sia partners

RÈGLEMENT EUROPÉEN SUR LA PROTECTION DES DONNÉES :

Comment se préparer d'ici mai 2018 ?

SOMMAIRE

ÉDITO

La collecte et le traitement des données sont des enjeux majeurs pour le secteur de l'assurance. Depuis quelques années, nous assistons à une révolution progressive du secteur. À travers la numérisation des canaux et des processus et le développement des objets connectés, les assureurs collectent de plus en plus de données à caractère personnel sur leurs assurés. L'objectif de ce modèle dit « data-driven » est multiple : les assureurs peuvent améliorer leurs méthodes de segmentation et de tarification, enrichir leur connaissance des clients, mais également renforcer d'autres activités telles que la détection des fraudes.

Cependant, la collecte et l'utilisation des données à caractère personnel génèrent de nombreux enjeux en matière de protection des droits des citoyens. Jusqu'à présent, l'exploitation de données personnelles a été soumise en France, à la Loi Informatique et liberté de janvier 1978, modifiée en 2004 et en Europe par la directive 95/46/CE sur la protection des données personnelles. Néanmoins, compte tenu du développement rapide des technologies, la règlementation s'avère totalement décorrélée de la réalité. Viviane Reding, ancienne vice-présidente de la Commission Européenne, arguait en ce sens en 2012 : «moins d'1 % des européens utilisaient Internet [en 1995]. À l'heure actuelle, de grandes quantités de données à caractère personnel sont transférées et échangées d'un continent à l'autre en quelques fractions de seconde». C'est pourquoi une réforme profonde de la règlementation en matière de protection des données au sein de l'Union européenne a été proposée par la commission afin de l'actualiser et la renforcer.

Approuvé le 15 décembre 2015 et publié le 4 mai 2016 dans le Journal officiel de l'Union européenne pour application le 25 mai 2018, Le Règlement Général sur la Protection des Données va profondément impacter l'ensemble des secteurs dont l'assurance dans la manière de collecter et d'exploiter les données. Outre les nouvelles règles beaucoup plus strictes qu'il introduit, le règlement alourdit les sanctions en cas de non-conformité - jusqu'à 20M€ ou 4% du chiffre d'affaires mondial d'une entreprise.

Sia Partners vous offre dans ce livret un décryptage des principaux articles de ce Règlement qui impacteront la manière dont vous collectez et traitez les données à caractère personnel.

Bonne lecture,

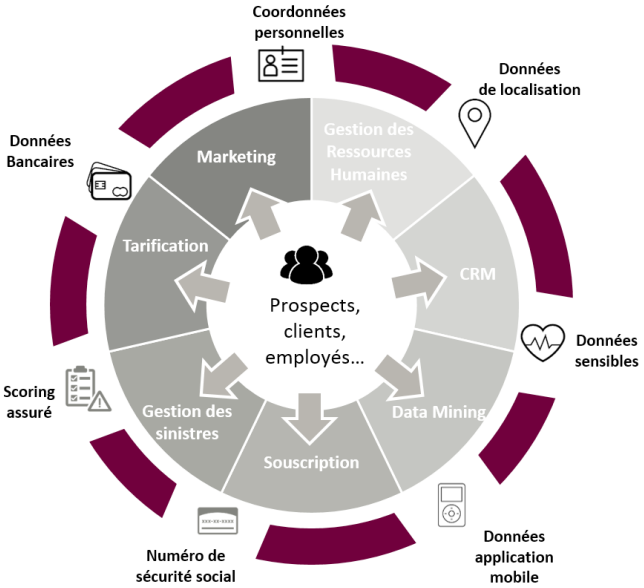
JÉRÉMIE LE SANT
Senior Consultant UC assurance
jeremie.lesant@sia-partners.com
Tel : +33 7 61 80 22 76

PHILIPPE MIGNEN
Consultant UC assurance
philippe.mignen@sia-partners.com
Tel : +33 6 66 01 86 77

JULIEN SAC
Partner
julien.sac@sia-partners.com
Tel : +33 6 26 11 24 02

LA DONNÉE EST UN ACTIF PRIORITAIRE ET DEVIENT L'UN DES ENJEUX MAJEURS DU SECTEUR DE L'ASSURANCE

La collecte et l'utilisation de données personnelles est au cœur du métier d'assureur



Les assureurs et leurs intermédiaires collectent et utilisent une grande quantité de données à caractère personnel et sensible sur leur clients et leurs employés et innovent en ce sens afin d'exercer leurs activités (souscription, gestion des sinistres, fraude etc.)

Il est aujourd'hui primordial de (re)penser la place de la donnée au sein de l'entreprise, en adoptant notamment une démarche de Data Management cohérente avec la stratégie globale de l'entreprise.

IT
Efficacité et stockage

- Data Management Platform
- Architecture & Gouvernance
- Dématérialisation

BUSINESS
Optimisation et Opportunités

- Data science
- Analyse de données & Big data
- Qualité des données

JURIDIQUE
Sécurité et Conformité

- Sécurité des données
- Protection des données

La protection de ces données prend ainsi une importance considérable sur ce marché. Sia Partners y consacre ainsi une étude complète, en vous proposant notamment un décryptage des principaux chantiers à mettre en œuvre dans l'optique du nouveau Règlement Général sur la Protection des Données.

Section 1

LES DONNÉES, UNE THÉMATIQUE UNIVERSELLE, DES DÉBATS LOCAUX

LES DONNÉES, UNE THÉMATIQUE UNIVERSELLE, DES DÉBATS LOCAUX

Les instances juridiques mondiales se sont aujourd'hui emparées du sujet de la protection des données personnelles et sensibles pour répondre à 3 dérives liées à l'usage de services et technologies toujours plus intrusives

Des règlementations au service du consommateur

COURSE À LA COLLECTE MASSIVE DE DONNÉES PRIVÉES

Les entreprises placent le curseur de plus en plus loin dans la collecte des données : la collecte est devenue prioritaire, qu'elle qu'en soit la finalité et la légalité

Microsoft a été mis en demeure par le régulateur français de mettre en conformité son nouveau système d'exploitation Windows 10 avec la loi Informatique et Libertés, en cessant notamment la collecte excessive de données ainsi que le suivi de la navigation des utilisateurs sans leur consentement.

DISPOSITIF DE PROTECTION DES DONNÉES LIMITÉ

De nombreuses entreprises ne disposent pas de dispositif de protection des données à même d'assurer la sécurité de celles-ci, dans un environnement pourtant de plus en plus hostiles (hacking, phishing etc.)

Zurich Insurance a été condamné pour perte des données personnelles de 46.000 clients y compris dans certains cas les numéros de compte bancaire et de carte de crédit.

CLIENTS PEU VIGILANTS LORS DE LA TRANSMISSION DES DONNÉES À CARACTÈRE PERSONNEL

Le client est peu sensible aux enjeux de protection des données et ne dispose donc pas de la culture de la vigilance lorsqu'il donne accès à ses données. Il donne ainsi son accord à tort ou à raison à toute application.

Niantich, développeur du phénomène Pokemon GO, a obtenu de chacun des utilisateurs l'autorisation de consulter et modifier la quasi-totalité des informations de leur compte Google.

Afin de palier à ces manquements et restaurer la bonne protection des données personnelles des clients, les régulateurs tendent à s'accorder sur un cadre commun restreignant les conditions de collecte et les traitements acceptables.

Pour faire respecter ce cadre de bienséance, la menace de sanctions financières (et réputationelles) est primordiale. Jusqu'alors, les sanctions, négligeables au regard des chiffres d'affaires, n'effrayaient pas les entreprises, qui préféraient poursuivre leurs activités dans l'illégalité au risque de se voir réprimander.

Le nouveau Règlement Général sur la Protection des Données prévoit une augmentation des sanctions financières jusqu'à 4 % du chiffre d'affaires global réalisé dans l'UE.

LES DONNÉES, UNE THÉMATIQUE UNIVERSELLE, DES DÉBATS LOCAUX

Les règlementations relatives à la protection des données reposent sur un socle commun de 7 principes tels qu'énoncés ci-après, qui entendent définir les questions clés pour assurer une gestion appropriée et raisonnable de données personnelles

Un socle théorique commun

FINALITÉ DE LA COLLECTE DE DONNÉES ET INFORMATION DU CLIENT
Premièrement, pourquoi collectez-vous des données ? Quelle en est la finalité ?

RECUEIL DU CONSENTEMENT DU CLIENT
Les personnes devraient-elles se voir proposer un choix au moment de la collecte de données ? Devraient-elles donner leur consentement ?

ACCESSIBILITÉ AUX DONNÉES ET DROITS DES CLIENTS
Au niveau de la transparence, les utilisateurs devraient-ils pouvoir accéder à leurs données, les supprimer et les rectifier ?

SÉCURITÉ DES DONNÉES
Les données ont-elles de la valeur ?

RESPONSABILITÉ ET CONTRÔLE
Qui est responsable en interne et en externe aux yeux de la loi ?

CONTRAINTES DE FINALITÉ
Si une société annonce qu'elle utilise les données pour une raison précise, une finalité déterminée, cet ensemble de données ne peut être utilisé à d'autres fins, à moins de demander à la personne concernée son accord par un consentement quelconque.

MINIMISATION DES DONNÉES COLLECTÉES
Les données collectées sont-elles toutes utiles à l'atteinte des finalités définies précédemment ?

Ces principes n'ont pas force de loi. Cependant ils constituent la colonne vertébrale de toute loi sur la protection des données et donnent les lignes directrices orientant la collecte, l'utilisation et la protection des informations à caractère personnel.
Ainsi, de fortes divergences transparaissent entre les différents pays, et notamment entre l'Union Européenne, les Etats-Unis et l'Asie contraignant d'autant plus les entreprises dans leur mise en conformité règlementaire.

LES DONNÉES, UNE THÉMATIQUE UNIVERSELLE, DES DÉBATS LOCAUX

Des divergences encore notables entre les différentes juridictions

Il apparaît aujourd'hui que les législations en matière de protection des données varient selon leur complétude : tandis que l'Union Européenne couvre l'ensemble des principes énoncés précédemment, on constate que la zone asiatique ne dispose pas d'une législation totale uniforme et que les Etats-Unis accusent par nature un retard sur la protection des données .

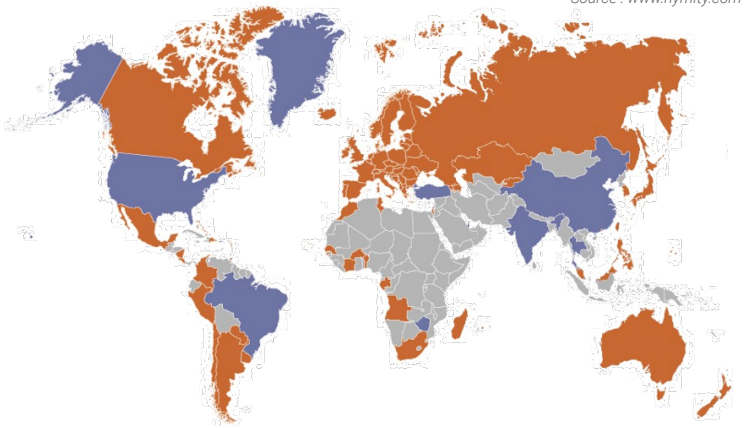
LEGENDE

Couverture complète Pays offrant une couverture complète assurée par une ou plusieurs lois en matière de protection de la vie privée ou des données.

Couverture partielle Pays possédant une législation sectorielle en matière de protection de la vie privée ou des données (ex. secteur public, financier ou télécommunications).

Aucune couverture Pays ne possédant pas de législation spécifique en matière de protection de la vie privée ou des données mais une forme de couverture intégrée à leur constitution ou d'autres lois.

Source : www.nymity.com



- En tant qu'acteur du marché européen de l'assurance, vous êtes potentiellement exposés à l'ensemble de ces règlementations. Si le nouveau Règlement Général sur la Protection des Données régira bientôt la grande majorité de vos process, il convient également de prendre en compte les règlementations des pays auprès desquels vous pouvez être amenés à effectuer des transferts.
- Vos activités sous-traitées, vos traités de réassurance, vos partenaires, vos entités : autant de cas pour lesquels une attention particulière devra être portée au bon respect des règlementations locales.
- Si cette carte fait montre de diversités notables entre les différents pays du monde, les règlementations tendent à s'harmoniser autour du cadre le plus contraignant, celui du nouveau Règlement Général sur la Protection des Données.

LES DONNÉES, UNE THÉMATIQUE UNIVERSELLE, DES DÉBATS LOCAUX

Des divergences encore notables entre les différentes juridictions

ÉTATS-UNIS

- Invalidé par la Cour de Justice de l'Union européenne en octobre 2015, l'accord de « Safe Harbor » (2000) est remplacé par l'accord dit « Privacy Shield », adopté par la Commission Européenne en juillet 2016. Cet accord encadrera le transfert de données personnelles des citoyens européens vers des data centers (« centres de données ») aux Etats-Unis.
- De fait, les négociations sur un nouvel accord avaient commencé dès 2014, suite aux révélations d'Edward Snowden sur les programmes de surveillance de masse des services de renseignements américains.

EUROPE

- La gestion des données personnelles était règlementée par la directive européenne de 1995 95/46 / CE, qui visait à protéger le consommateur concernant le traitement des données personnelles et à règlementer la libre circulation des données.
- La directive est maintenant éloignée de la réalité. Les nouveaux objectifs du Règlement sont l'harmonisation des législations locales et de donner plus de droits aux assurés / clients.

ASIE

- Certaines évolutions règlementaires importantes au cours des dernières années en Asie

◊ **Chine - 2015 |**
«Mesures pour Peines contre les atteintes aux droits et intérêts des consommateurs "

◊ **Hong Kong - Avril 2013 |**
«Données personnelles (Privacy) Ordinance (Cap . 486) "

◊ **Japon - Septembre 2015 |**
Révision de la «Loi sur la protection des renseignements personnels»

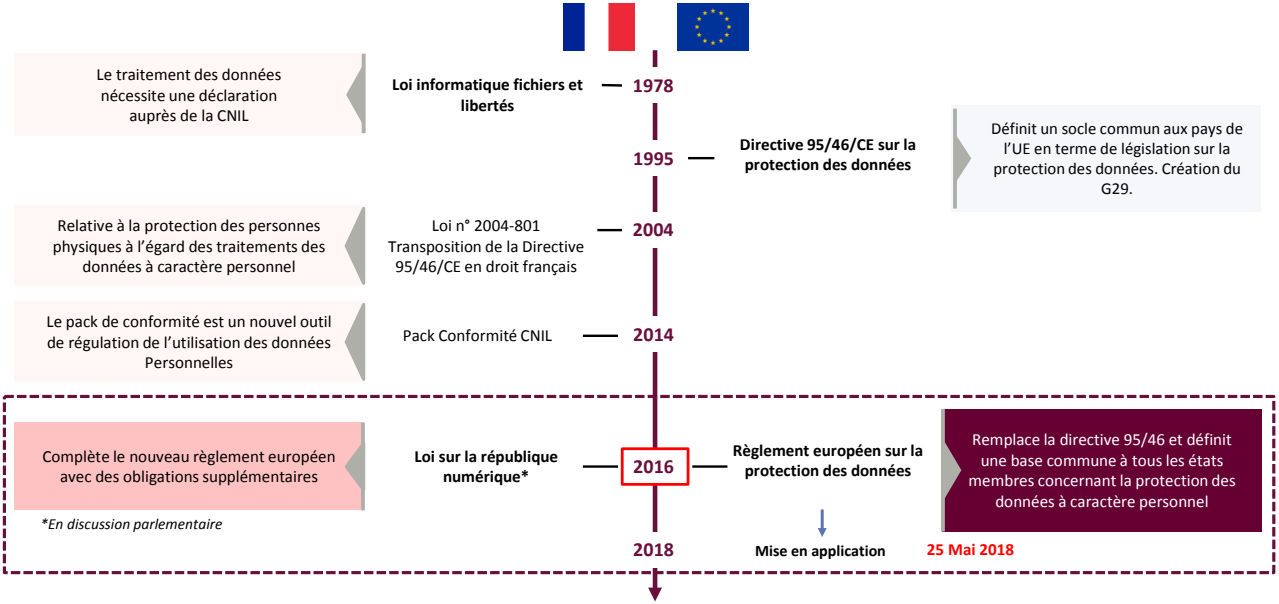
Section 2

DÉCRYPTAGE DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

DÉCRYPTAGE DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Le Règlement Général sur la Protection des Données (RGPD) : à l'origine, la France

La France apparaît comme un pionnier sur la thématique des protections des données : les principes décrétés en 1978 dans la Loi informatique et libertés ont longtemps fait office de référence.
Nouvelles technologies, Big Data, Internet des objets : les données n'ont aujourd'hui plus de frontières et la nécessité d'un renforcement du cadre règlementaire s'impose. L'Europe s'est ainsi emparée du sujet en promulguant la directive 95 / 46, dont l'entrée en vigueur en mai 2018 marquera l'avènement d'une règlementation stricte, adaptée aux nouveaux usages et harmonisée.



DÉCRYPTAGE DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Le nouveau règlement européen sur la protection des données est constitué de 9 chapitres dont la criticité pour votre organisation varie : le tableau ci-dessous décline les principaux articles impactant les métiers de l'assurance.

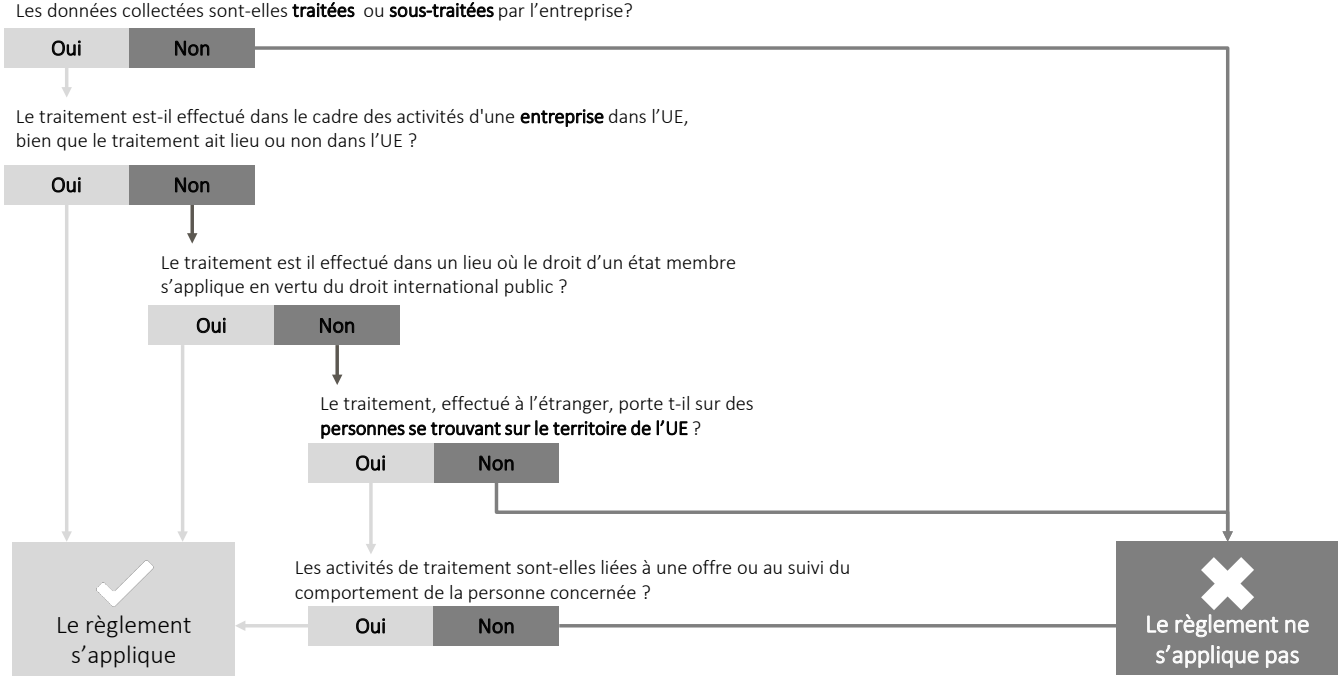
Les principaux articles impactant du Règlement Général sur la Protection des Données

- Sia Partners vous propose ci-après le décryptage de 24 articles à fort impact pour votre entreprise.
- Le choix de ces articles est un parti pris excluant de fait nombre de thématiques qui pourraient vous être également primordiales. Nous sommes bien évidemment disponibles pour vous accompagner dans le décryptage de l'ensemble des articles de ce Règlement.

DÉCRYPTAGE DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Un champ matériel et territorial d'application très large

Le champ d'application du Règlement, défini aux articles 2 (champ d'application matériel) et 3 (champ d'application territorial) est beaucoup plus large que celui de la directive. En particulier, le Règlement instaure une règle d'application extraterritoriale du droit européen et les sous-traitants sont à présent directement concernés par la règlementation.
Le graphique ci-dessous vous renseigne sur l'applicabilité du Règlement.



DÉCRYPTAGE DU RÈGLEMENT GÉNÉRAL SUR LA PROTECTION DES DONNÉES

Les grands enjeux pour un assureur

Afin de vous aider dans l'identification des principaux enjeux inhérents à chaque article décrypté ci-après, Sia Partners a défini 4 principaux axes de travail. Ceux-ci permettent d'anticiper les acteurs à solliciter et les charges de travail à envisager dans la mise en conformité vis-à-vis du Règlement Général sur la Protection des Données.

GOUVERNANCE

Ce Règlement vise à encourager les assureurs à mettre en place un dispositif autosuffisant de protection des données.
L'une des principales difficultés sera d'assurer une communication permanente entre l'ensemble des directions et le délégué à la protection des données. La mise en place de ce type de dispositif nécessite l'animation d'un réseau de correspondants afin de veiller à la fluidité de la communication.

SYSTÈMES D'INFORMATION

L'une des origines de ce Règlement était d'intégrer les évolutions technologiques à la règlementation européenne. Outre le renforcement de la sécurité des données, les assureurs devront mettre en œuvre les moyens nécessaires pour tracer les données afin d'identifier les potentielles violations, de s'assurer du respect des délais de conservation et de permettre leur suppression. D'autre part, les assureurs devront également s'assurer du niveau de protection adéquat dès la conception (Privacy by design) des nouveaux outils/nouvelles applications traitant des données personnelles.

REPORTINGS

Les assureurs devront également mettre en place des nouveaux processus de production des reportings à destination des assurés (communication des données collectées et traitées), de l'autorité de contrôle (communication des violations de données, registre des traitements) et des dirigeants (résultat de l'analyse d'impact, rapport annuel de revue du dispositif de protection des données).

PROCESS

D'ici 2018, les assureurs devront revoir la manière de collecter les données personnelles. L'introduction du consentement explicite, de la limitation du traitement et du droit à l'oubli, impose aux assureurs de clarifier le type de données nécessaire à la poursuite de leurs activités et de répondre en continu aux demandes des clients, y compris des demandes de transfert des informations aux concurrents (portabilité des données).
Un travail d'audit et d'amélioration des processus existants sera alors indispensable.

SIA PARTNERS INDEX

Nous vous proposons pour l'ensemble des articles décryptés ci-après une évaluation des impacts selon ces 4 axes de réflexion

Gouvernance ☆☆☆☆

SI ☆☆☆☆

Reportings ☆☆☆☆

Process ☆☆☆☆

RÈGLEMENTATIONS : QUELLES ÉVOLUTIONS ?

Que dit la règlementation actuelle?

La règlementation française définissait déjà ces deux concepts clés : une compagnie d'assurance peut collecter des données des assurés tant que ces derniers donnent l'accord de traitement pour une finalité définie et licite.

Quels changements sont portés par le nouveau Règlement Général sur la Protection des Données ?

Le règlement clarifie les conditions de la collecte des données personnelles et notamment :

- Il précise les finalités de traitement considérées comme licites, tout en laissant une marge de manœuvre aux Etats membres
- Il contraint à la cessation du traitement en cas d'évolution d'incompatibilité des finalités (suite à une évolution du traitements)
- Il apporte des conditions supplémentaires en matière de consentement et notamment en matière de consentement électronique

QUELS SONT LES CHANTIERS À METTRE EN OEUVRE ?

1. Refondre le processus de collecte des données personnelles

- Revoir les clausiers types des contrats afin d'intégrer les informations clés attendues par le Règlement
- Intégrer dans le processus de souscription, le consentement explicite de l'assuré quant à l'utilisation de ses données à caractère personnel et sensible
- Revoir le dispositif de protection des données en place dans les applications B to C (site internet, application mobile…)

2. Prouver en tout temps le consentement explicite de l'assuré et la licéité du traitement

- Mise en place d'un processus de stockage des consentements
- Formaliser le processus de demande de consentement
- Justifier la conformité du traitement par rapport au consentement préalable

RÈGLEMENTATIONS : QUELLES ÉVOLUTIONS ?

Que dit la règlementation actuelle?

La loi Informatique et Libertés impose une information obligatoire concernant sept éléments (identité du responsable, finalité poursuivie, caractère obligatoire ou facultatif des réponses, des conséquences pour la personne d'un défaut de réponse, destinataires des données, droits des personnes concernées, transferts de données), ainsi qu'un régime particulier pour les questionnaires et les abonnés ou utilisateurs d'un service de communication électronique.

Quels changements sont portés par le nouveau Règlement Général sur la Protection des Données ?

Les éléments d'informations se densifient, incluant :

- L'éventuel délégué à la protection des données , le fondement juridique du traitement en sus des finalités , et les intérêts légitimes du responsable
- L'éventuel transfert de données, l'absence de décision d'adéquation du niveau de protection, des garanties prises ou des moyens d'obtenir une copie
- La période de conservation des données ou les éléments permettant de la déterminer, l'existence de l'ensemble des droits reconnus à la personne, le droit d'introduire une réclamation auprès d'une autorité de contrôle
- L'existence d'une prise de décision automatisée telle que le profilage, la logique sous-jacente et les conséquences du traitement pour la personne
- Les changements de finalité par rapport à la finalité initiale, impliquant une nouvelle information préalable sur les éléments précités

Le règlement précise aussi que le responsable doit fournir ces informations à la personne concernée SOIT dans un délai raisonnable qui n'excède pas un mois après la collecte SOIT s'il est envisagé de communiquer les informations à un autre destinataire ou d'utiliser les données pour une communication à la personne concernée, au plus tard lorsque les informations sont communiquées pour la première fois.

QUELS SONT LES CHANTIERS À METTRE EN OEUVRE ?

Mettre à disposition l'ensemble de ces informations

- Revoir les moyens de communication et le contenu adressés aux personnes concernées
- Réviser les clauses des contrats afin d'inclure ces nouvelles informations obligatoires
- Mettre à jour les contrats par des avenants pour informer les personnes dont les données sont déjà collectées

RÈGLEMENTATIONS : QUELLES ÉVOLUTIONS ?

Que dit la règlementation actuelle?

Aujourd'hui, le client peut exiger du responsable d'un traitement que soient rectifiées, complétées, mises à jour, verrouillées ou effacées les données personnelles le concernant et qui seraient inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdite.

Quels changements sont portés par le nouveau Règlement Général sur la Protection des Données ?

Cette disposition fixe en plus les conditions d'exercice du droit à l'oubli et à la limitation, soulignant l'obligation pour le responsable de traitement d'informer tous les éventuels processeurs des données clients de ces conditions.

Ainsi l'effacement doit être obtenu dans les meilleurs délais lorsque l'un des motifs décrits dans l'art. 17 est évoqué : l'inutilité au regard des finalités de traitement, l'illicéité du traitement, le retrait du consentement qui fonde le traitement avec absence de fondement juridique au traitement, etc.

De la même façon, la limitation du traitement des données peut être demandée dans les cas suivants tels que : le temps pour le responsable de contrôler lors de la contestation de l'inexactitude des données, l'illicéité du traitement, le temps de procéder à la vérification de la balance des intérêts entre les intérêts légitimes du responsable et ceux de la personne concernée

- Quoique plus nécessaires à la poursuite des finalités du traitement, la personne concernée en a besoin pour la constatation, l'exercice ou la défense de ses droits en justice ;

QUELS SONT LES CHANTIERS À METTRE EN OEUVRE ?

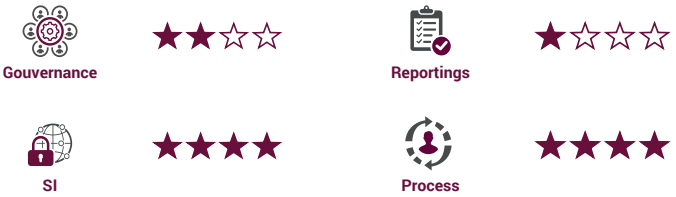
Mettre en place un dispositif de traitement des requêtes

- Mettre en place un registre pour tracer l'ensemble des traitements effectués et leurs responsables de traitement
- Formaliser le processus d'information des responsables de traitement par le responsable de traitement principal lors de requête de rectification, de limitation ou d'effacement

Mettre en place un dispositif d'information des personnes concernées

Informer et rappeler leurs droits aux personnes concernées par le traitement de leurs données personnelles :

- Les clients lors de la souscription du contrat
- Les employés à la signature du contrat d'embauche et lors de campagnes de communication interne



Privacy by design and by default – Article 25

RÈGLEMENTATIONS : QUELLES ÉVOLUTIONS ?

Que dit la règlementation actuelle?

Ni la règlementation française ni la directive européenne ne faisaient mention de ces deux concepts

Quels changements sont portés par le nouveau Règlement Général sur la Protection des Données ?

La protection dès la conception (privacy by design) introduit des prérequis en matière de développement des nouvelles technologies. En effet, chaque nouvelle technologie traitant ou collectant des données personnelles devra garantir dès sa conception et lors de chaque utilisation, le plus haut niveau de protection des données. L'entreprise devra donc mettre en œuvre les moyens nécessaires pour protéger les données personnelles sans que l'utilisateur n'en ait besoin de s'en assurer. La protection par défaut (privacy by default) impose aux entreprises d'offrir aux personnes concernées, sans délai et facilement, le plus haut niveau de protection possible.

Ces deux concepts reposent sur les principaux principes suivants:

- Des mesures proactives et préventives
- Une protection systématique
- Une sécurité continue des informations (de la collecte à la destruction)

QUELS SONT LES CHANTIERS À METTRE EN OEUVRE ?

- Mettre en œuvre une étroite collaboration entre les différents métiers au sein de l'organisation : data scientists, département juridique et conformité, départements métiers (marketing, commercial…)
- Intégrer les processus spécifiques de contrôle au processus d'analyse d'impact sur la protection des données, afin de garantir la protection dès la conception
- Définir également des critères concrets permettant de s'assurer du respect des deux concepts

RÈGLEMENTATIONS : QUELLES ÉVOLUTIONS ?

Que dit la règlementation actuelle?

La règlementation française contraignait déjà le sous-traitant à présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité. Un contrat ou acte juridique obligatoire entre le sous-traitant et le responsable de traitement devait formaliser la sous-traitance des traitements de données personnelles. Le responsable du traitement devait également veiller au respect de ces mesures.

Quels changements sont portés par le nouveau Règlement Général sur la Protection des Données ?

Le règlement accorde plus d'importance au sous-traitant dans le dispositif de protection des données. Le contrat doit à présent préciser les principales informations sur le traitement lui-même (finalité, type de données et durée du traitement, etc.), ainsi que mentionner les nouvelles obligations du sous-traitant en matière de sécurité, de restriction du traitement des données à la seule finalité définie, de remontée des alertes au responsable de traitement en cas de violation des données personnelles, afin que ce dernier puisse fournir l'ensemble de informations exigées par le règlement.

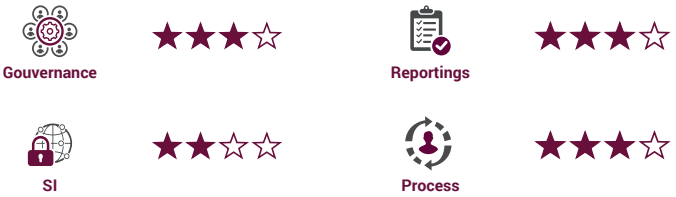
QUELS SONT LES CHANTIERS À METTRE EN OEUVRE ?

1. Apporter une réponse aux conséquences immédiates pour les responsables de traitement

- Revoir l'ensemble des contrats de sous-traitance en cas de traitement de données à caractère personnel et sensible afin d'intégrer les éléments requis par le règlement
- Définir un processus de reporting avec les sous-traitants

2. Apporter une réponse aux conséquences immédiates pour les sous-traitants

- Mettre en place un dispositif de protection des données permettant de justifier du respect du règlement, notamment en matière de sécurité, durée de conservation, transfert vers un sous-traitant secondaire
- Etudier la possibilité de certification ou d'adhésion à un code de conduite pour prouver l'existence de garanties suffisantes
- Définir un processus de remontée des alertes jusqu'au responsable de traitement en cas de violation de données



RÈGLEMENTATIONS : QUELLES ÉVOLUTIONS ?

Que dit la règlementation actuelle?

Afin de réduire la charge déclarative des entreprises, l'article 67 de la loi Informatique et Libertés permet de déroger à certaines obligations de notification auprès de la CNIL. Lorsqu'un Correspondant Informatique et Libertés est nommé, une entreprise peut déroger à certaines obligations en ce qui concerne les traitements mis en œuvre aux seules fins d'exercice. Le CIL devait les recenser dans un registre à tenir à disposition de la CNIL.

Quels changements sont portés par le nouveau Règlement Général sur la Protection des Données ?

Le règlement a généralisé cette pratique à l'ensemble des traitements en supprimant les obligations de notification couteuse et peu efficace. Aussi, l'ensemble des responsables et des sous-traitants devront tenir des registres pour toutes les catégories d'activité de traitement relevant de leur responsabilité. Ce registre devra être présenté sous une forme écrite, y compris électronique, et être tenu à disposition de l'autorité de contrôle.

Les entreprises de moins de 250 salariés pourront déroger à cette règle, à moins que :

- Le traitement soit susceptible de comporter un risque élevé au regard des droits et des libertés des personnes concernées
- Le traitement ne soit pas occasionnel
- Le traitement porte sur des données sensibles

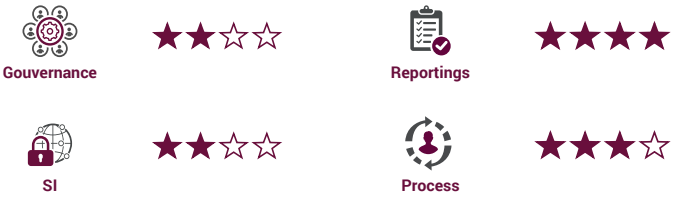
QUELS SONT LES CHANTIERS À METTRE EN OEUVRE ?

1. Informations à fournir pour le responsable de traitement :

- Le nom et les coordonnées des co-responsables du traitement et du délégué à la protection des données
- Les finalités du traitement
- Une description des catégories de personnes concernées et de données à caractère personnel
- Les catégories de destinataires
- Les transferts de données à caractère personnel et les documents attestant de l'existence de garanties appropriées
- Les délais de conservation
- Une description générale des mesures de sécurité structurelles et techniques

2. Informations à fournir pour le sous-traitant

- Le nom et les coordonnées du sous-traitant et de son responsable du traitement et du délégué à la protection des données
- les catégories de traitements effectués pour le compte de chaque responsable du traitement
- Les transferts de données à caractère personnel et les documents attestant de l'existence de garanties appropriées
- Une description générale des mesures de sécurité structurelles et techniques



RÈGLEMENTATIONS : QUELLES ÉVOLUTIONS ?

Que dit la règlementation actuelle?

La règlementation française imposait au responsable de traitement et au sous-traitant de prendre toutes les précautions utiles pour préserver la sécurité des données et, notamment, empêcher leur déformation et leur accès à des personnes non-autorisées.

Quels changements sont portés par le nouveau Règlement Général sur la Protection des Données ?

Le règlement complète la règlementation existante en précisant que l'obligation ou non de mettre en œuvre des mesures techniques et organisationnelles pour garantir un niveau de sécurité satisfaisant doit être justifiée par le risque encouru, c'est-à-dire :

- Analyser les coûts et la faisabilité opérationnelle au regard de la nature, la portée, le contexte et les finalités du traitement…
- Etudier l'utilisation des moyens proposés par le règlement : la pseudonymisation et le chiffrement des données à caractère personnel, l'aptitude à restaurer la disponibilité et l'accès aux données dans un délai raisonnable en cas d'incident physique ou technique, la mise en place d'un processus régulier de test et d'évaluation…

QUELS SONT LES CHANTIERS À METTRE EN OEUVRE ?

1. Mettre en place une gouvernance de la protection des données

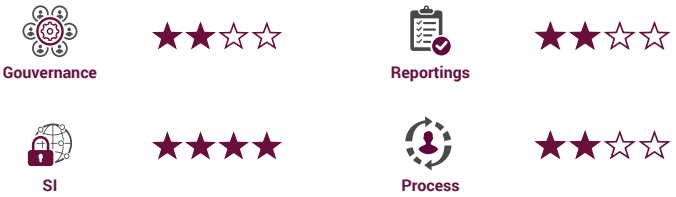
Inclure les différentes entités de l'entreprise (le département juridique et de conformité, le Data Protection Officer, le département SI, le responsable Sécurité de l'Information et les opérationnels) afin de favoriser un échange régulier entre les acteurs concernés

2. Mettre en place un audit interne régulier et formalisé

A partir du registre des traitements, faire une analyse de risques liés à la sécurité des données personnelles afin de déterminer un plan d'action pour adapter les mesures techniques et organisationnelles existantes

3. Mettre en place un processus de remédiation en cas de faille de sécurité

- Définir un processus d'analyse des impacts en cas de violation des données personnelles
- Définir le processus de remontée des informations : pour rappel le responsable de traitement doit notifier le régulateur d'une violation de données sous 72 heures à moins qu'il puisse justifier le dépassement du délai



RÈGLEMENTATIONS : QUELLES ÉVOLUTIONS ?

Que dit la règlementation actuelle?

La règlementation actuelle ne fait pas mention d'une quelconque obligation d'analyser les impacts de traitement de données personnelles. De telles démarches peuvent néanmoins être entreprises dans une démarche plus globale d'évaluation des risques de non-conformité.

Quels changements sont portés par le nouveau Règlement Général sur la Protection des Données ?

Désormais, la réalisation d'une analyse d'impact est requise pour certains traitements « à haut risque » (exposition à un risque élevé au regard des droits et libertés des personnes), et notamment pour les opérations de traitement d'un volume de données personnelles conséquent et à grande échelle (régional à supranational). On peut citer, par exemple, le big data à travers les réseaux sociaux.

Lorsqu'un traitement est porteur de risque, le responsable de traitement est alors tenu d'évaluer l'origine, la nature, la portée, le contexte, la particularité et la gravité de ce risque. Cette analyse doit contenir a minima :

- Une description systématique des traitements envisagés et des finalités poursuivies
- Une analyse de la nécessité et de la proportionnalité des activités de traitement au regard des finalités poursuivies
- Une évaluation du risque pour les droits et libertés des personnes concernées
- Les mesures envisagées pour atténuer ce risque

QUELS SONT LES CHANTIERS À METTRE EN OEUVRE ?

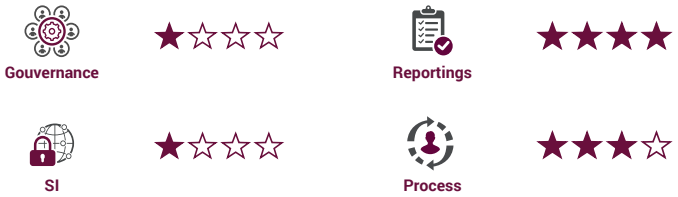
1. Identifier les risques concernées

Il s'agira de mener une étude afin de :

- Déterminer les risques qui nécessiteraient une analyse d'impact, notamment ceux qui ne sont pas mentionnées dans l'art.35
- Apprécier l'importance du risque notamment au regard du volume de données personnelles en jeu et de l'échelle d'exposition

2. Mettre en place l'analyse d'impact

- Définir un template d'analyse d'impact harmonisé pour l'ensemble des entités du groupe, en collaborant notamment avec la direction des Risques Opérationnels pour les échelles d'évaluation du risque
- Etudier les coûts de l'analyse d'impact en regard de l'ampleur des traitements
- Mobiliser les ressources compétentes en interne et en externe



Délégué à la Protection des Données – Articles 37, 38 et 39

RÈGLEMENTATIONS : QUELLES ÉVOLUTIONS ?

Que dit la règlementation actuelle?

Afin de réduire la charge déclarative des entreprises, la règlementation française avait créé le statut de Correspondant Informatique et Libertés, chargé d'assurer le respect des obligations en matière de protection des données. Il était l'interlocuteur privilégié de la CNIL et avait pour principale obligation de tenir à jour un registre des traitements automatisés et établir un bilan annuel des activités à présenter au responsable de traitement et à tenir à disposition de la CNIL

Quels changements sont portés par le nouveau Règlement Général sur la Protection des Données ?

Afin d'harmoniser les pratiques entre l'ensemble des pays européens, la nomination d'un délégué à la protection des données est rendu systématique :

- Lorsque les activités de base consistent en des traitements qui nécessitent un suivi régulier et systématique des personnes concernées
- Lorsque les activités de base consistent en des traitements à grande échelle de données sensibles ou pénales

L'entreprise devra alors s'assurer que le délégué est indépendant des activités concernées par le règlement afin d'éviter de potentiels conflits d'intérêt et lui donner l'ensemble des moyens nécessaires à ses missions. L'un des difficultés majeures pour le délégué sera d'imposer les mesures nécessaires pour assurer la mise en conformité des traitements.

QUELS SONT LES CHANTIERS À METTRE EN OEUVRE ?

1. Garantir l'intégration de la protection des données dans l'ensemble de l'organisation

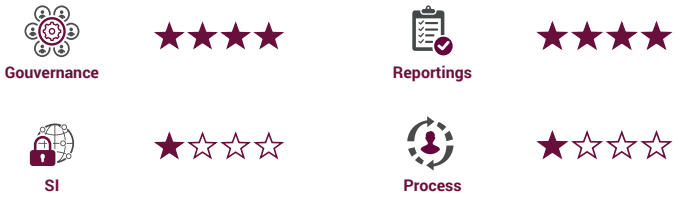
- Assurer ou organiser des formations qui devront être intégrées au plan de formation tenu par la direction des Ressources Humaines
- Emettre un avis lors de tout nouveau traitement
- Valider l'analyse d'impact relative à la protection des données

2. Garantir la conformité au règlement et aux règles internes

Emettre un avis lors de tout nouveau traitement en adoptant une démarche de Privacy by design

3. Incarner le référant et le point de contact de l'environnement extérieur à l'entreprise

- Gérer les réclamations des clients en la matière (suppression, modification…)
- Echanger avec la CNIL, notamment sur les déclarations de traitements de données personnelles ainsi que le suivi de formations



RÈGLEMENTATIONS : QUELLES ÉVOLUTIONS ?

Que dit la règlementation actuelle?

La règlementation française a introduit le principe d'adéquation : un transfert de données à caractère personnel vers un pays en dehors de l'Union européenne ne peut avoir lieu que si le pays destinataire des données assure un niveau de protection adéquat. Le responsable de traitement a ensuite l'obligation de notifier le régulateur du transfert ou d'en demander l'autorisation. Concernant les transferts intragroupe, la mise en place de Binding Corporate Rules (ou règles interentreprises) permet de simplifier les démarches administratives auprès du régulateur.

Quels changements sont portés par le nouveau Règlement Général sur la Protection des Données ?

Le règlement élargit le champ de d'application de la protection des données. Ainsi, les responsables de traitement devront suivre, les transferts de données personnelles, dans le cadre d'un traitement en cours ou prévu, vers un pays tiers ou à une organisation internationale, mais aussi les traitements ultérieurs du pays tiers destinataire vers un autre pays ou une autre organisation. Le texte de loi précise également qu'en plus des garanties appropriées, un transfert n'est autorisé qu'à condition que les personnes concernées disposent de droits opposables et de voies de droit effectives.

Enfin, la décision sur le caractère adéquat du niveau de protection d'un pays tiers appartient désormais à la Commission européenne, et non plus aux régulateurs locaux. Si le pays tiers n'est pas reconnu, mais que les garanties appropriées définies dans le règlement sont fournies, le responsable de traitement peut réaliser le transfert sans que cela ne nécessite une autorisation particulière d'une autorité de contrôle.

QUELS SONT LES CHANTIERS À METTRE EN OEUVRE ?

Mettre en place un processus de protection des données pour les transferts et les traitements ultérieurs

- Réaliser une cartographie de l'ensemble des transferts de données, ainsi que les informations requises (finalité, durée de conservation, transfert ultérieur…) et lister l'ensemble des obligations requises par le règlement
- Pour l'ensemble des pays non reconnus par la commission, se mettre en conformité en collectant l'ensemble des documents requis par le règlement (clause de protection des données, code de conduite, certification…)
- En cas de flux importants au sein d'un groupe, étudier la possibilité de mettre en place les BCR

Section 3

DATA PRIVACY OFFICER : INCARNER LA PROTECTION DE LA DONNÉE, DIFFUSER UNE CULTURE AU SEIN DE L'ENTREPRISE

DATA PRIVACY OFFICER : INCARNER LA PROTECTION DES DONNÉES, DIFFUSER UNE CULTURE AU SEIN DE L'ENTREPRISE

C'est dans un environnement complexe, à la croisée des exigences imposées par les régulateurs, d'une vélocité accrue des données, et de la volonté des entreprises de les exploiter, que le Data Privacy Officer trouve sa place : porteur du message de conformité, il embarque l'ensemble des directions dans un effort de régularisation du traitement des données à caractère personnel.

Un rôle à plusieurs facettes, pour un profil à la croisée des compétences juridiques et techniques

LE DPO, AU-DELÀ DU TITRE, UN ACTEUR MAJEUR DE LA DYNAMIQUE DE DATA MANAGEMENT

Qui est donc ce nouvel acteur ?

Nommé pour répondre aux nouvelles exigences règlementaires, le Data Privacy Officer n'est pas toujours un nouveau poste à créer. Cette fonction est nécessaire, d'autant plus pour des activités à forte densité de données et très règlementées, et les responsabilités sont nouvelles, mais les ressources sont parfois déjà là.

Quel profil pour le Data Privacy Officer ?

Faire **le lien** à tous les niveaux de l'organisation et y incarner **la culture de la protection de la donnée.**

Définir les processus à même de répondre aux exigences règlementaires

Avoir une **vision transversale de l'organisation** afin de capter les points de sensibilité

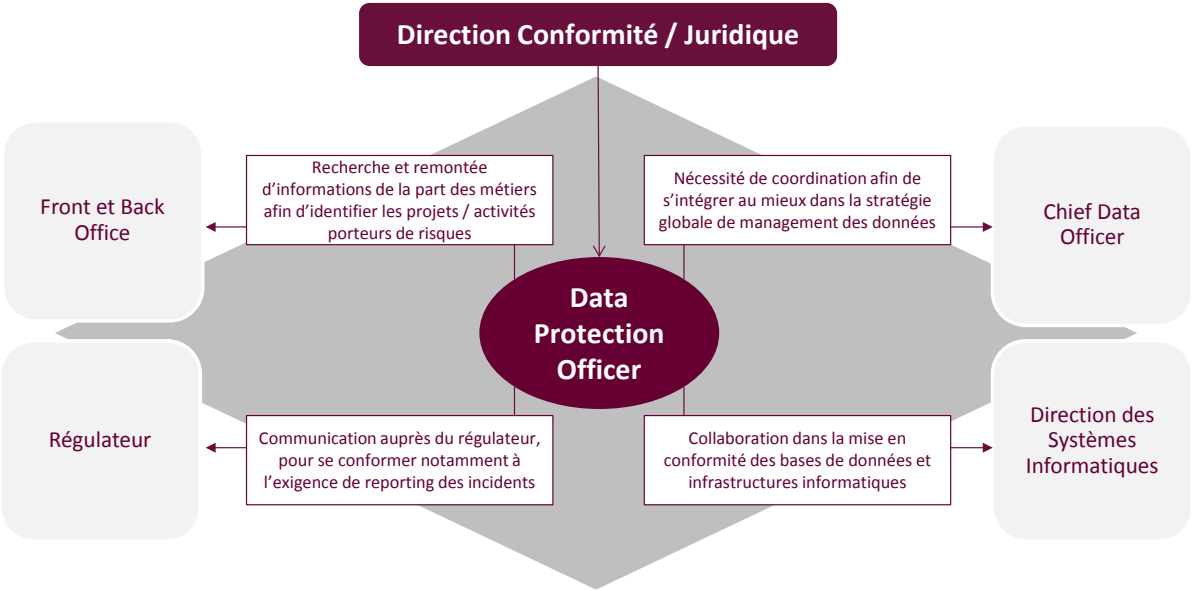
Comprendre et anticiper **les enjeux liées à l'exploitation de données** : règlementations, risques, sécurité, etc.

DATA PRIVACY OFFICER : INCARNER LA PROTECTION DES DONNÉES, DIFFUSER UNE CULTURE AU SEIN DE L'ENTREPRISE

Au centre de l'entreprise,

au plus près des évènements de risques

Parce les données sont de plus en plus nombreuses, volumineuses et diversifiées, le DPO occupera une fonction à responsabilité croissante. Par ailleurs, du fait du fond règlementaire des problématiques à adresser, le DPO doit être rattaché à la direction Conformité / Juridique. Cependant, il doit travailler en étroite collaboration tant avec la DSI qu'avec le responsable du Data Management.



Section 4

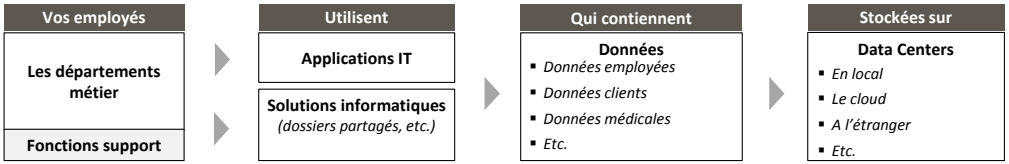
COMMENT SIA PARTNERS PEUT VOUS AIDER ?

NOTRE APPROCHE POUR SE PRÉPARER À L'ENTRÉE EN VIGUEUR DU GDPR

Avant de lancer un projet de cette envergure, c'est-à-dire qui concernera et impactera l'ensemble de votre entreprise, il est essentiel de mener un diagnostic afin d'identifier les chantiers prioritaires.

Comprendre votre exposition aux données à caractère personnel et sensible

Quel niveau d'exposition données à caractère personnel ?



L'environnement de travail décrit ci-dessus est porteur d'enjeux quant à la protection des données personnelles. Des enjeux que nous déclinons ci-dessous et qui sous-tendent les actions de mise en conformité à déployer au sein de votre entreprise dans l'optique du RGPD.

L'importance de réaliser un inventaire

Finalité	**Localisation**	**Source**	**Flux de données**
Classification	**Sécurité**	**Durée de rétention**	

Les enjeux en matière de localisation et de sécurité

Les données circulent constamment et rapidement à travers le globe. Elles sont stockées dans divers localisations qui sont soumises à des législations différentes en matière de sécurité des données ou de transfert des données (Safe Harbor)

Les demandes des clients et des régulateurs

Les régulateurs, tout comme les clients, peuvent demander le détails des informations personnelles collectées, traitées, transférées… Il est primordial pour les assureurs de mettre en place un processus efficace permettant de répondre au plus vite à ces demandes

" SIA PARTNERS VOUS PROPOSE DE RÉALISER UN DIAGNOSTIC DU NIVEAU DE MATURITÉ DE VOTRE DISPOSITIF EXISTANT "

NOTRE APPROCHE POUR SE PRÉPARER À L'ENTRÉE EN VIGUEUR DU GDPR

La phase de diagnostic

NOTRE MÉTHODOLOGIE EN 4 ÉTAPES

Nous vous proposons de réaliser un diagnostic en 4 étapes clés afin de définir une feuille de route et lancer un projet stable de mise en conformité

Phase de diagnostic

- **Identification des traitements et transferts effectués.**
  - *Comprendre où se trouvent les données que vous collectez et traitez*
- **Analyse du dispositif de protection existant**
  - *Comprendre les moyens existants pour mettre sous contrôle les risques de protection des données*
- **Analyse des écarts à la règlementation**
  - *Evaluer votre niveau de maturité pour prendre conscience des manquements et des développements à envisager*
- **Définition d'une feuille de route**
  - *Définir les grands chantiers à mener (yc la charge) au regard de la stratégie d'entreprise et du niveau de maturité actuel*

" TOUT AU LONG DE NOTRE AUDIT, NOUS ESSAYONS ÉGALEMENT DE SENSIBILISER NOS INTERLOCUTEURS AUX ENJEUX DE LA PROTECTION DES DONNÉES AFIN DE PRÉPARER LA CONDUITE DU CHANGEMENT "

Afin de faciliter le déroulement de ces audits, Sia Partners a développé un outil d'évaluation de votre dispositif de protection des données. Cet outil, déclinant votre performance selon 10 axes de travail d'étude, vous permettra de définir un plan d'action de mise en conformité et d'adresser ainsi efficacement les exigences du Réglement Général sur la Protection des Données

NOTRE APPROCHE POUR SE PRÉPARER À L'ENTRÉE EN VIGUEUR DU GDPR

Lancez un projet de mise en conformité adapté à vos besoins

La règlementation européenne change profondément la manière de traiter les données à caractère personnel. Les assureurs ont jusque mai 2018 pour se mettre en conformité, mais quelle approche doivent-ils adopter pour éviter à la fois de prendre du retard et de créer un organisation déséquilibrée ?

SE POSER LES BONNES QUESTIONS

1. Où se trouvent les données à caractère personnel et sensible que vous collectez ? Quelle est la finalité de leur collection ?
2. Avez-vous déjà mis en place un dispositif de protection des données ? (nomination d'un CIL, production d'une politique de protection des données, mise en place de contrôles, production d'un rapport annuel sur le niveau de maturité du dispositif et la définition de plans d'amélioration…)
3. Quel est votre niveau de maturité au regard de la règlementation actuelle ? Au regard du règlement général sur la protection des données ?
4. Quelle est votre stratégie d'utilisation des données ? (un minimum de collection possible pour réaliser ses activités versus une collection et exploitation approfondies de données dans le but de découvrir des opportunités potentielles)
5. Comment concevez-vous l'organisation de votre dispositif de protection des données ? (quel poste ou quelle direction portera le projet ?)

NOTRE APPROCHE POUR SE PRÉPARER À L'ENTRÉE EN VIGUEUR DU GDPR

Points d'attention et facteurs clés de succès

LES DIFFICULTÉS POTENTIELLES DE MISE EN ŒUVRE

- L'animation du dispositif :
  - Faire adhérer les employés au dispositif
  - Donner les moyens au DPO de dynamiser le dispositif
- La mise à jour continue de la cartographie des données et des processus
- La capacité des SI à répondre aux exigences règlementaires (droit à l'oubli)
- L'exigence en matière de documentation des preuves
- La récupération d'informations auprès des sous-traitants

FACTEURS CLÉS DE SUCCÈS

- Définir préalablement les données concernées, les processus impactés avant de lancer une phase projet sans avoir
- Lier les contraintes règlementaires en matière de protection des données et stratégie de l'entreprise
- Réfléchir à la mise en place d'un un dispositif pérenne
- Faire adhérer l'ensemble des employés au projet
- Eviter de traiter les articles du règlement séparément

SIA PARTNERS, UN CABINET DE CONSEIL EN MANAGEMENT DISPOSANT D'UNE PRÉSENCE GLOBALE

Sia Partners est le leader français indépendant des cabinets de conseil en management. Fort d'une équipe de consultants de haut niveau, nous accompagnons nos grands clients dans la conduite de leurs projets de transformation. Avec un portefeuille d'expertises de premier plan, nous apportons un regard innovant et des résultats concrets. Sia Partners est une partnership mondiale détenue à 100% par ses dirigeants.

1999
Date de création

140
M€ de CA en 2016

20
Bureaux

x2
La taille du cabinet a doublé en trois ans

Nos équipes

850+
Consultants

25+
Nationalités

21
Équipes Sectorielles & Transverses

Notre offre de services

15%
Stratégie

70%
Projets de transformation

15%
Stratégie IT & Digitale

Nos clients

230
Clients

7,000
Missions depuis notre création

20%
Des entreprises du Fortune 500

NOTRE OFFRE ASSURANCE

Des références dans toutes les branches du secteur

CHIFFRES-CLÉS

75%
du top 20 de l'Assurance client de Sia Partners

500
Missions Assurance depuis notre création

80+
Consultants dans 15 bureaux à travers le monde

PRINCIPALES OFFRES DE TRANSFORMATION

Se conformer aux réformes règlementaires et bonnes pratiques

- Directive Distribution
- GDRP / Protection des données personnelles
- LCB-FT
- Devoir de conseil
- Contrôle Interne
- Solvabilité 2

Concevoir et lancer de nouvelles offres

- Structuration de nouveaux produits / segments de clientèle
- Développement de nouveaux marchés
- Paiements mobiles, Développement multi-canal
- Digitalisation des processus

Optimiser ses processus / IT

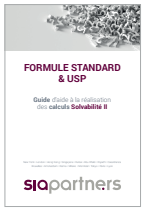
- Plans de productivité et d'efficacité opérationnelle
- Approches DILO / Lean Six-sigma
- Maitrise des processus et coûts IT
- Mise en place des démarches de professionnalisation et d'urbanisation

Data Management

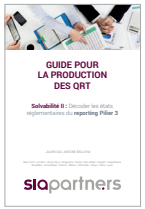
- Mise en place de dispositifs de data management (qualité des données, protection des données …)
- Data Science

NOS PUBLICATIONS

GUIDES PRATIQUES



Guide pour la production des QRT



Guide Formule standard et USP

Guide Conformité

CLUB

Club
Risques Opérationnels

Club
Conformité

PETITS DÉJEUNERS

Senior

Impacts IT

Solvabilité

Conformité …

NOTES

siapartners

Driving Excellence!

Abu Dhabi
PO Box 54605
West Tower #605
Abu Dhabi Mall - UAE
T. +971 4 443 1613

Amsterdam
Barbara Strozzilaan 101
1083 HN Amsterdam - Netherlands
T. +31 20 240 22 05

Bruxelles
Av Henri Jasparlaan, 128
1060 Brussels - Belgium
T. +32 2 213 82 85

Casablanca
14, avenue Mers Sultan
20500 Casablanca - Morocco
T. +212 522 49 24 80

Charlotte
401 N. Tryon Street, 10th Floor
Charlotte, NC 28202 - USA
T. +1 646 496 0160

Doha
PO Box 27774 Doha
Tornado Tower #2238
West Bay - Qatar
T. +974 4429 2524

Dubaï
PO Box 502665
Shatha Tower office #2115
Dubai Media City
Dubai - UAE
T. +971 4 443 1613

Hong Kong
23/F, The Southland Building,
48 Connaught Road Central
Central - Hong Kong
T. +852 2157 2717

Houston
4306 Yoakum Boulevard
Suite 350
Houston TX 77066
T. +1 832 248 1041

Londres
2nd Floor, 4 Eastcheap
London EC3M 1AE - United
Kingdom
T. +44 20 7933 9333

Luxembourg
7 rue Robert Stumper
L-2557 Luxembourg
T. +352 28 85 87 1

Lyon
3 rue du Président Carnot
69002 Lyon - France
T. +33 1 42 77 76 17

Milan
Via Gioberti 8
20123 Milano - Italy
T. +39 02 89 09 39 45

Montréal
2000 McGill College, Suite 600,
Montreal QC H3A 3H3 - Canada
T. +1 514 926-2626

New York
40 Rector Street, Suite 1111
New York, NY 10006 - USA
T. +1 646 496 0160

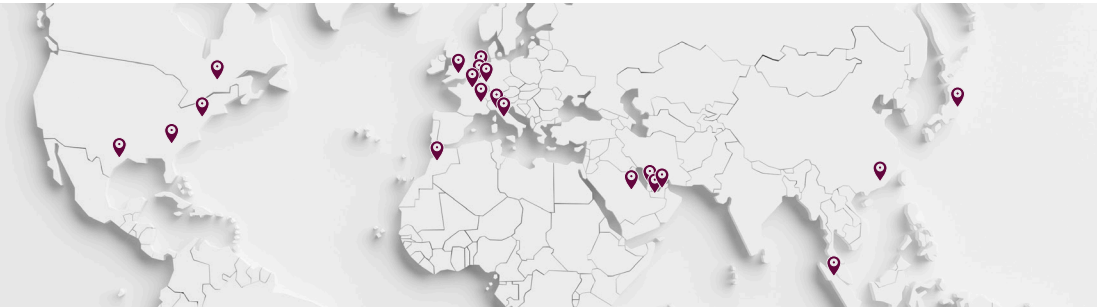
Paris
12 rue Magellan
75008 Paris - France
T. +33 1 42 77 76 17

Riyad
PO Box 502665
Shatha Tower office #2115
Dubai Media City
Dubai - UAE
T. +971 4 443 1613

Rome
Via Quattro Fontane 116
00184 Roma - Italy
T. +39 06 48 28 506

Singapour
137 Market Street #10-02
Grace Global Raffles
Singapore 048943
T. +65 6635 3433

Tokyo
Level 20 Marunouchi Trust Tower-
Main
1-8-3 Marunouchi, Chiyoda-ku
Tokyo 100-0005 Japan
T. +81 3 5288 5101



Suivez-nous sur **LinkedIn**

et **Twitter** **@SiaPartners**