets initiés postérieurement au 25 mai 2018 et à ceux qui, bien qu'ils soient antérieurs à cette date, feraient l'objet d'une modification après l'entrée en application du RGPD. Dans ce cadre, l'article 25 du RGPD énonce que le responsable du traitement met en œuvre *« tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées ».* Son objectif demeurant alors la protection des droits de la personne concernée au moyen de mesures techniques appropriées pour garantir que sont traitées « *seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement.* »

A ceci s'ajoute le fait que les éditeurs de logiciels sont incités à « *s'assurer que [leurs clients] sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données. Les principes de protection des données dès la conception et de protection des données par défaut devraient également être pris en considération dans le cadre des marchés publics.* »

Quelles sont les obligations de l'éditeur de logiciels vis-à-vis de son client utilisateur ?

Un éditeur de logiciel est en premier lieu **fournisseur d'un bien incorporel,** en l'occurrence une solution logicielle, et à ce titre débiteur d'une « **obligation de délivrance** »[3] conforme aux prévisions contractuelles.

Au-delà de la délivrance conforme, il incombe également à l'éditeur de logiciel de mettre à la disposition de son client – profane en la matière – une compétence professionnelle, qui comprend **une obligation d'information**, voire **une obligation de conseil**[4] qui est la forme la plus avancée de l'obligation d'information. Cette obligation d'information qui pèse sur l'éditeur est à l'origine d'une part importante des litiges informatiques.

L'utilisateur d'un logiciel est tenu de respecter le RGPD, chaque fois qu'il réalise des traitements de données à caractère

LE SAVIEZ VOUS ?

Article 25 du RGPD sur les obligations des éditeurs :

« 1. Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, (…) le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées (…) afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée.

2. Le responsable du traitement met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées (…). »

personnel à travers l'utilisation dudit logiciel. Le défaut de prise en compte de la protection des données dès la conception et par défaut placerait d'office l'utilisateur en situation de manquement au regard de la réglementation (il en serait ainsi par exemple d'un logiciel qui prévoirait la saisie de données excédant ce qui est nécessaire à la poursuite des finalités de l'activité exercée).

« C'est pourquoi il semble difficilement envisageable pour l'éditeur de logiciels de faire abstraction de cette exigence qui intéresse l'usage effectif de la chose fournie »

C'est pourquoi il semble difficilement envisageable pour l'éditeur de logiciels de faire abstraction de cette exigence qui intéresse l'usage effectif de la chose fournie, au moins pour ceux des utilisateurs dont les activités de traitement sont soumises au RGPD. Au demeurant lorsqu'il délivre un service complémentaire à l'utilisateur du logiciel – qu'il s'agisse d'une prestation d'hébergement, de maintenance, etc. –, l'éditeur se voit qualifié de sous-traitant au sens du RGPD (cf. article 28); et en cette qualité, il est directement visé par le RGPD.

C'est ainsi qu'en tant que « *sous-traitant* » l'éditeur est tenu notamment de présenter « *des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du [RGPD] et garantisse la protection des droits de la personne concernée* »[5], de prendre « *toutes les mesures requises en vertu de l'article 32* » du RGPD[6], etc.

Qu'en est-il de l'émergence d'une cause de responsabilité de l'éditeur au titre des principes de protection des données dès la conception et par défaut ?

La conclusion d'un contrat suppose de la part des cocontractants la conscience des droits et obligations qui en résultent à leur égard. Dit autrement, dans tout processus contractuel chaque partie doit avoir conscience des risques qu'elle endosse, soit à raison de l'inexécution de ses propres obligations, soit en raison de l'inexécution des obligations de son cocontractant.

La Loi Informatique et Libertés dans ses versions antérieures au RGPD n'imposait pas explicitement la mise en œuvre d'une démarche de *privacy by design* et *by default*. La question d'une éventuelle obligation juridique des éditeurs de logiciels n'avait donc pas lieu d'être.

Le fait que le RGPD impose une conformité du traitement dès la conception et par défaut change radicalement la donne : ces nouvelles exigences ont vocation à porter les obligations liées à la protection des données à caractère personnel au niveau de l'éditeur du logiciel. Du reste, l'implication des éditeurs de logiciel à la conformité RGPD était en germe dans certains travaux du G29 antérieurs au texte. Tout particulièrement un avis de 2014 relatif à l'Internet des objets relevait **la difficulté pour les utilisateurs de modifier les paramétrages industriels paramétrés par défaut et recommandait aux éditeurs de fournir un niveau adéquat d'informations aux utilisateurs finaux**[7].

LE SAVIEZ VOUS ?

Article 25 considérant n° 78

« (…) Lors de l'élaboration, de la conception, de la sélection et de l'utilisation d'applications, de services et de produits (…) il convient d'inciter [les éditeurs de logiciels] à prendre en compte le droit à la protection des données (…) et, compte dûment tenu de l'état des connaissances, à s'assurer que [leurs clients] sont en mesure de s'acquitter des obligations qui leur incombent en matière de protection des données. Les principes de protection des données dès la conception et de protection des données par défaut devraient également être pris en considération dans le cadre des marchés publics. »

Le considérant n° 78 précité, qui vise à inciter les éditeurs de logiciels à « *prendre en compte le droit à la protection des données (…) [et] à s'assurer que [leurs clients] sont en mesure de s'acquitter des obligations qui leur incombent* », a donc confirmé cette orientation partagée à la fois par le législateur européen et par les organismes de régulation.

En pratique, cela signifie que l'obligation d'information et de conseil de l'éditeur de logiciels doit désormais intégrer les principes de protection dès la conception et par défaut ?

Ainsi, il est vraisemblable que les contentieux qui seront initiés à l'avenir sur le fondement d'un défaut de conseil de l'éditeur de logiciels et/ou d'un défaut de livraison conforme, seront complétés par l'argument du défaut de prise en compte des principes de protection dès la conception et par défaut (défaut de mise en garde sur le respect de la conformité au RGPD et défaut de conseil dans l'expression subséquente du besoin du client).

Certaines jurisprudences annoncent le risque judiciaire qui pèse désormais sur les éditeurs de logiciels. Il en est ainsi en particulier de la décision qui avait été rendue par la chambre commerciale de la Cour de cassation le 19 février 2008[8] au sujet du passage à l'an 2000, au terme de laquelle : « *(…) tout concepteur d'un progiciel a l'obligation de s'assurer que ce*

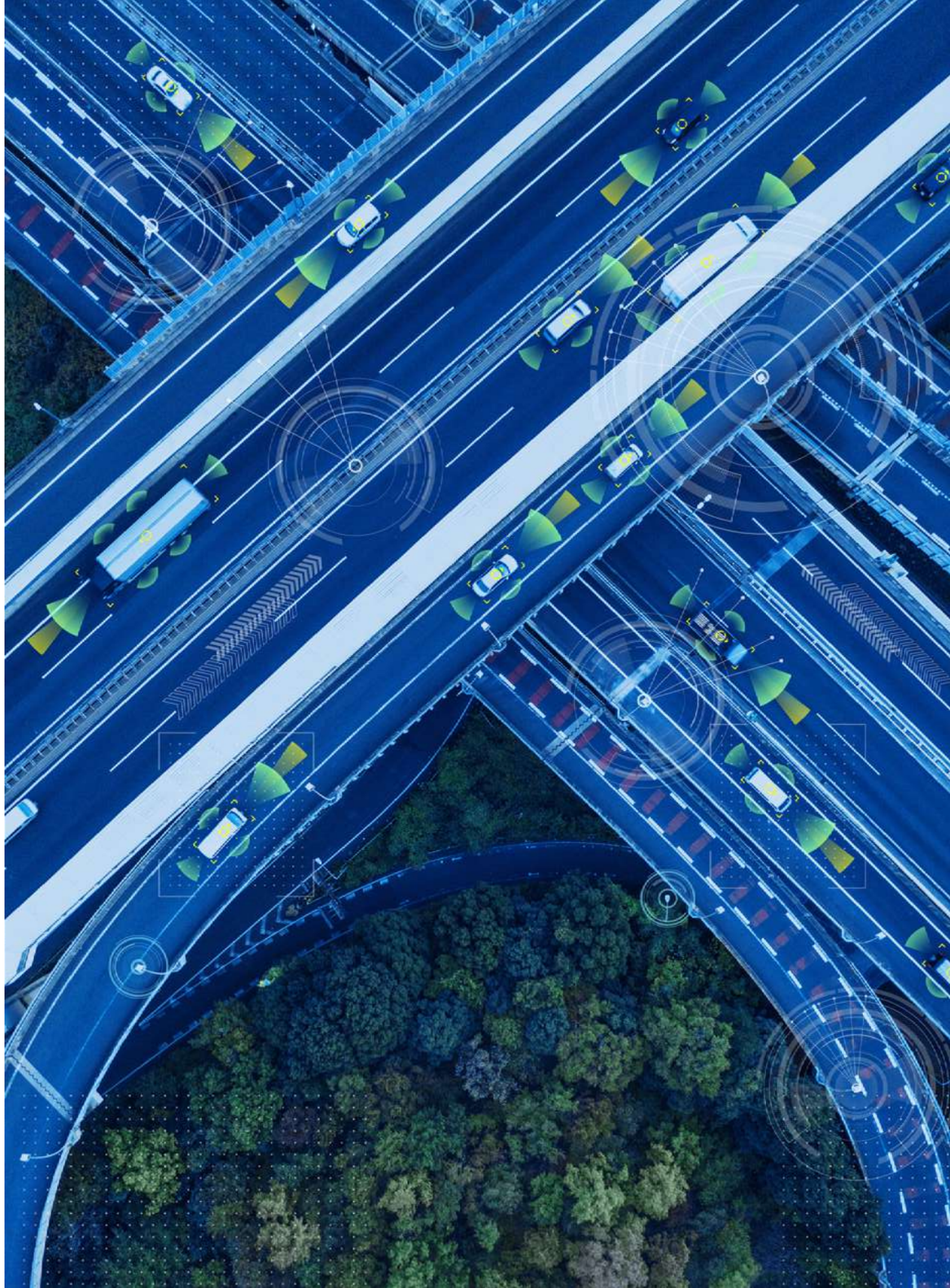
progiciel, au moment de sa cession, réponde tant aux besoins du client qu'aux obligations légales prévues ou prévisibles pour sa durée de vie (…) »

A ce stade on peut entrevoir une limite à cette nouvelle « obligation » des éditeurs de logiciels : l'obligation de conseil au regard des principes de protection dès la conception et par défaut (qui débouche sur l'obligation de fournir un logiciel adapté) ne vaudrait qu'au jour de la conclusion du contrat, l'éditeur ne s'engageant pas (sauf stipulations contractuelles en ce sens) à assurer la maintenance évolutive du logiciel – en l'occurrence la conformité à une réglementation postérieure au contrat – en cours d'exécution du contrat[9]. Autrement dit, seuls les logiciels vendus postérieurement à l'adoption du RGPD devraient être concernés.

Pour finir, on rappellera que le RGPD énonce dans son considérant 78 que les « *principes de protection des données dès la conception et de protection des données par défaut devraient également être pris en considération dans le cadre des marchés publics* ». Ce qui signifie que les principes de protection dès la conception et par défaut sont et seront de plus en plus des éléments de sélection des logiciels dans le cadre d'appels d'offres publics.
Nul doute que cette exigence se généralisera également dans le secteur privé ; d'ailleurs les opérateurs privés ont déjà tendance à se doter de guides ou de procédures en matière de protection des données dès la conception et par défaut, en vue de sélectionner leurs prestataires et les solutions logicielles qui répondent à leurs impératifs en matière de conformité au RGPD.

Il est possible d'en conclure que la sanction d'un logiciel qui ne tiendrait pas compte des principes de protection dès la conception et par défaut, sera économique (défaut de vente) avant d'être juridique (contentieux).

1. Règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données n°2016/679 du 27 avril 2016.
2. Les concepts de privacy by design et by default ont fait leur apparition dans un rapport de 1995 dédié aux « technologies améliorant la confidentialité » préparé par l'Organisation néerlandaise pour la recherche scientifique appliquée, des représentants de l'Autorité de protection des données néerlandaise et la Commissaire à l'Information et la Vie Privée de l'Ontario de l'époque, Madame Ann Cavoukian.
3. CA Versailles, 3ème chambre, 26 octobre 1990 : D. 1991, sommaire p.166 ; Cass 1ère civ. 3 mai 2006, n° 04-20432 : Bull. civ. 2006, I, n° 217 ; Cass. com 11 juillet 2006, n° 04-17.093 ; Cass. com. 19 février 2008, n° 06-17.669 ; Cass. com. 5 octobre 2010, n° 08-11.630 : Jurisdata n° 2010-017800 ; Cass. com 6 décembre 2017, n°16-19615 ; CA Saint Denis 21 février 2018.
4. Cass. com 11 juillet 2006, n° 04-17.093 ; CA Paris, pôle 5 chambre 11, 16 octobre 2015 ; CA d'Aix en Provence 7 juin 2018, n°13/18867.
5. RGPD art. 28 §1.
6. RGPD art. 28 §3 c.
7. Avis 8/2014 sur les récentes évolutions relatives à l'internet des objets, adopté le 16 septembre 2014, p.24.
8. Cass. com., 19 février 2008, n° 06-17669.
9. Cf. en ce sens CA Rouen 21 juin 2018, n° 16/05587.



Faire rimer l'accumulation de données avec le RGPD

Le constat est probant, les entreprises ont de plus en plus recours à des outils logiciels et numériques susceptibles d'utiliser des données personnelles. Un travail de fond est donc nécessaire pour déterminer ce qu'elles détiennent réellement en termes d'informations sur leurs salariés, prospects, clients ou même partenaires. A celui-ci s'ajoute l'inquiétude quant à l'usage réellement opéré par les entreprises et leurs prestataires de ces mêmes données.

Un véritable travail digne de Sisyphe à mesure que se développe l'activité d'une société et qu'elle agrège davantage d'éléments externes. C'est pourquoi, il convient de prendre soin de mobiliser son attention car ces mêmes acteurs sont également soumis aux mêmes obligations et finiront par rendre des comptes aux dirigeants à propos de ce qu'ils font de leurs données personnelles.

Un monde de Big Data et d'IA

Le progrès dépend de l'accumulation de données. Une lapalissade dont les termes introspectifs sont le Big Data et l'intelligence artificielle. Le premier, qui consiste en la captation, le transfert, le stockage et le traitement des données personnelles, dépasse de loin les attentes du marché. Quant à l'intelligence artificielle, elle se présente comme un corollaire naturel indispensable qui permet d'augmenter la puissance des algorithmes.

Ces intelligences artificielles sont de véritables leviers de croissance et réalisent des performances exceptionnelles. Elles permettent d'identifier grâce aux algorithmes de reconnaissance faciale certains éléments ciblés parmi des millions. Des innovations capables de renouveler et dépasser l'existant.

En Chine, par exemple, Alibaba a développé le City Brain dans la ville de Hangzhou (6 millions d'habitants). Les embouteillages ont consécutivement été réduits de 11 %, le nettoyage des rues amélioré, l'attribution des places de parking optimisée et le contrôle de la qualité de l'air ont été renforcés. Fort de ce succès, Alibaba s'apprête à déployer City Brain dans 15 autres villes ainsi qu'en Malaisie. Le modèle utilise les données des autorités publiques et conçoit, en retour, des services pour les usagers. Il s'agit-là d'un échange de bons procédés entre l'Etat, les BATX (les GAFAM chinois) et les citoyens.

Le RGPD se présente comme une sorte de code de la route

L'Europe adopte une position audacieuse

De manière beaucoup plus structurante, le Règlement Européen pour la Protection des Données Personnelles apporte un nouveau cadre juridique et technique pour la préservation de ces éléments. Le règlement se présente comme une sorte de code de la route.

Dans cette optique, le groupement européen d'avocats en droit du travail Ius Laboris a rassemblé des données provenant de 28 pays de l'UE à propos de la façon dont le règlement a été appliqué. Ainsi la Belgique, la Croatie, le Royaume-Uni, la République tchèque, le Danemark, la Finlande, l'Irlande, l'Italie, la Slovaquie, la Slovénie ou bien encore la Suède n'ont pas encore infligé d'amende à quiconque. Cela s'explique principalement par leur relatif retard à implémenter le RGPD dans leur législation ou, pour d'autres, à l'adoption d'une approche plus légère en matière d'application.

A l'inverse, les pays qui ont imposé des amendes au titre du RPGD l'ont généralement fait à une échelle très limitée. Par contre, la France et l'Allemagne ont infligé les amendes les plus lourdes. Outre-Rhin, pas moins de 75 amendes ont été délivrées pour un total de 449 000 euros. Le montant le plus élevé était de 80 000 euros. En France, la Cnil a infligé des contraventions importantes allant jusqu'à plusieurs centaines de milliers d'euros.

Chaque entreprise, quelle que soit sa taille et son domaine d'activité **est donc susceptible de faire l'objet d'une sanction lourde, en termes de montant, d'image ou de valorisation.** Il est donc important pour chacun que ce type d'information fasse l'objet d'une certaine protection. Un travail permanent donc chaque entreprise doit s'emparer.

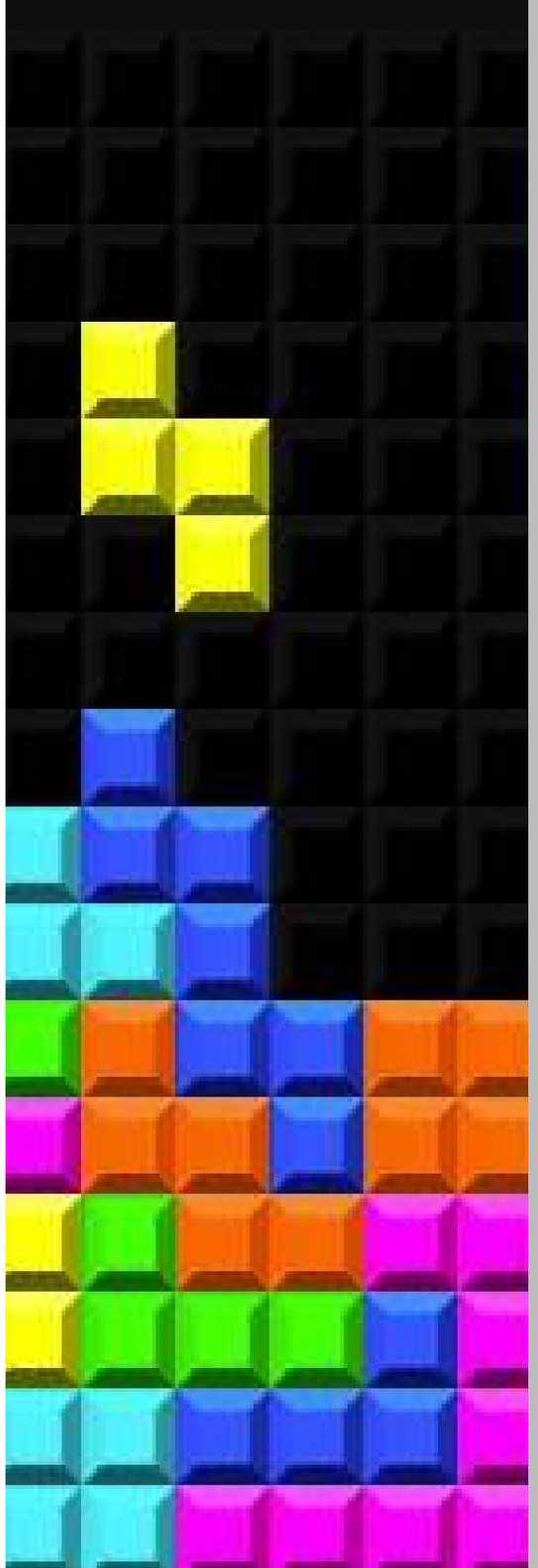
Quelle réponse apporter ?

Pour tout éditeur de logiciel, la problématique du RGPD fait partie de son cœur de métier. Afin de mieux en comprendre les risques réels liés à son activité certains logiciels permettent de guider sa conformité mais également de mener les projets

en mode Privacy by Design. Voire le cas échéant, de mener des PIA (analyses d'impacts).

Parmi les fonctionnalités les plus utilisées par des outils tels que ceux proposés par Data Legal Drive figure la fiche projet Privacy by Design. Cette dernière va justement guider les professionnels dans la mise en œuvre de leurs projets. Grâce à des questionnaires personnalisables et séquencés avec son workflow intégré, ces derniers sont pilotés de manière fluide et sans perte de temps.

Les analyses d'impact s'avèrent donc nécessaires afin de gérer sa propre conformité RGPD. La logique d'accountability fait naître en effet des obligations nouvelles pour chacun. Et il convient de prendre à bras le corps les responsabilités qui sont siennes.



02

IMPLÉMENTER AU MIEUX LE RGPD CHEZ LES PARTENAIRES CLIENTS...

Avis d'experte : Jawaher Allala, CEO Systnaps.

L'impact du RGPD sur le cycle de développement.

Gouvernance des données: les bonnes pratiques à connaître.

AVIS D'EXPERTE

Jawaher Allala

CEO
Systnaps

La mise en conformité RGPD ne peut être un projet one-shot

En quoi être conforme au RGPD constitue une obligation permanente en termes de gouvernance de la donnée ?

La conformité au RGPD est un processus d'amélioration continue. Une entreprise va subir plusieurs crises lors de ses phases de croissance et de développement qui auront un impact sur sa stratégie, sa configuration, sa culture d'entreprise et ses moyens humains et technologiques.

A ceci s'ajoutent les contraintes réglementaires nationales et internationales complexes. Les évolutions de rupture obligent les professionnels à adapter rapidement leurs modèles économiques et leurs stratégies. Les activités opérationnelles sont ainsi de plus en plus externalisées et les processus sont rationalisés et accélérés.

Une entité doit donc s'organiser pour se doter d'un cadre de référence avec lequel ses membres pourront orienter leurs actions en toute confiance. Une confiance qui influencera les activités de l'ensemble et contribuera à justifier son processus de transformation.

Les processus concernant le RGPD sont ceux liés à la mise en œuvre d'un système de management de la protection de la vie privée (SMVP – ISO 27701) et d'un système de management du système d'information (SMSI– ISO 27001). Ils permettent par exemple de mettre en place une gouvernance, des politiques suite à une analyse du contexte interne et externe et de risques liés aux personnes physiques. Ou bien encore de mettre en œuvre des mesures relatives à la vie privée et à la sécurité organisationnelles et techniques ainsi que leur suivi dans le temps.

Les processus dits « de mesure » inclus dans le SMVP et SMSI vont permettre de suivre l'efficacité des processus eux-mêmes, en fournissant la mesure des écarts entre les résultats et les objectifs définis. Ces processus sont au cœur de l'optimisation et la sécurisation des processus et de leurs données personnelles dont la finalité est de limiter les risques pour l'organisation et leurs parties prenantes. L'exploitation de ces mesures permettent l'amélioration continue des processus et des données qu'ils traitent. La mise en conformité RGPD ne peut donc pas être un projet « one shot », si tel était le cas cela impliquerait que l'organisation soit au point mort. Elle n'a pas d'autre choix que de se transformer pour s'adapter aux impacts liés à son écosystème interne et externe.

La solution Regtech « eDatask » a été développée dans un principe d'amélioration continue en tenant compte du contexte de l'organisation et son écosystème avec pour objectif de :

- reprendre facilement et rapidement le contrôle
- faire la preuve de sa conformité réglementaire au-delà du RGPD dans un cadre structuré d'architecture d'entreprise et de normes ISO.

Quels sont les jalons intermédiaires permettant la validation du développement logiciel dans le cadre de sa conformité règlementaire ?

Le « cycle de vie d'un logiciel » correspond à l'ensemble des étapes de développement d'un logiciel, de sa conception à sa fin de vie. L'objectif d'un découpage par étape du cycle de vie permet d'avoir un cadre commun pour l'ensemble des acteurs afin d'y définir lors d'un projet les jalons intermédiaires permettant la validation et la vérification de sa conformité aux besoins exprimés et objectifs fixés.

Le cadre diffère d'une entreprise à l'autre selon la méthode employée (classique ou agile) et du mode d'automatisation et/ou d'implication des acteurs lors des phases de test, de livraison et d'exploitation. Quoi qu'il en soit la mise en conformité doit être vue sur l'ensemble des étapes du cycle de vie de développement et d'exploitation de l'application : planification, conception, développement, tests, release, déploiement et exploitation.

La mise en place d'une procédure de gestion des risques dès la conception d'une application doit être mise en œuvre de façon systématique dès le lancement d'un projet, c'est le premier jalon et l'un des plus important. Les autres étapes du projet restent en suspens tant que celui-ci n'a pas donné le point de départ.

La profondeur de cette analyse de risque diffèrera en fonction des faisceaux d'indicateurs imposant la réalisation ou pas d'une IAPD (Analyse d'Impact relative

à la Protection des Données) impliquant la mise en place d'une sécurité plus adapté au contexte et au niveau de risque détecté.

Le concept de **"Privacy by Design" a pour objectif de garantir que la protection de la vie privée soit intégrée dans l'ensemble des phases de développement de l'application, produits ou services traitant des données à caractère personnel dès leur conception.** A ne pas confondre avec « Privacy by default », qui consiste à permettre à l'utilisateur de l'application, produits ou services de ne pas être obligé d'agir (en cochant des cases par exemple) pour activer sa protection, cette protection doit être activée par défaut.

Le second jalon consiste à lancer le développement dans le cadre défini par l'AIPD par les personnes en charge, du code, des données, des supports, de l'application et de l'infrastructure selon le besoin de sécurité. Une revue de l'analyse de risque est souhaitable à cette étape. Le troisième jalon, quant à lui, permet de tester les fonctionnalités ou *user stories* selon les contraintes imposées par l'AIPD, la robustesse de la sécurité attendue et les fonctionnalités relatives au principe de « privacy by default ».

Le concept de "Privacy by Design" a pour objectif de garantir que la protection de la vie privée soit intégrée dans l'ensemble des phases de développement de l'application, produits ou services traitant des données à caractère personnel dès leur conception.

Le quatrième jalon, également appelé phase de *release*, permet la préparation du package de livraison qui dans son ensemble constitue une sortie applicative. L'objectif, ici est de s'assurer que les éléments liés à la protection des données sont bien intégrés au package sans altération aucune.

Le cinquième jalon est le déploiement. Il consiste à s'assurer que la livraison en production se réalise en toute sécurité, qu'un plan de déploiement a été rédigé et qu'il est mis en œuvre en suivant celui-ci.

Enfin, le sixième et dernier jalon est l'exploitation. Il revient à s'assurer que les mesures de sécurités organisationnelles et techniques sont opérationnelles et vérifiées régulièrement. Cela permet d'identifier les incidents ou violations qui risqueraient d'avoir un impact sur l'application et ses données afin de réagir le plus rapidement pour limiter les risques.

Par la suite en quoi les obligations telles que la mise en œuvre de mesure d'anonymisation, d'archivage, de suppression changent la donne ?

Les données personnelles ne peuvent être conservées de façon indéfinie : une durée de conservation doit donc être déterminée en fonction de l'objectif ayant conduit à la collecte de ces données. Une fois cet objectif atteint, ces données doivent être archivées, supprimées ou anonymisées.

L'anonymisation permet aux organisations de pouvoir utiliser leurs données personnelles en dehors de leur finalité première et de s'affranchir ainsi du RGPD. Par exemple lors de tests ou dans le cas d'une exploitation dans un projet d'intelligence artificielle sans consentement de la personne concernée.

L'archivage et la suppression des données sont également liées à la finalité des données. Dès que celle-ci est atteinte, les informations devront être archivées ou supprimées selon le sort final qui leur sera assigné par le référentiel de durée de conservation.

Dorénavant, **les consommateurs de données de toute sorte appartenant à l'organisation ou à son écosystème devront utiliser la donnée dans le respect des droits de la personne concernée.** L'usage est limité dans le temps et le transfert est encadré juridiquement en fonction de la finalité du traitement et du fondement qui la supporte.

La maîtrise et la gestion automatisée des données au sein de l'organisation dans une démarche d'amélioration continue via une solution logicielle tel que Systnaps est plus que nécessaire du fait que celle-ci se joue maintenant au niveau de la personne physique. Une connaissance de son patrimoine informationnel et du parcours de la personne qu'elle soit physique ou morale sont les moteurs de l'économie du 21ème siècle.

Comment prendre en considération la gestion du risque. Les actifs de données d'une organisation peuvent-ils rapidement devenir un passif ?

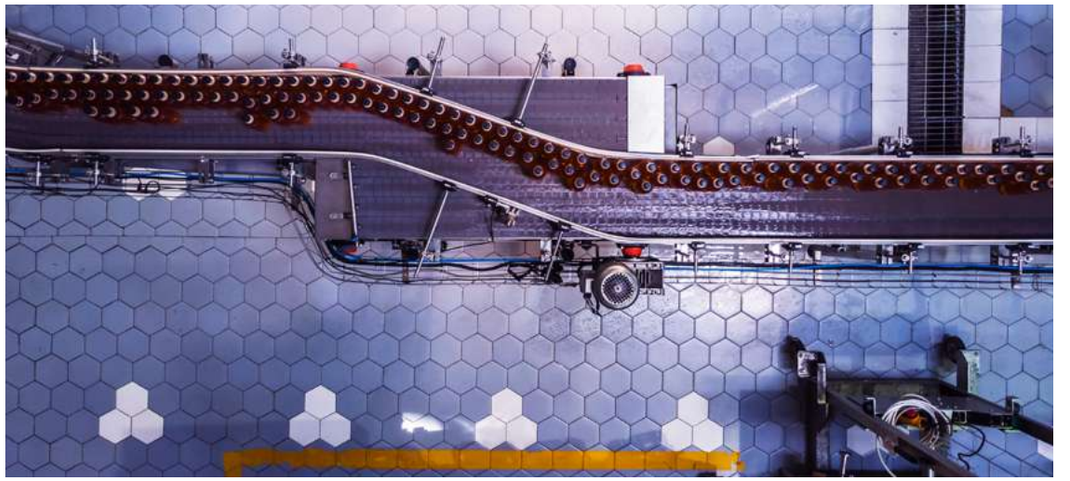
Les principaux risques qui peuvent affecter les données d'une organisation sont l'absence d'organisation et de compétences permettant d'aligner la connaissance des données, la stratégie et les opérations de l'entreprise. A ceci, il convient d'ajouter l'insuffisance du dispositif de contrôle interne permettant d'assurer la protection des données (non-altération) et le respect des réglementations ou bien encore les risques de pertes et de fuites de données (vol, fuite involontaire, intrusion, sabotage…).

Ces risques peuvent être lourds de conséquences comme la perte de réputation et d'image, le blocage des systèmes, la perte de maîtrise du système... Ils impliquent un coût financier et une baisse du chiffre d'affaire.

La gestion du risque est le garde-fou de la mise en conformité, elle permet de dimensionner le niveau de sécurité à mettre en place et de réagir rapidement en cas de défaillance.

L'impact du RGPD sur le cycle de développement

Etablir une bonne gouvernance des données depuis la collecte jusqu'à leur destruction



« La mise en place d'une gouvernance consiste en premier lieu à considérer les données manipulées par l'entreprise et son écosystème comme un actif stratégique »

Jawaher Allala, CEO de Systnaps

Afin de comprendre la manière d'intégrer les éléments relatifs au RGPD au sein des outils logiciels, il est opportun de rappeler ce sur quoi reposent les traitements de données personnelles. A la manière de la formule de Nicolas Boileau énonçant que ce qui est correctement conçu peut s'énoncer clairement, le développement logiciel prend en compte le volet du traitement de données personnelles. Cette opération, ou plutôt cet ensemble d'opérations, porte sur des datas sans considération du procédé utilisé : collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication...

Il s'agit donc véritablement d'une notion délibérément large impliquant un traitement et une finalité déterminée préalablement au recueil des données et à leur exploitation. Aussi, tout traitement de datas doit être licite dans la mesure où il se doit de reposer sur l'une des six bases légales autorisées par le RGPD. Entrent ainsi en considération des éléments tels que l'obtention du consentement préalable de la personne, l'exécution d'un contrat conclu avec elle, l'accomplissement d'une mission d'intérêt public, le respect d'une obligation légale qui impose le traitement de ces données, etc...

Autant d'éléments devant être intégrés au sein de logiciels destinés à être utilisés par les professionnels. Dans ce cadre, il convient de prendre en compte ces nouvelles obligations tout en assurant qu'ils conservent un caractère innovant. A la lumière de la maxime de Lawrence Lessig devenue célèbre, « Code is law », la technique fait office d'outil de régulation. La régulation par la technologie peut ainsi s'accompagner d'une régulation par le design. Cela se concrétise par des considérations relatives à la conception d'un produit, ses interfaces, les expériences qui y sont jointes, l'ergonomie...

Il devient ainsi utile d'adopter de bonnes pratiques afin de mettre en place une gouvernance des données stables dans le temps. Une position que soutient Jawaher Allala, CEO de Systnaps : " *La mise en place d'une gouvernance consiste en premier lieu à considérer les données manipulées par l'entreprise et son écosystème comme un actif stratégique, et à ce titre assurer leur gestion comme telle. Les valeurs importantes s'avèrent être l'acquisition, la collecte, la responsabilité, la standardisation, la facilitation de l'accès, la diffusion, la réutilisation, le partage, l'archivage et la destruction sécurisée pour en maximiser la valeur*".

Pour mettre en place une gouvernance stable des données dans le temps, il est primordial de se réapproprier, puis de maintenir la cartographie des données de son organisation afin d'identifier ses données et de les gérer comme un actif stratégique. Il s'agit donc de mettre en conformité ses données avec l'ensemble des exigences réglementaires (RGPD, NIS, ePrivacy, solvency III...) tout en sécurisant ses données via la classification de celles-ci selon leur niveau de sensibilité.

Le Data Lifecycle Management pour établir une bonne gouvernance des données

Parmi les moyens permettant d'établir une bonne gouvernance des données et de bâtir des outils idoines, figurent les logiques de Data Lifecycle Management (DLM). Autant de règles qui aident les entreprises à se conformer aux textes réglementaires tels que le RGPD. Une stratégie DLM efficace vise par exemple à assurer une redondance de sorte que les données soient en sécurité en cas d'urgence. Elle contribue également à éviter que les données clients soient dupliquées dans différents endroits de l'infrastructure dans un souci évident de sécurité.

Ainsi, les données utiles sont propres, exactes et directement accessibles aux utilisateurs. L'automatisation facilite ce processus, dont l'ensemble aidera l'entreprise à gagner en agilité et en efficacité. Il s'agit-là véritablement d'un investissement essentiel dans l'élaboration d'une approche de gestion du risque pour assurer la conformité permanente d'une entreprise.

Une telle stratégie permet inévitablement à une entreprise de dégager des avantages concurrentiels. Jawaher Allala, précise : "*Une bonne gouvernance des données est devenue incontournable afin de s'aligner au business et d'en rationaliser les processus opérationnels depuis la prospection jusqu'à la fin des relations contractuelles. Ce qui correspond selon le point de vue du cycle de vie de la donnée aux processus de collecte jusqu'à ceux de sa destruction* ".

Start-ups, PME-ETI, grands comptes : une maturité différente

Cependant, force est de constater que la mise en œuvre de ces éléments n'est en rien triviale. Il est même possible de dresser un constat en termes de maturité du secteur en fonction de la typologie des sociétés. A l'heure actuelle, nombre de start-ups ne disposent pas d'une vision résolument précise quant à la validation de leur modèle économique basé sur des données personnelles. Ils n'intègrent donc que peu, voire pas, la notion de « privacy by design/by default » imposée par le RGPD dans le cycle de vie de leur développement. La priorité est donnée à leur projet et au financement de celui-ci. Cela dit, ils s'interrogent et s'inquiètent de l'impact que pourrait avoir le réglementaire sur leur business. L'un des freins considérable qu'ils rencontrent est l'accès ardu aux données dû à la complexité administrative et réglementaire ainsi qu'à la culture du secret que certaines organisations françaises cultivent. C'est pourquoi, dans cette optique la Cnil a publié un guide spécifiquement destiné aux développeurs. Il permet de les accompagner dans la mise en conformité de leurs travaux.

De leur côté, les PME et ETI, dont des éditeurs de logiciels, découvrent le RGPD par leurs clients sont incités à se mettre en conformité pour assurer leur propre conformité. Ces structures, qui ont toujours fonctionné en mode agile, ont pris connaissance des nouvelles responsabilités qui leur incombent. Ils doivent ainsi prendre des mesures de sécurité organisationnelles et techniques dont la mise en œuvre doit être rapide au vu de la pression liée à la perte d'une nouvelle affaire ou de leur portefeuille clients.

Enfin, les grandes organisations font face à une problématique de complexité selon leur taille. A ceci s'ajoute le fait que leur écosystème (dans une logique d'externalisation) doit également suivre ces mêmes préconisations.

Le constat est donc évident. Là où la donnée est le pétrole de demain, la mise en conformité constitue indéniablement un nouveau moteur qui permettra à l'organisation de continuer l'extraction afin de valoriser ses données ou celle de son client.

Cnil : un rôle majeur en termes de suivi

Dans ce concert, le "gendarme des données" que constitue la Cnil dispose d'un rôle non-négligeable. L'organisation insiste sur le fait que la nouvelle réglementation est un facteur permettant aux professionnels de se développer. Et aux éditeurs de promouvoir de nouveaux services innovants.

Sophie Nerbonne, Directrice chargée de co-régulation économique au sein de la Cnil explique : " *Le RGPD consiste à créer un cadre de confiance. Son ADN est de renforcer la maîtrise et le contrôle que les individus peuvent avoir sur la collecte et le traitement de leurs données personnelles. Il permet d'avoir de la compétitivité dans le sens où cette chaîne va valoir pour les clients, les prospects et les partenaires commerciaux c'est-à-dire toute la chaîne de valeur. Le RGPD par le fait des droits qu'il confère comme le droit à la portabilité par exemple est un facteur d'innovation pour le déploiement de nouveaux services ou de nouveaux produits*". Dans une optique de co-construction, la Cnil édite de nouveaux outils de de conformité, tout comme des moyens de certifier les bonnes pratiques. Ces ensembles permettent d'édifier des codes de conduite professionnels par branche afin de dégager les meilleurs moyens de demeurer en conformité avec les textes

A terme, la Cnil devrait conserver un positionnement bienveillant sur les entreprises et éditeurs qui font montre d'avancements réels sur le sujet de l'intégration et des conséquences du RGPD sur les process et les responsabilités de chacun. Elle doit toutefois faire preuve de davantage de visibilité quant aux évolutions prochaines de la réglementation ou de la jurisprudence et des implications qu'elles entraînent.

Gouvernance des données: les bonnes pratiques à connaître.

- Définir, communiquer et piloter l'exécution de la stratégie de données et la gouvernance des données.
- Établir et appliquer des politiques relatives à la gestion, à l'accès, à l'utilisation, à la sécurité et à la qualité des données et des métadonnées.
- Définir et appliquer des normes de qualité des données et d'architecture de données.
- Fournir des observations pratiques, des vérifications et des corrections dans les domaines clés de la qualité, des politiques et de la gestion des données.
- S'assurer que l'organisation peut satisfaire aux exigences de conformité réglementaire liées aux données.
- Identifier, définir, transmettre et résoudre les incidents liés à la sécurité des données, à l'accès aux données, à la qualité des données, à la conformité réglementaire, à la propriété des données, aux politiques, normes, terminologie ou procédures de gouvernance des données.
- Etablir des normes et des processus pour définir de façon cohérente la valeur opérationnelle des actifs de données.

03

LES SOLUTIONS TECHNOLOGIQUES **PERTINENTES.**

Un levier pour innover.

Avis d'experte, Chloé Rousselet, Data Protection Officer Cegid.

Infographie : Optimiser le traitement des données grâce au Machine Learning.

Privacy by Design vs Privacy by Default.

Un levier pour innover

Dans l'optique de poursuivre l'implémentation du RGPD auprès des partenaires et des utilisateurs, de nombreux outils existent. Ces derniers constituent une ossature technologique forte en mesure d'épauler les professionnels dans leur démarche d'observance des règles relatives au RGPD.

Historiquement, les responsables de traitement se sont tournés vers les éditeurs afin de répondre à leurs questionnements. Mais surtout à leurs obligations réglementaires. Ils y ont trouvé des réponses au moyen de démarches pédagogiques claires. A présent, éditeurs et entreprises en cours de transformation numérique se doivent d'aborder des problématiques précises tel que la gestion des principes dits de Privacy by design ou de Privacy by default. Des concepts bien connus de la sphère de la sécurité informatique, mais qui dépassent désormais leur cadre strict.

La question est véritablement prégnante. A l'heure actuelle, peu d'éditeurs témoignent de ce qui relève ou non de ces deux concepts majeurs du Règlement général sur la protection des données. C'est pourquoi, il est important que les éditeurs puissent disposer de l'ensemble de l'expérience nécessaire pour adopter des démarches prospectives en termes de besoin de gestion des données personnelles. Un sujet sur lequel certains professionnels comme Cegid ou bien encore Coheris ont d'ores-et-déjà pris une avance certaine.

Éditeurs et entreprises en cours de transformation numérique doivent aborder la gestion des principes dits de Privacy by design ou de Privacy by default

Il est donc évident que le RGPD constitue un véritable moyen d'opérer un levier pour encourager l'innovation. C'est dans ce contexte que nombre d'entre eux entreprennent de développer de concert respect de la réglementation et innovation. C'est notamment possible grâce aux méthodes utilisant l'intelligence artificielle afin de les intégrer au sein d'**outils complexes tels que les ERP ou les CRM**. Une véritable marche en avant dont l'optique est de réduire les irritants pour l'ensemble des professionnels et de conduire à constituer des relais de croissance notables pour les éditeurs.

AVIS D'EXPERTE

Chloé Rousselet

Data Protection Officer CEGID

Il faut faire attention aux déclarations de "conformité RGPD totale" : la réalité est plus complexe pour les éditeurs

Quelles sont les garanties et les éventuelles limites du privacy by design, qui se trouve au coeur du RGPD ?

Il faut d'abord rappeler que le RGPD concerne tous les métiers - expertise comptable, fiscalité, paie, RH, retail... - la gestion des données personnelles y étant plus ou moins centrale.

Certes, l'approche privacy by design vise à garantir la conformité des traitements de ces données personnelles en prenant en compte dès la conception et par défaut dans les projets les principes de protection des données personnelles issus du RGPD. **Mais contrairement aux idées reçues, le RGPD ne fait pas référence à la conformité du logiciel.**

En réalité, le client - qui est très souvent un responsable de traitement - garde deux responsabilités importantes : le choix de son logiciel, d'une part, et l'utilisation qu'il en fait dans son contexte métier, d'autre part. C'est cet ensemble qui va l'engager vis-à-vis du RGPD.

Par exemple, dans une PME, un système manuel de suppression des données peut très bien convenir. Mais ce même système, peu adapté aux processus d'une grande entreprise, pourrait finalement l'exposer à un risque de non-respect du RGPD.

Il est donc impératif, pour un client, de faire sa propre analyse des risques. Puis, sur cette base, d'associer les bons logiciels avec les bons processus, c'est-à-dire d'adopter une approche duale.

L'importance de cette approche duale «choix du logiciel et gestion des processus» est-elle bien comprise par les clients ?

Les premiers mois, cette double approche était difficile à expliquer car certains responsables de traitement pensaient qu'une solution clé en main saurait régler tous les problèmes « par conception ».

Un client doit faire sa propre analyse des risques, puis sur cette base, associer les bons logiciels avec les bons processus.

Dans un deuxième temps, après quelques déconvenues, ils se sont tournés vers les éditeurs pour obtenir des réponses aux nombreuses questions qui ont surgi. D'où l'ouverture d'une période d'accompagnement et de pédagogie qui s'est globalement bien passée. Pourtant, pendant de nombreuses années, c'était plutôt la méfiance qui prévalait dans la relation d'externalisation, en particulier envers les éditeurs en SaaS.

Quelle est l'approche de Cegid en matière de privacy by design ?

Pour un éditeur, la priorité est d'intégrer le principe même du privacy by design. La demande émane généralement des clients, lesquels attendent une démarche forte. Cegid a donc travaillé sur les aspects juridiques, d'une part, et sur l'implémentation du privacy by design, d'autre part. **Cette création de fonctions dites privacy by design, ou by redesign pour les offres legacy. Ne pouvant s'appuyer sur des directives précises de la Cnil, nous avons dû faire des choix a priori pertinents pour nos clients.**

Un plan de développement commun à l'ensemble de nos offres a donc vu le jour fin 2017, grâce au travail de l'équipe projet pluridisciplinaire RGPD de Cegid. L'équipe a déroulé une à une les exigences des responsables de traitement, en vue d'y associer une fonctionnalité. Les équipes de développement ont ensuite intégré ces propositions dans leurs roadmaps respectives, en les adaptant à leur contexte d'utilisation - une offre RH n'ayant pas les mêmes contraintes RGPD qu'une offre de gestion des stocks.

Pour prendre l'exemple de notre offre retail, nous y avons intégré des fonctions de gestion de la fidélité client. Et cela en anticipant les besoins de nos clients responsables de traitement puisque, en octobre 2017, nous ne disposions pas d'un recul ou de retours clients suffisants. Notre objectif est désormais de mesurer comment cette offre aide effectivement nos clients à répondre à leurs obligations RGPD.

La responsabilité financière de l'éditeur peut-elle être engagée en cas de manquement au RGPD ?

Aujourd'hui, le recul juridique est insuffisant pour affirmer qu'une telle responsabilité de l'éditeur a été clairement établie. Nous ne pouvons donc faire que des hypothèses, en distinguant le cas d'une licence On Premise, mettant à dis-

position un logiciel avec installation en local chez nos clients, et celui du SaaS, mettant à disposition de nos clients un logiciel déjà hébergé.

Dans le cas d'une licence On Premise sans service associé, il n'y a pas de relation de sous-traitance au sens du RGPD. En effet, la donnée ne transite pas chez l'éditeur et le RGPD ne s'applique donc pas. Prenons ce cas de figure : une amende de la Cnil est prononcée à l'encontre d'un client responsable de traitement, suite à la diffusion de données personnelles, celle-ci résultant d'une faille de sécurité logicielle. La Commission pourrait estimer ainsi que le responsable de traitement n'a pas mis en œuvre toutes les mesures nécessaires pour empêcher cette fuite de données. Quant à l'éditeur, il ne serait pas sanctionné par la Cnil, sur le fondement du RGPD, puisqu'il n'est pas sous-traitant. Nous pourrions envisager que le client puisse se retourner contre son éditeur, mais en invoquant une autre base légale que le RGPD.

Dans le cas du SaaS, une relation de sous-traitance, au sens du RGPD, est établie. **L'éditeur endosse donc les responsabilités qui y sont liées.** Imaginons cet autre cas : une personne physique fait une demande de réparation de préjudice, suite à une fuite de données. Si la responsabilité de l'éditeur est établie dans ce manquement de sécurité, le client sera exonéré - mais sous réserve qu'il prouve bien que le dommage ne lui est nullement imputable. Dans un tel cadre, le client pourrait demander une intervention forcée de l'éditeur au cours de la procédure.

En résumé, dans le cadre général défini par le RGPD, c'est le responsable du traitement qui est - par défaut - responsable de tout dommage. Sauf s'il parvient à prouver que ce dommage ne lui est pas imputable. La responsabilité du sous-traitant pourra être engagée s'il est avéré qu'il a fait preuve de manquements aux obligations spécifiques qui incombent à un sous-traitant.

Quant aux éditeurs SaaS, ils sont certes plus exposés mais ils ont aussi une opportunité de se différencier en proposant des fonctions RGPD très utiles à leurs clients.

Des questions liées au Cloud Act aux Etats-Unis restent également posées. Le texte est, par nature, contraire au RGPD dans l'Union Européenne.

Les discours autour d'une « totale conformité » avec le RGPD sont-ils bénéfiques pour le marché ?

Pas vraiment ! De façon générale, en matière de sécurité informatique, il est quasiment impossible de prendre des engagements de résultat, puisque la sécurité à 100 % n'existe pas. Ce qui soulève un point important de responsabilité et de garantie. Le même raisonnement s'applique en matière de conformité au RGPD : il faut donc faire attention aux déclarations de « conformité RGPD totale » car sa mise en oeuvre est complexe pour les éditeurs.

Attention, donc, à toute forme de surenchère portant sur la conformité ou sur la garantie de sécurité : les éditeurs doivent résister à cette tentation car elle aurait des conséquences sur l'ensemble de la chaîne, au moment où nous avons peu de recul juridique. Et à ce jour, peu d'annonces ont été faites sur d'éventuels travaux en collaboration avec la Commission sur ce sujet. Donc prudence.

La Cnil a adopté une démarche de sensibilisation, tout en prononçant des amendes. Cette double approche va-t-elle se prolonger ?

La Cnil poursuit effectivement une double stratégie de sensibilisation et de sanction. À ce jour, les amendes ont souvent été prononcées à l'encontre de sociétés ayant laissé passer des failles de sécurité importantes ou ayant agi de mauvaise foi. Pour les autres entreprises fautives, c'est l'approche de pédagogie et de sensibilisation qui a été préférée - sans qu'on puisse prédire la durée de cette double stratégie.

Dans le même esprit, la Cnil sensibilise sur les thématiques de la gouvernance des données et des processus. Mais des doutes persistent sur certains points comme la durée de conservation* des données, par exemple : les éditeurs disent encore manquer de visibilité. Des efforts de pédagogie restent donc nécessaires.

A l'avenir, comment les éditeurs vont-ils se positionner par rapport au RGPD ?

Il n'y a pas de consensus, aujourd'hui, chez les éditeurs. Et pour cause : sur la question de la responsabilité du sous-traitant, notamment, des doutes persistent dans l'interprétation des textes de la Cnil.

D'autres ambiguïtés concernent ce qui relève du cloud public et du cloud privé. Par exemple, en matière de cloud public, la Cnil avait indiqué il y a plusieurs années que l'éditeur pourrait ne pas être assimilé à un sous-traitant mais se verrait plutôt qualifié de responsable conjoint. Cela soulève des interrogations chez les éditeurs, qui les empêchent de se positionner durablement.

De plus, des questions liées au Cloud Act aux Etats-Unis restent également posées. Le texte est, par nature, contraire au RGPD dans l'Union Européenne. Mais en termes d'application de la réglementation, rien n'est encore tranché. Le rapport Gauvain a été remis au premier Ministre dans le courant de l'année 2019 et propose plusieurs pistes de réflexions pour renforcer la protection des entreprises contre les lois extraterritoriales au niveau de la France et de l'Europe. On comprend donc que la position des éditeurs soit encore appelée à évoluer, en particulier au fil de la jurisprudence. Pour sa part, Cegid va maintenir des relations fortes avec la Cnil et avec ses clients, dans une approche de co-construction et d'amélioration continue.

* La Cnil publie des lignes directrices concernant les durées de conservation. Elaborées en juillet 2020, elles ont été rédigées avec le Service interministériel des archives de France (SIAF)

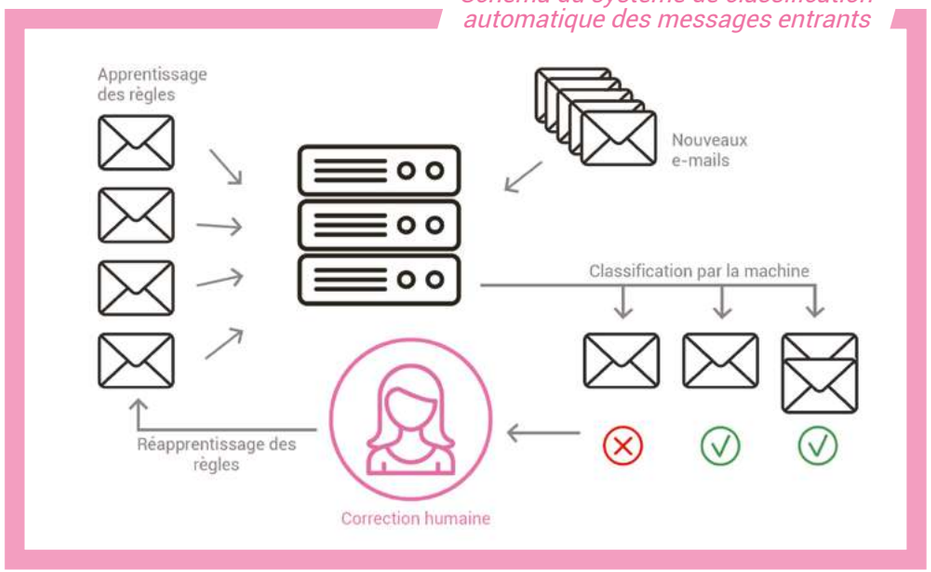
Optimiser le traitement des données grâce au Machine Learning.

Le RGDP constitue un bon moyen de mêler respect de la réglementation et innovation. Nombre de process peuvent et doivent être automatisés afin de libérer les collaborateurs de tâches rébarbatives. Il est, par exemple, possible d'optimiser le traitement des messages entrants grâce au Text Mining et au Machine Learning.

Son fonctionnement est plutôt simple. Une machine va recevoir les premiers messages préalablement catégorisés, lui permettant ainsi d'apprendre les règles de catégorisation. Puis, dès l'entrée de nouveaux messages, la machine est en mesure de classer elle-même les messages entrants. En cas d'erreur, une intervention humaine peut corriger la machine.

Le Machine Learning permet donc de véritablement cartographier les données sensibles autour de glossaires spécialisés enrichis autorisant les moteurs à s'approprier les mots spécifiques à une entreprise. L'analyse sémantique permet ainsi d'interdire la saisie de termes prohibés dans les champs texte ou les zones de commentaire des applications d'entreprise de type CRM ou ERP. Ce qui évitera l'enregistrement d'informations contraires au RGPD.

Schéma du système de classification automatique des messages entrants



Privacy by default vs by design : Les best practices

Privacy by default

Fermer, par défaut, une application. Les accès ne sont ainsi ouverts qu'en fonction des profils. Les droits sont donc progressivement ouverts aux utilisateurs.

Pseudonymiser les données. Ces mesures empêchent d'**associer des données à une personne physique précise** sans avoir recours à des informations supplémentaires.

Chiffrer les datas par le biais de moyens cryptographiques. Ces derniers vont permettre d'apporter une garantie en termes de confidentialité.

Minimiser les données. Les services professionnels ne peuvent **utiliser que les informations dont ils ont besoin, pertinentes et nécessaires pour leur activité**.

Mettre en avant les droits d'information en donnant la possibilité à l'utilisateur d'accéder à la politique de confidentialité, au registre de traitement ou le mode opératoire pour qu'il puisse les obtenir.

Permettre à l'utilisateur de **télécharger ses données dans un format structuré**, couramment utilisé et lisible. Un formulaire peut être mis à disposition pour rationaliser les demandes.

Rendre possible l'effacement des données qui prendra en compte les droits de la personne concernée et les durées de conservation.

Mettre en place des procédures de gestion de crise afin d'effectuer rapidement les actions nécessaires à la protection des informations des personnes concernées (exemple : bloquer le compte et imposer le changement du mot de passe après authentification).

Aller plus loin

La Cnil édite ses propres recommandations. Disponibles sur son site.

Privacy by design

Inclure une note d'information RGPD à la connexion qui s'affiche lorsqu'un utilisateur se connecte. La fonctionnalité indique les zones libres dans lesquelles il ne faut pas saisir de données personnelles.

Permettre l'exercice des droits des personnes. Possibilité de modifier/supprimer un champ, export en CSV par un profil particulier ou par l'utilisateur.

Notifier une **rectification ou un effacement par e-mail** suite à l'exercice du droit des personnes.

Développer un menu déroulant proposant les justifications du traitement effectué suivant la/les finalités du produit.

Disposer d'un module de log pour renforcer la traçabilité des accès et actions sur les données personnelles. Cela fournit une traçabilité (logs exportables, lisibles et purgeables).

Proposer un outil à même de gérer la durée de conservation des données suivant leur nature. Les durées de conservation doivent être déterminées par le responsable de traitement (un bulletin de salaire est conservé 5 ans en France).

Minimiser les données : ne disposer que de champs stockant **des données personnelles strictement nécessaires pour les finalités du produit.** S'il y a un doute sur la nécessité du champ, laisser la possibilité pour le responsable de traitement de supprimer ce champ.

Mettre en place un outil de gestion du consentement : si les finalités du produit nécessitent un consentement et que les personnes concernées ont un accès à ce produit, permettre au responsable de traitement de collecter ce consentement via le produit avec horodatage.

Mettre sur pied un outil de la gestion de l'information : proposer un outil permettant de pousser une information (par email, pop-up…) pour répondre à l'exigence d'information de l'article 13 du RGPD.

04

RETOURS D'EXPÉRIENCES CONFORMITÉ RGPD.

EasyVista

Renault

CHU de Lille

Groupe Matmut

BNP Paribas

Saint-Gobain

RETOUR D'EXPERIENCE

easyVISTA™

" Etant employeur, client et fournisseur, Easyvista s'est projeté sur trois perspectives pour la mise en conformité "

Avant même l'entrée en vigueur du RGPD, EasyVista était sensibilisé à la gestion des données personnelles, notamment pour le compte de ses clients. En effet nous sommes audités chaque année depuis 2017 par un organisme qui valide notre conformité par rapport aux exigences de l'audit SSAE 18 - SOC2. Il permet une vérification de l'implémentation de processus liés à la sécurité de l'information de nos clients, notamment des données personnelles des utilisateurs.

Le RGPD a ajouté de nouvelles obligations et de nouvelles exigences. Nous avons donc lancé un chantier RGPD pour toute l'entreprise. **Nous nous sommes projetés sur trois perspectives pour la mise en conformité, étant à la fois employeur, client et fournisseur**. Sur chacun de ces axes, le premier défi a été de définir les priorités pour élaborer des plans d'actions. En outre, EasyVista étant implanté dans six pays européens, et l'Amérique du Nord (Canada et Etats-Unis), nous avons dû intégrer dès le départ une dimension internationale. De plus, il n'existe aucune solution clé en main pour la mise en conformité.

Nous avons été accompagnés au départ par une avocate spécialisée pour les entreprises IT et nous nous sommes appuyés sur les supports mis à disposition par la Cnil. L'autorité de contrôle propose des articles répondant aux questions essentielles que l'on peut se poser au sujet du RGPD, mais aussi un référentiel de documents de bonnes pratiques, et des modèles de

documents (registre de traitement, analyse d'impact). Les premières priorités (2018) Un groupe de travail a été constitué dès le mois d'Avril 2018 réunissant des compétences complémentaires : le RSSI dédié aux architectures clients SaaS, le Directeur Administratif et Financier, une avocate spécialisée en droit des NTIC ainsi qu'un Data Gouvernance Manager recruté notamment pour ce projet.

Nos premières priorités ont été le marketing, les contrats des clients existants et les données personnelles de nos collaborateurs. Concernant le marketing, les données personnelles de prospects sont récoltées via des formulaires sur notre site web public, ou via l'inscription à des évènements (salons informatiques) auxquels EasyVista participe. Nous avons apporté les modifications nécessaires pour **mettre en conformité nos supports de collecte de données, c'est-à-dire recueillir le consentement des visiteurs de notre site, préciser la finalité du traitement des données et vérifier les durées de conservation**. Cette mise en conformité a nécessité un travail conjoint avec le marketing groupe, et a conduit à une refonte significative de nos méthodes e-marketing.

Nous avons également adapté et mis en ligne notre Politique sur les données à caractère personnel et le respect de la vie privée, qui concerne les données collectées dans le cadre des ventes et du marketing, de la livraison du logiciel, de la réalisation des services associés, et de la gestion administrative.

Concernant les contrats des clients existants, certains se sont rapprochés de nous pour veiller à la bonne application de l'article 28 du RGPD par EasyVista en tant que sous-traitant. Cela s'est traduit notamment par **la signature conjointe d'un DPA (Data Privacy Agreement, Accord sur la Confidentialité des Données)** annexé au contrat principal pour une quarantaine de clients. Dans ce document, nous rappelons les obligations de chaque partie, notamment par rapport aux mesures techniques et organisationnelles à prendre, à la notification aux autorités en cas de violation de données personnelles et aux droits d'une personne physique (Articles 16 à 20 du RGPD).

Les données personnelles de nos collaborateurs ont également fait l'objet d'une attention particulière, car la société détient des informations liées à la famille du collaborateur, son numéro d'identification national, ses fiches de paye, ses données géographiques (adresse du domicile). Nous avons donc émis d'une note à tous les salariés rappelant les obligations de la société vis-à-vis de leurs données personnelles. Les registres de traitement des applications informatiques et autres supports ont été rédigés, et ils sont accessibles par les salariés sur demande. Il leur est aussi rappelé dans cette note qu'ils s'engagent à respecter la Charte IT de l'entreprise, qui traite la sécurité et les bonnes pratiques à mettre en œuvre au quotidien. Comme prévu au règlement, nous avons formalisé une formation de sensibilisation à la sécurité informatique dont les premières sessions sont intervenues dès mi-2018. Un chantier permanent (2019).

Pour libérer nos commerciaux des tâches administratives liées au RGPD, nous avons renforcé notre équipe de travail par une présence juridique accrue.

Même après avoir traité ces premières priorités, il demeure un travail continu à effectuer. Nous traitons régulièrement des demandes de signature d'annexes RGPD provenant de nos clients et prospects français et d'autres pays. **En plus de ces annexes, les prospects ont des questions toujours plus approfondies et demandent des preuves détaillées.** Le travail effectué pour remplir les réponses aux appels d'offre est minutieux et peut mobiliser des collaborateurs de plusieurs services.

Il en est de même des clients existants, lorsqu'il s'agit de renouveler ou modifier un contrat. Afin de centraliser toutes ces demandes et libérer nos commerciaux des tâches administratives liées au RGPD et leur permettre de se concentrer sur le business, nous avons renforcé notre équipe de travail par une présence juridique accrue au sein de l'entreprise en 2019.

Nous avons également dû adapter nos outils de gestion de la gouvernance pour la conformité RGPD, en adoptant l'application DataLegalDrive permettant notamment d'établir des registres de traitement, suivre les signatures de DPA avec nos clients et nos fournisseurs, suivre le taux de collaborateurs ayant suivi la formation de sécurité informatique que nous organisons régulièrement, répertorier les audits effectués au sein du groupe, et classer tout document lié au RGPD.

En parallèle du travail continu du RGPD, il faut également intégrer l'évolution. L'adoption de DataLegalDrive devra être faite au niveau international, avec la constitution de groupes de travail par pays.

Pour notre système d'information interne, des tests devront être effectués pour vérifier la robustesse de nos procédures de sécurité. Des tests d'intrusion peuvent être faits sur les applications les plus sensibles. Enfin, EasyVista étant implantée dans des pays hors Union Européenne, nous allons mettre en place des BCR (Binding Corporate Rules) selon les exigences listées à l'article 47 du RGPD. Les BCR permettent d'éviter de conclure autant de contrats qu'il existe de transferts au sein du groupe EasyVista, d'uniformiser les pratiques liées à la protection des données personnelles, et de placer la protection des données au rang des préoccupations éthiques de l'ensemble du groupe.

Nous pouvons conclure de nos échanges avec nos clients et fournisseurs, ainsi que des démarches que nous faisons nous-mêmes, que la protection des données personnelles fait partie des préoccupations principales des entreprises, au même titre que les problématiques liées à la stratégie RSE.

EasyVista

Membre du Cigref

RETOUR D'EXPERIENCE

RENAULT

" En réalité, nous avons connu peu d'incidents de sécurité "

Pour le Groupe RENAULT, en ne comptant que les traitements gérés au niveau Corporate, nous avons eu à vérifier la conformité de près d'un millier de traitements, impliquant plusieurs centaines de fournisseurs et partenaires.

Les points qui ressortent du travail avec ces partenaires :

- Une grande disparité dans la réactivité ; certains nous ont spontanément proposé une nouvelle version des clauses contractuelles dès l'entrée voire même avant l'entrée en vigueur du RGPD, d'autres ont accepté en l'état nos clauses sans les négocier, alors qu'avec d'autres le dossier n'est pas encore abouti.
- La difficulté dans certains cas à établir le partage des responsabilités ; la notion de co-responsable de traitement vs responsable indépendant vs sous-traitant n'est pas encore complètement maîtrisée.
- En cas de modifications à apporter aux traitements, les grands fournisseurs l'ont fait sans problème majeur, mais pour les petits cela a pu représenter un surcoût difficile à absorber.

Nous notons aussi au bilan que nos anticipations n'ont pas toujours été vérifiées : ainsi, **nous nous attendions à avoir régulièrement des incidents de sécurité**, et dans la réalité il y en a peu ; en revanche, nous n'avions pas prévu l'explosion des demandes d'exercice des droits de la part de nos clients, et l'organisation pour y répondre a nécessité un supplément de travail et de ressources.

Par Bruno Lalande, Expert Data, Records & Knowledge Management, Groupe Renault, Protection & Security Dept

RETOUR D'EXPERIENCE

CHU LILLE

" Se mettre en ordre de bataille pour obtenir une conformité RGPD de notre propre entrepôt de données "

Les services publics, en particulier les hôpitaux ont dû rapidement se plier aux obligations inhérentes aux règles du RGPD. Le CHU de Lille a ainsi été l'un de premiers à mettre en place les mesures adéquates.

« *Le RGPD renforce le principe de transparence et de traçabilité dans le traitement des données personnelles. L'engagement de la direction et de la Commission Médicale d'Etablissement, l'implication des porteurs du projet et l'accompagnement éclairé de la Cnil nous ont permis de définir un cadre organisationnel et sécuritaire cohérent avec le RGPD et nos valeurs éthiques basées sur le consentement explicite des patients* », explique Guillaume Deraedt, Data Protection Officer au CHU de Lille.

Voilà comment le complexe s'est mis en ordre de bataille dans l'optique d'obtenir une véritable conformité RGPD destinée à être appliquée à son propre entrepôt de données. La Cnil a en effet validé cette évolution de la réglementation afin de préserver la sécurité des installations et services du CHU en termes de sécurité et de protection des données du patient.

Dans ce cadre, l'**organisme a entrepris de bâtir un véritable entrepôt de données de santé dont le but est de mettre en commun les données produites pour le soin et la recherche**. Cet assemblage au sein du projet baptisé « Include » se fait alors de manière totalement sécurisée mais également anonyme. Le projet nourrit également des ambitions à long terme puisqu'il doit permettre de constituer une importante source de données tout comme une

Nous avons bâti un véritable entrepôt de données de santé dans le but de les mettre en commun pour le soin et la recherche.

mise à disposition d'experts dans le domaine de l'intelligence artificielle.

Les actuels co-porteurs du projet Include Grégoire Ficheur, Vincent Sobanski et Didier Théis expliquent ainsi que l'obtention de l'autorisation Cnil « *est l'aboutissement d'une première étape. Nous sommes prêts à débuter le traitement encadré des données et ravis de pouvoir lancer les premières études.* »

Le CHU de Lille a ainsi mis sur pied un groupe composé de plusieurs corps de métiers dans le but de déterminer l'ensembles de tenants et aboutissants relatifs à la protection des données. Ce sont donc non seulement **des médecins, des personnels paramédicaux, tout comme des ingénieurs et des représentants des directions fonctionnelles du CHU qui ont agi de concert.**

Toujours est-il que cette expérience a permis de développer de nouveaux outils. Frédéric Boiron, Directeur Général du CHU de Lille explique : « *Il est essentiel d'apporter ce niveau de sécurité et de confidentialité pour nos patients. La confiance entre les équipes de soins et les patients de notre établissement est un préalable essentiel à la mise en œuvre de travaux de recherche innovants*. » De nouvelles recherches vont donc, à terme, se développer en puisant dans le terreau de cette mise en conformité RGPD.

Matmut

> **“ Un plan d'action a été établi durant l'année précédant la date fatidique ”**

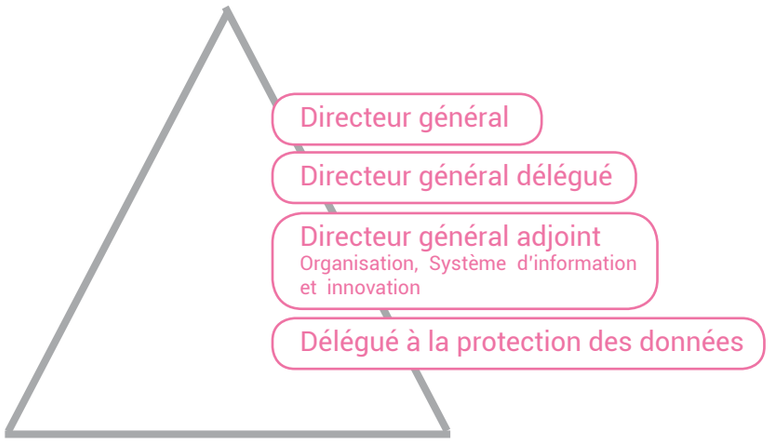
Le Groupe Matmut n'était pas sans déjà se préoccuper de protection des données personnelles, la Loi Informatiques et Libertés ayant été publiée, en sa première mouture, le 6 janvier 1978.

Néanmoins, l'entrée en application du RGPD le 25 mai 2018 supposant des obligations accrues et quelques réelles nouveautés, comme par exemple le droit à la portabilité ou encore la notification des violations de données personnelles, un plan d'actions a été établi durant l'année précédant la date fatidique, à partir d'analyses d'impacts, construites sur les différences entre ce qu'impose le RGPD et le déjà existant dans le Groupe, pour toutes les grandes thématiques de la protection des données personnelles :

- Information des personnes concernées quant aux traitements de leurs données personnelles
- Droits de ces personnes sur leurs données personnelles
- Gestion du consentement de la personne lorsque celui-ci est nécessaire pour pouvoir traiter ses données personnelles
- Sécurisation de ces données personnelles
- Contractualisation des obligations respectives des parties en matière de protection des données personnelles, avec nos partenaires et sous-traitants
- Accountability (tenue du registre des traitements de données personnelles, analyses d'impact pour les traitements les plus sensibles, les plus à risque)
- Procédure de prise en considération de la protection des données personnelles dans le mode de gestion projet (« privacy by design »).

Organisation

- Désignation, en respect de l'obligation nouvelle créée par le RGPD du Délégué à la Protection des Données (DPO), à effet du 25 mai 2018 : DPO interne, avec connaissance de la matière assurantielle, pour des avis en connexion avec le métier d'assureur (protection des données appliquée aux différents domaines d'activité du Groupe) et mutualisé entre les entités du Groupe
- Rattachement au DPO de 2 collaboratrices, un expert technique et une chargée d'études
- Rattachement administratif à la DGA OSII (avantage : proximité avec le Directeur Système d'Information (DSI) et le Responsable de la Sécurité du Système d'Information (RSSI), non négligeable pour ce qui concerne la nécessaire sécurisation des données personnelles) mais reporting d'activité directement à la DG, pour un maximum d'autonomie dans l'exercice de ses fonctions



- Lien permanent avec la Direction Juridique, Fiscale et Conformité et relais protection des données personnelles dans chacune des directions

Procédures, outils d'accountability

- Gestion projets : privacy by design
- Sollicitations métiers via formulaire, accès au portefeuille général des projets, avis DPO requis sur fiches produits, expressions de besoins, spécifications fonctionnelles pour développements informatiques …
- Gestion demandes d'usage des droits sur données personnelles :
- Boîte mail dédiée, accessible à partir du site internet du Groupe, traitements
- Conjoint entre relais protection des données personnelles des différents directions du Groupe et l'équipe DPO, base de suivi commune
- Logiciel de documentation de l' « accountability » du Groupe, regroupant les éléments ci-dessus, ainsi que les registres des traitements de données personnelles et des violations de données personnelles et divers autres documents

Relations patenaires / sous-traitants

- Questionnaire de maturité Protection des Données Personnelles et Sécurité du Système d'Information avant sélection de candidats pour appels d'offre.
- Intégration des avis DPO et RSSI dans la procédure d'achats (logiciels et autres prestations).
- Trames-type de contractualisation obligations respectives en matière de PDP et annexe descriptive des traitements de données personnelles par le ST.
- Difficulté la plus grande : la qualification, au sens RGPD, des parties prenantes au contrat. Responsable de Traitement (RT) et Sous-Traitant ? Responsables de Traitement distincts ? Responsables de Traitements conjoints ?

BNP PARIBAS

> " La protection de la vie privée et des données personnelles des clients et employés a toujours été au cœur de la stratégie du Groupe "

Au sein du Groupe les clients, les partenaires, et les employés nous confient depuis toujours des informations personnelles dans le cadre de leur activité professionnelle ou de leurs projets personnels. Notre responsabilité est de les accompagner en leur proposant des produits et services adaptés à leurs besoins, tout en respectant la confidentialité, la transparence et l'éthique dans le traitement de leurs données, et en se conformant aux exigences de minimisation édictées par le règlement.

La protection de la vie privée et des données personnelles des clients et employés a toujours été au cœur de la stratégie du Groupe BNP Paribas. **L'entrée en vigueur du RGPD ne constitue pas en France et dans certains pays l'acte fondateur révélant l'importance de la gestion des données à caractère personnelles.** Cependant, le règlement a permis de faire entrer la problématique de gestion des risques liés à ces données de manière prégnante dans les comportements quotidiens des employés du Groupe.

Dans le contexte du développement digital et avec l'arrivée de technologies complexes, capables de manipuler de larges volumes de données, l'arrivée de RGPD a aidé à une prise de conscience de chaque individu concernant la valeur de ses propres données. Pour la Banque, la mise en place de RGPD a été l'occasion de renforcer son dispositif en matière de protection des informations personnelles et de communiquer largement sur sa politique globale dans ce domaine.

Une auto-évaluation complète

Dès 2017, le Groupe BNP Paribas s'est lancé dans un vaste exercice d'auto-évaluation, déployé dans l'ensemble des métiers et fonctions du groupe. **Cet exercice a permis d'identifier les points à consolider**, pour permettre au Groupe d'atteindre une « position défendable » dès l'entrée en vigueur de RGPD, en mai 2018. La Banque a d'ailleurs su capitaliser sur la structure et la visibilité d'un vaste programme Groupe axé sur « Know Your Data », qui avait déjà permis d'initier une gouvernance forte autour de la qualité et l'intégrité de la donnée. La dimension « protection » s'est naturellement rajoutée à cette gouvernance.

L'information et le consentement de nos clients ont été une priorité absolue, des solutions rapidement opérationnelles ont été mises en place pour automatiser et faciliter l'exercice de leurs droits. Les Data Protection Notices émises par tous les métiers ont permis de communiquer en toute transparence sur l'utilisation des données de nos clients et sur leur protection, au sein de notre Groupe. Pour autant, **le sujet du consentement reste un sujet de vigilance qu'il faut désormais appréhender de manière globale dans le but de parfaire encore le parcours de nos clients.**

La remédiation contractuelle avec les fournisseurs et la mise en place des mesures de sauvegarde appropriées pour les transferts transfrontaliers ont constitué un vaste chantier, faisant l'objet de cartographies détaillées et de diverses

actions coordonnées au niveau du Groupe, entre les acteurs des métiers, les équipes Achats, Legal et les Data Offices. Des « règles d'entreprises contraignantes » (Biding Corporate Rules) ont pu être mises en place sur le périmètre des processus RH du Groupe. S'ils affichent aujourd'hui des résultats positifs, ces travaux ont été menés sur plusieurs années, avec un nombre de ressources important issues des équipes centrales et également des différents territoires.

La mise en place du concept de « Protection des données dès la conception » a été un aiguillon central pour promouvoir une méthodologie responsable et axée sur les risques portés par un processus/un produit. Plus qu'une obligation, se préoccuper dès le démarrage d'un projet des aspects relatifs à la Protection des données personnelles a permis d'ancrer la systématisation des analyses de risques ainsi que la tenue à jour des registres des traitements comme des outils faisant partie du quotidien des chefs de projets/produits. Les équipes en charge de promouvoir et d'expliquer ces sujets restent mobilisées pour continuer l'acculturation et ancrer encore plus profondément cela dans la réalité opérationnelle.

Sur un plan organisationnel, si le réseau des Data Protection Officers s'est rapidement déployé et a pu être moteur sur les différentes initiatives, celui des Chief Data Officers, déjà existant à l'arrivée de RGPD, doit désormais en mode « BAU » prendre pleinement ses responsabilités en tant que garant au quotidien de la protection des données au sein des métiers. Les Data Protection Officers pourront ainsi se concentrer sur l'exercice de leur rôle de contrôle et veille réglementaire.

Les facteurs clés de réussite

Deux ans après, nous pouvons avec recul lister les facteurs clés de réussite du programme mis en place pour répondre aux exigences du régulateur :

- L'accueil du règlement vécu non comme une nouvelle contrainte réglementaire, mais comme une opportunité.
- La mise en place rapide d'un réseau opérationnel de Data Protection Officers, en lien étroit avec celui des Chief Data Officers.
- La prise en charge de la mise en conformité réglementaire grâce à l'insertion de ces travaux au sein d'un programme référent sur les données.

Membre du Cigref

RETOUR D'EXPERIENCE

SAINT-GOBAIN

> **" Tous nos processus informatiques ont été revus pour intégrer le Privacy by design "**

Chez Saint-Gobain, la gouvernance des données passe par la mise en place d'un réseau de collaborateurs sensibilisés aux enjeux de la protection des données, au sein des différentes entités du groupe. Tous nos processus informatiques ont également été revus pour intégrer l'approche « Privacy by design » afin de se conformer aux exigences du RGPD et nous avons mis à disposition des entités concernées, un outil de gestion de la protection des données afin de leur permettre d'anticiper ces questions dès la conception d'un projet.

Saint-Gobain place également la conformité au RGPD au cœur de ses échanges avec ses prestataires. Cette gouvernance des données se retrouve ainsi dès la phase pré contractuelle et implique notamment de réfléchir à la qualification des parties. Le prestataire est-il un sous-traitant ou un responsable de traitement distinct ? **Il s'agira parfois de faire comprendre à certains sous-traitants que les clauses relatives aux données personnelles qu'ils tentent de nous imposer doivent faire l'objet d'une négociation** puisque le responsable de traitement décide aussi des moyens essentiels du traitement. Nous avons également élaboré une procédure afin de vérifier les garanties présentées par nos partenaires en termes de conformité au RGPD, avant de conclure un contrat avec eux. A ce titre, nos fournisseurs potentiels doivent remplir deux questionnaires, pour évaluer respectivement leur maturité en termes de protection des données personnelles et de cybersécurité.

Par Isaure de CHATEAUNEUF, Directrice Juridique Technologies de l'Information, Déléguée à la Protection des Données à la COMPAGNIE DE SAINT-GOBAIN

À propos de TECH IN France

Créée en 2005, TECH IN France est une association professionnelle de loi 1901 qui a pour but de rassembler et de représenter les éditeurs de logiciels, de services internet et de plateformes en france. Porte-parole de l'industrie numérique, TECH IN France compte 400 entreprises adhérentes : de la startup à la multinationale en passant par la PME et les grands groupes français ; soit 8 milliards d'euros et 90 000 emplois.

Les missions de TECH IN France :

- Agir pour faire entendre la voix des entreprises de la filière auprès des institutions et pouvoirs publics
- Assurer la promotion du rôle stratégique de la filière dans l'économie et la société
- Animer l'écosystème en offrant une large gamme de services qui améliorent la perofrmance des entreprises
- Faire vivre la communauté : créer des opportunités de dialogue entre pairs et d'identification

Contact adhérents:
Allyson Parmentier, a.parmentier@techinfrance.fr

TECH IN France
13 rue La Fayette
75009 Paris
0140324590
www.techinfrance.fr

OURS

Directeur de publication
Pierre-Marie Lehucher
Coordination
Loïc Rivière
Rédaction
Olivier Robillart

Création graphique & maquette
Sixtine Crosnier

Impression
Axiom Graphic

Remerciements
Chloé Rousselet
Floriane Richiardi
Jawaher Allala
Radhouan Mahrez
Sylvain Staub
Cigref
Cnil
EasyVista

TECH'IN FRANCE

Réservé aux adhérents de TECH IN France
- 2020 -