Pioneer of Consulting 4.0

Protection des données personnelles : comment se mettre en conformité ?

siapartners

sia-partners.com

SOMMAIRE

Préambule

Le 25 mai 2018 est entré en application le **Règlement Général sur la Protection des Données (RGPD).** Tous les organismes privés et publics sont désormais soumis à un ensemble d'obligations, qui pour certaines, préexistaient sous l'égide de la Directive 95/46/CE et la loi dite « Informatique et Libertés ».

Parcours client et collecte de données : établir une relation de confiance

Cette réglementation impacte tous les processus d'entreprise dans la mesure où la donnée personnelle est un actif important. Si le RGPD vise à mieux encadrer la protection des données à caractère personnel de toutes les personnes concernées (clients, prospects, employés, prestataires, etc.), les enjeux sont particulièrement impactant sur la gestion client.

En effet, lors du parcours client, la collecte de données à caractère personnel est un atout : elle permet de mieux connaître la personne concernée et de lui adresser le produit ou service le plus adapté à ses besoins. En parallèle, **la valeur que le client** accorde à ses données personnelles progresse au fur et à mesure que le **caractère sensible** des données s'accentue, que leur périmètre s'élargit et que les bénéfices tirés de leur utilisation passent aux mains de l'entreprise.

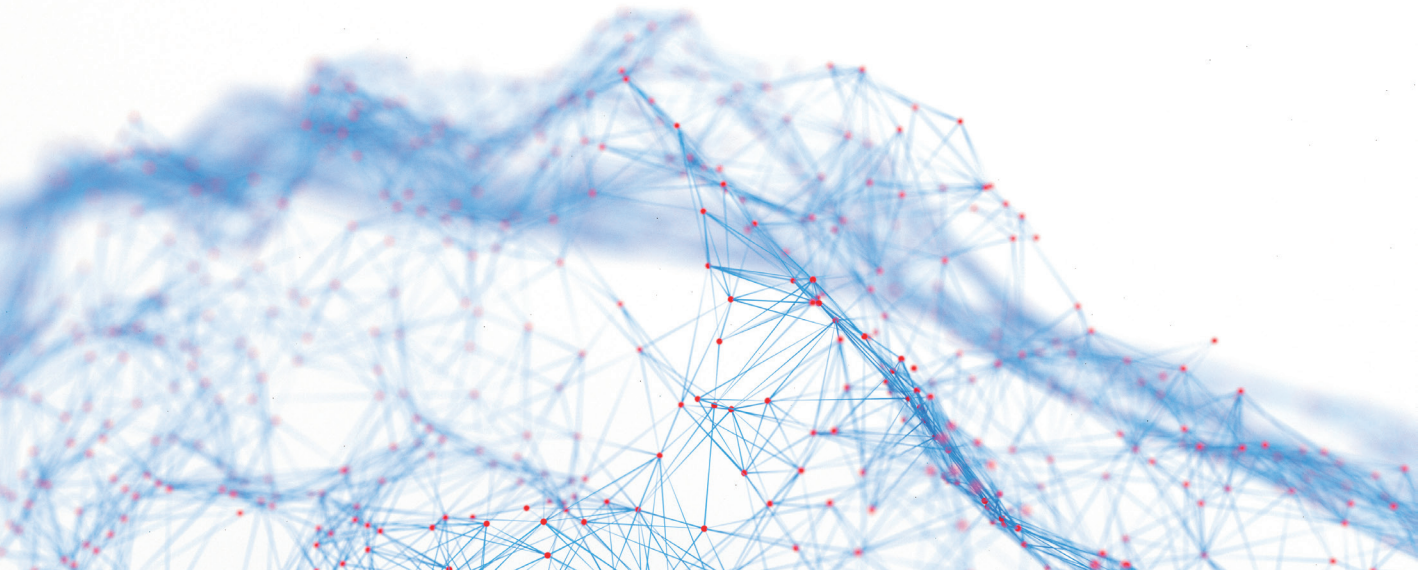
Les entreprises font donc face à un nouveau défi : concevoir des produits et des services de manière transparente, tout en maîtrisant le caractère confidentiel des données. Pour le client, cela se traduit par un prix adapté aux données qu'il a bien voulu donner, une information claire et transparente des usages de ses données par l'entreprise ainsi que la possibilité de les contrôler à tout moment.

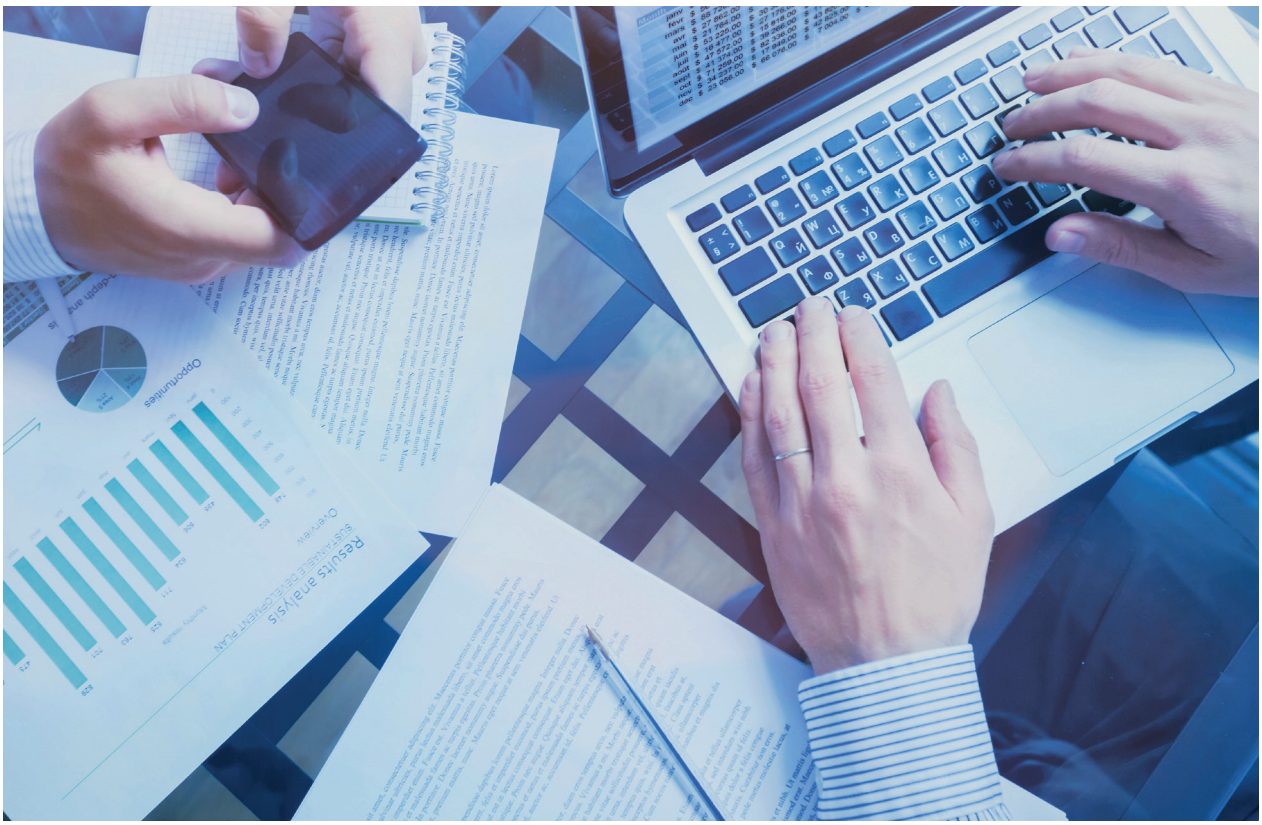
Des sanctions renforcées et des opportunités à saisir

Le risque de non-conformité est d'autant plus fort que les consommateurs sont de plus en plus attentifs à la protection renforcée de leur vie privée, au risque que l'entreprise perde des parts de marché et s'expose à un risque d'image fort. A celui-ci viennent s'ajouter un risque financier ainsi qu'un risque judiciaire (sanction pénale et réparations civiles).

L'entrée en application de ce nouveau règlement introduit un nouveau paradigme. Si avant mai 2018, la non-conformité constituait un risque maîtrisé, ce n'est désormais plus le cas. En effet, ne pas respecter le RGPD peut coûter jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires (amende administrative), le chiffre le plus élevé des deux étant retenu. Sans évoqué la perte de capital, chaque entreprise doit revoir son organisation, les règles régissant ses systèmes d'informations et ses processus, peu importe la localisation de son siège social à partir du moment où des données personnelles de résidents européens sont concernées.

Le présent document a pour objectif de vous accompagner dans la prévention, la gestion et la minimisation de l'ensemble des risques découlant d'une non-conformité à cette nouvelle réglementation.





Eléments de lecture du document

Une mise en conformité au RGPD nécessite de diviser le projet en **plusieurs chantiers.** Afin de faciliter la lecture du document, les chantiers projet associés à chacune des problématiques abordées sont identifiés en bas de page selon les visuels suivants :

Gouvernance, politique et procédures	**Gouvernance**
Registre des traitements	**Registre**
Analyses d'impact (PIA)	**PIA**
Privacy by design & by default	**PbD**
Gestion des droits des personnes	**Droits**
Communication interne & formation	**Formation**
Information et transparence	**Transparence**
Consentement	**Consentement**
Sécurisation IT	**Sécurité**
Gestion des tiers	**Tiers**
Conservation et suppression des données	**Conservation**

Plan détaillé

Section 1 : Le cycle de vie des données personnelles

Chaque organisme doit pouvoir encadrer la gestion des données personnelles de leur collecte à leur suppression et piloter leur utilisation.

1. La licéité des traitements de données personnelles ou comment justifier leur réalisation
2. La conservation et la suppression des données ou comment maitriser leur cycle de vie
3. Le registre des traitements, pierre angulaire du dispositif de conformité

Section 2 : La gouvernance de la protection des données

La règlementation impose un nouveau cadre d'entreprise lié à la protection des données personnelles. Cette gouvernance s'appuie sur un réseau d'acteurs dont les rôles et responsabilités sont clairement définis et communiqués à l'ensemble des collaborateurs des organismes. Celle-ci est particulièrement importante dans le cadre de la gestion des réponses à apporter aux demandes d'exercice de droits.

1. L'organisation interne autour de la protection des données : quels rôles et quelles responsabilités ?
2. La gestion des demandes d'exercice de droits : quel process mettre en place ?

Section 3 : La sécurité des systèmes d'information

Chaque organisme doit mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité de son système d'information adapté au niveau de risque auxquelles il s'expose.

La sécurité des systèmes d'information :

1. La gouvernance des systèmes d'information
2. Capitaliser sur la norme ISO27001 dans le cadre d'une mise en conformité RGPD
3. La gestion des violations de données à caractère personnel

Section 4 : La déclinaison opérationnelle du RGPD dans les organismes

Chaque organisme traite quotidiennement des données personnelles afin de répondre aux besoins de leurs clients et de développer leur place sur le marché. Il est toutefois nécessaire d'anticiper et encadrer les risques qui peuvent résulter de ces activités en gardant et en maitrisant le contrôle des données personnelles.

1. Information, transparence et contractualisation : quelles sont les obligations vis-à-vis des parties prenantes à vos activités ?
2. Le Privacy by design et by default et l'analyse d'impact : comment anticiper et atténuer les risques ?
3. La valorisation des données personnelles : quels points d'attention ?

SECTION 1 :
LE CYCLE DE VIE DES DONNÉES PERSONNELLES

La licéité des traitements de données personnelles ou comment justifier leur réalisation

“ Le consentement demeure l’une des six bases juridiques permettant de traiter des données à caractère personnel, telles qu'énumérées à l’article 6 du RGPD. Lorsqu’il entreprend des activités qui impliquent le traitement de données à caractère personnel, le responsable du traitement doit toujours prendre le temps d’examiner quelle serait la base juridique appropriée pour le traitement envisagé. ”

Lignes directrices sur le consentement au sens du Règlement 2016/679, Groupe de travail « Article 29 »

D’après **l’article 6 du RGPD**, tout traitement de données personnelles doit reposer sur une base légale. Cette base légale est à déterminer **par traitement**.

Comment déterminer la base légale d’un traitement ?

Le traitement est-il réalisé afin de se conformer à une obligation légale ? Existe-t-il un autre moyen que le traitement des données pour se conformer à cette obligation ?
Si non, la base est **l’obligation légale**.

Existe-t-il ou va-t-il exister un contrat avec la personne concernée ? Le traitement est-il nécessaire à l’exécution de ce contrat ou de la mesure précontractuelle ?
Si oui, la base est **l’exécution du contrat**.

Le traitement est-il réalisé afin de servir les intérêts commerciaux ou sociaux? Les personnes concernées peuvent-elles raisonnablement s’attendre à ce traitement ?
Si oui, la base est **l’intérêt légitime**.

Le traitement est-il réalisé dans le cadre d’une activité ou d’une fonction d’intérêt public ? L’activité ou la fonction est-elle qualifiée d’intérêt public par la loi ?
Si oui, la base est **l’intérêt public**.

Le traitement est-il réalisé pour protéger ou sauver la vie de la personne concernée? Une autre base légale est-elle envisageable ? En particulier, l’individu est-il en capacité de consentir au traitement de ses données ?
Si non, la base est **l’intérêt vital**.

L’utilisation d’une autre base légale est-elle possible ? Existe-t-il un déséquilibre des pouvoirs entre le Responsable de traitement et la personne concernée ?
Si non, la base légale est **le consentement**.

Dans certains cas, les traitements doivent faire l'objet d'un consentement explicite de la part de la personne concernée par ce traitement.

Comment collecter un consentement ?

Pour être **valide**, le consentement doit répondre à un certain nombre de conditions.

- Il doit être **donné librement,** c'est-à-dire qu'il ne peut pas conditionner l'accès à un service ou être donné dans le cas d'un déséquilibre des pouvoirs *(exemple : salariés)*.
- Il doit être **spécifique**. Le consentement n'est valable que pour une seule finalité *(exemple : prospection commerciale par voie électronique)*.
- Il doit être **éclairé,** c'est-à-dire précédé d'une mention d'information sur le traitement.
- Il doit être **univoque,** formalisé par une case à cocher ou une déclaration écrite.

Quand collecter un consentement ?

Il n'existe pas de liste réglementaire des traitements devant faire l'objet d'un consentement préalable.

Toutefois, certains traitements doivent obligatoirement être consentis comme par exemple : la **prospection commerciale** par voie électronique à destination de prospects, le **profilage** automatique et les traitements portant sur des **données sensibles** sauf exceptions.

Comment tracer un consentement ?

Quatre éléments sont nécessaires pour réussir à tracer un consentement : l'identité de la personne, la finalité du traitement pour lequel elle a consenti, la date de consentement et sa source. Ces éléments doivent être indiqués dans le registre des consentements.

Quelle association avec le droit d'opposition ?

Si le droit d'opposition n'est pas une base légale au même titre que le consentement, il est important de rapprocher ces deux principes. En effet, le retrait du consentement et l'opposition entrainent tous deux l'arrêt des traitements des données personnelles associées. Il est donc opportun d'adresser ces 2 enjeux ensemble, notamment lors de la revue des processus touchant le SI.

LES QUESTIONS À SE POSER POUR BIEN GÉRER LE CONSENTEMENT DANS LES SYSTÈMES D'INFORMATION

Qui donne son consentement ? (Par exemple, M. Dupont)
Pour quoi le consentement est-il donné ? (Par exemple, l'inscription à la newsletter)
Sur quel canal le consentement est-il donné ? (Par exemple, via le site internet)
A quelle occasion le consentement est-il donné ? (Par exemple, lors de l'achat d'un produit)
Comment le consentement est-il donné ? (Par exemple, une case à cocher)
Comment le consentement est-il retiré ? (Par exemple, un lien « se désinscrire »)
Pendant combien de temps le consentement est-il valide ? (Par exemple, trois ans à partir du dernier contact)

L'essentiel

La licéité des traitements de données personnelles ou comment justifier leur réalisation

Problématiques

Un traitement ne peut être mené que s'il est **licite**, le responsable de traitement, doit donc s'assurer que tout traitement dispose d'une base légale afin que celui-ci soit réalisé. Dans le cas contraire, il est nécessaire de **collecter le consentement** des personnes concernées.

Enjeux

S'assurer que les traitements réalisés par le responsable de traitement sont justifiés et limités au strict nécessaire.
Renforcer le **capital confiance** de ses clients.

Recommandations

Identifier les consentements devant être recueillis par obligation légale ou par exécution du contrat puis identifier les bases légales pour chacun des autres traitements.

Justifier l'intérêt légitime à réaliser des traitements lorsque cette base légale est utilisée.

LES PREUVES DE MISE EN CONFORMITÉ / " DOSSIER D'ACCOUNTABILITY "

Registre des consentements

Ce registre trace les consentements collectés par l'entreprise et doit faire apparaitre :

- La **personne** à laquelle est rattachée le consentement (ex : ID1234, M. DUPONT)
- La **finalité** pour laquelle le consentement est donné (ex : prospection commerciale)
- La **date** de collecte du consentement (ex : 01/01/2019)
- La **source** de collecte (ex : case à cocher sur le devis en ligne)

Notes justificatives de l'intérêt légitime

Ces notes, à réaliser pour chaque traitement reposant sur l'intérêt légitime, doivent comporter :

- La **qualification** de l'intérêt de l'entreprise, sa **licéité** et sa **transparence**
- Le caractère **nécessaire** du traitement pour répondre aux intérêts de l'entreprise
- Une **mise en balance** de l'intérêt avec la possible atteinte dudit intérêt aux droits et libertés des personnes concernées

Dossier explicatif sur la gestion informatique du consentement

Ce dossier doit expliquer en quoi l'entreprise est capable de tracer l'obtention d'un consentement ainsi que son retrait. Il doit comprendre :

- Les **systèmes d'opt-in** utilisés (case à cocher)
- La **remontée** de l'information dans les applicatifs
- La **visualisation** sur les applicatifs du consentement

La conservation et la suppression des données ou comment maitriser leur cycle de vie

Pour chaque document contenant une ou des données à caractère personnel, une **durée de conservation doit être définie** dans une politique de conservation et **appliquée** aussi bien dans les systèmes d'information et que sur la gestion des archives papiers.

Une durée de conservation limitée

Comment sont déterminées les durées de conservation ?

Cas 1 : La durée de conservation est définie par la loi. Exemple : les données d'identification à des fins de prospection commerciale sont conservées 3 ans à compter de la dernière communication émanant du prospect.

Cas 2 : La loi est silencieuse. Dans ce cas, la durée de conservation est définie par le responsable de traitement en fonction de ses besoins.

Comment organiser le cycle de vie des données ?

Base courante : les données sont conservées dans cette base à partir de leur collecte jusqu'à la fin de leur utilisation courante. Pendant cette période, le responsable de traitement doit mettre en place des mesures de sécurité standards.

Archives intermédiaires : cette base conserve les données utiles administrativement, notamment en cas de contentieux. L'accès à cette base doit être particulièrement restreint.

Archives définitives : il s'agit de la mise en œuvre du sort final. Si les données ne sont pas supprimées, elles peuvent être anonymisées et conservées dans cette base. La conservation devient alors illimitée.

Le cas des données non structurées

Qu'est-ce qu'une donnée non structurée ?

Les données non structurées sont des données qui ne sont pas contenues dans une base de données ou toute autre type de structure : mails, documents PDF, images, présentations, enregistrements audios, vidéos, etc.

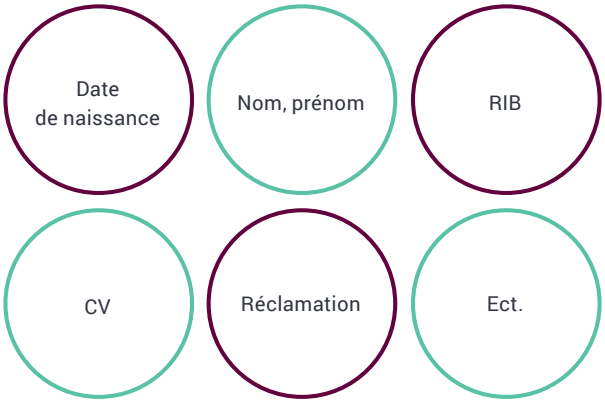
Où sont localisées les données non structurées ?

Deux catégories d'environnements peuvent contenir des données non structurées :

- **Environnements informatiques de l'utilisateur** (documents enregistrés sur l'ordinateur, e-mails reçus, etc.)
- **Environnements partagés** (intranets, espaces collaboratifs, etc.)

Comment respecter les durées de conservation des données non structurées?

Il est indispensable de faire une recherche de **mots clés** au sein des différents environnements pour retrouver les documents contenant des données personnelles. Cette opération doit être renouvelée régulièrement.



La durée de conservation varie selon les différentes finalités. Ainsi, la conservation d'une même donnée peut varier en fonction des objectifs poursuivis par les traitements qui l'utilisent.

L'essentiel

La conservation et la suppression des données ou comment maîtriser leur cycle de vie

Problématiques

Pour chaque document contenant des **données à caractère personnel,** une durée de conservation doit être définie.
Il est nécessaire d'identifier le lieu de stockage des données personnelles quelque soit son support, ainsi que de déterminer si les documents font l'objet d'une durée de conservation définie par la loi.

Enjeux

S'assurer que les durées de conservation des données, définies par le responsable, sont alignées avec la réalité opérationnelle pour ne **purger que les données** dont le traitement n'est plus un besoin afin de mener son activité. Aussi, s'assurer que la durée de conservation retenue soit la plus longue afin de répondre à toutes les exigences (plusieurs durées de conservation possibles pour une même donnée faisant l'objet de plusieurs traitements).

Recommandations

Poser les principes des **données à archiver et à purger,** en identifiant par application du SI les données interrogées pour réaliser chaque traitement.
Faire de la sensibilisation auprès des collaborateurs pour la suppression des données non structurées.

LES PREUVES DE MISE EN CONFORMITÉ

Politique et procédure de conservation et d'archivage

Cette procédure doit comporter :

- Une description des **règles à appliquer** en matière de conservation, archivage et suppression des données
- Les **rôles et responsabilités** associés (DPO, DSI, etc.)
- **Les modes opératoires** liés à la détermination de la durée de conservation et son application

Référentiel de durées de conservation

Ce référentiel doit présenter pour chaque traitement réalisé :

- La **typologie de conservation** (archive courante, intermédiaire ou définitive)
- La **durée** de conservation associée
- Ce référentiel peut faire partie intégrante du **registre des traitements**

Plan de purge

Un plan de purge doit être mis en place et expliquer :

- Quelles données seront supprimées (données liées aux opérations marketing, à la vie du contrat, etc.)
- Comment elles seront supprimées (suppression automatique ou manuelle)
- Où elles seront supprimées (applicatifs, dossiers papiers, etc.)

Le registre des traitements, pierre angulaire du dispositif de conformité

Sauf exceptions, les organismes de plus de 250 salariés ont l'obligation de consigner les traitements dans un document appelé « registre des traitements ». Ce document n'est pas qu'une obligation : il permet d'avoir une vision d'ensemble sur les actions à mettre en œuvre pour être en conformité. Il doit être appréhendé comme un outil de pilotage et géré de manière dynamique.

Les caractéristiques à indiquer pour piloter sa conformité

- Finalité
- Département/Service
- Activités liées
- Source
- Catégories de personnes
- Catégories de données
- Données sensibles
- Transferts internes
- Transferts externes
- Transferts hors UE
- Stockage
- Conservation des données
- Sécurité
- Base légale
- Modalités d'exercice des droits

Les bonnes pratiques à suivre pour construire le registre

Définir une méthodologie au sein du groupe.

Si l'organisme fait partie d'un groupe d'entreprise, utilisez la méthodologie du groupe

Définir une méthodologie d'identification adaptée à la structure de l'entreprise et ses activités en limitant le nombre de traitements

Définir un nombre limité de traitements par entité mais cohérent avec les activités permet de garantir une granularité suffisamment large et compréhensible pour les personnes concernées, tout en évitant de noyer d'informations les acteurs

Prioriser l'identification des traitements en fonction des données traitées et des sensibilités associées

Identifier par interview les macro traitements et tâches réalisés, identifier les traitements de DCP et définir la finalité des traitements

Contrôler la cohérence et l'exhaustivité des traitements identifiés

Vérifier la cohérence des flux des données et l'intérêt afin de garantir la sécurité des données et l'identification de l'ensemble des macro traitements

L'essentiel

Le registre des traitements, pierre angulaire du dispositif de conformité

Problématiques

Toute manipulation de données personnelles, ou traitement, est inscrit et intégré au registre des traitements. Celui-ci doit être tenu à jour par les opérationnels sous la responsabilité du responsable de traitement.
Dans l'approche de Sia Partners, la réalisation du registre est la première action à effectuer pour se mettre en conformité.

Enjeux

Définir la granularité du registre afin d'homogénéiser le document. Le registre peut être un outil central de pilotage des chantiers identifiés au sein de l'organisme.

Recommandations

- Renseigner le registre des traitements avec une vision process et outils.
- Définir un nombre limité de traitements par entité mais cohérent avec les activités.
- Identifier la documentation la plus à jour (cartographie des SI, processus, risques).
- Définir une procédure de mise à jour du registre.

Comment construire son registre des traitements ?

Utiliser un **logiciel tableur** dont l'organisme a l'habitude

Compléter le registre en **atelier** avec le DPO et le Correspondant métier

Faire apparaitre chaque **direction/département** de manière distincte

SECTION 2 :
LA GOUVERNANCE DE LA DONNÉE PERSONNELLE

L'organisation interne autour de la protection des données : quels rôles et quelles responsabilités ?

Différents acteurs peuvent intervenir dans le dispositif de protection des données personnelles. Chacun de ses acteurs a des rôles bien identifiés.

Les différentes fonctions à mettre en place

Le Délégué à la Protection des Données (DPO)

Le DPO sera le chef d'orchestre de la conformité au RGPD. Tous les organismes n'ont pas pour obligation d'en nommer un (cf. Lignes directrices du G29 sur le DPO), mais une telle nomination participe à démontrer la bonne foi d'un organisme à respecter la réglementation. Il est aussi possible de nommer un référent interne qui ne sera pas déclaré à la CNIL.

Le DPO participe à l'application de toutes les obligations :

- Gérer les droits des personnes
- Accompagner et valider les analyses d'impacts sur la vie privée (PIA)
- S'assurer de la mise à jour du registre des traitements
- Assurer la formation des collaborateurs
- Piloter le plan d'actions de mise en conformité de l'entité
- S'assurer de la prise en compte du privacy by design et by default

Pour assurer le respect de ces obligations, il va également définir et présenter la **politique de protection des données personnelles** aux entités, coopérer avec l'autorité de contrôle, piloter et coordonner les travaux des relais DPO et consolider les reportings et les présenter aux dirigeants.

Le relai DPO

Positionnés dans chaque direction de l'entreprise, des relais DPO peuvent être identifiés par des organismes dont la taille ou les activités le nécessiteraient. Celui-ci aura un rôle fonctionnel.

Il doit être le support du DPO dans son domaine métier afin de s'assurer de la prise en compte du RGPD dans l'ensemble des activités de l'entreprise. Les domaines concernés peuvent être les suivants :

- Direction Marketing
- Direction Client
- Direction Juridique
- Direction des Systèmes d'Information
- Direction des Ressources Humaines
- Direction du Contrôle Interne
- Direction de la Communication
- Direction Financière

Le cas des groupes d'entreprises

Un DPO peut être nommé pour un seul et même groupe d'entreprises. Dans ce cas, il doit être assisté par des référents positionnés dans chacune des entités.

La possibilité de mutualisation

Plusieurs entreprises d'un même secteur peuvent mutualiser leur DPO. Il est toutefois indispensable que chacune des entreprises accordent des moyens équivalents pour que le DPO puissent exercer ses missions.

Les formations et sensibilisations à dispenser

DPO : il doit être formé à l'ensemble des sujets relatifs à la conformité des traitements de données personnelles, ainsi qu'aux outils et techniques de management et de suivi de conformité

Relais DPO : ils doivent être particulièrement formés au privacy by design et à l'analyse d'impact, à la gestion des tiers, à l'information et à la conservation des données.

Métiers impactés : les directions projets doivent être formées au privacy by design, le marketing au consentement, le juridique et les achats à la gestion des tiers, et les services clients à la gestion des droits.

Totalité des collaborateurs : tous les collaborateurs doivent être sensibilisés à la protection des données et à la sécurité, en particulier aux bonnes pratiques de confidentialité.

L'essentiel

L'organisation interne autour de la protection des données : quels rôles et quelles responsabilités ?

Problématiques

Le RGPD consacre de nouveaux acteurs, dont le Data Protection Officer (DPO) est le principal dans la logique de responsabilisation voulue par le RGPD. Tous les collaborateurs doivent être sensibilisés pour pérenniser le dispositif.

Enjeux

Définir une gouvernance des données personnelles au sein de l'organisme de façon à ce que ce réseau d'acteurs, en soutien du DPO, aient des rôles et des responsabilités clairement définis et communiqués à l'ensemble des collaborateurs.

Recommandations

Définir différents acteurs pouvant intervenir dans le dispositif de protection des données personnelles, ainsi que leur rôle.

Adapter la formation à chaque population et à leur rôle dans la protection des données.

LES PREUVES DE MISE EN CONFORMITÉ

Politique de protection des données

- Description des grands principes à respecter
- Description des rôles et responsabilités, ainsi que de la comitologie
- Déclaration CNIL de nomination du DPO et liste des relais

Supports et suivi des formations

- Feuilles d'émargement prouvant la présence à la formation
- Plan de formation décrivant les cibles, le contenu des formations et leurs modalités

La gestion des réponses aux demandes d'exercice de droits : quel process mettre en place ?

Une attention particulière doit être portée par le responsable de traitement concernant les demandes d'exercice de droits. En effet, le non respect de cette obligation est passible de la sanction la plus élevée et n'est pas toujours priorisé dans les plans d'action de mise en conformité.

Les droits des personnes concernées

Droit d'accès : La personne concernée peut accéder à ses données.

Droit de rectification : La personne concernée peut demander que ses données soient corrigées ou complétées.

Droit d'opposition : La personne concernée peut demander à tout moment que ses données personnelles ne soient pas/plus traitées. Exemple : une personne peut se désinscrire de la newsletter de l'organisme et ne devra plus recevoir de telles communications.

Droit à l'oubli : La personne concernée a droit à ce que ses données soient effacées.

Droit à la limitation : La personne concernée peut demander que le traitement des données personnelles la concernant soit verrouillé pendant un certain temps.

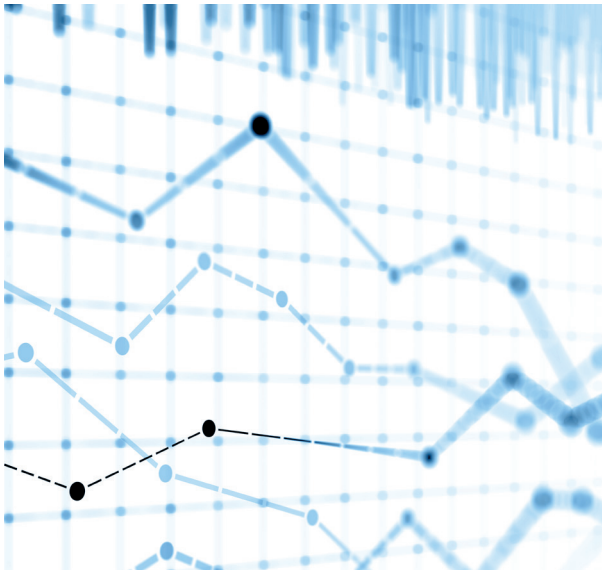
Droit à la portabilité : La personne concernée a le droit d'obtenir ses données personnelles dans un format qui lui permettra de les transmettre à un autre responsable de traitement.

Retrait du consentement : La personne concernée peut retirer le consentement précédemment accordé au traitement de ses données personnelles.

Sort post-mortem : La personne concernée peut décider du sort de ses données personnelles en cas de décès.

Les bonnes pratiques pour répondre à une demande

1. Créer une **structure** qui reçoit, contrôle et suit les demandes des personnes concernées
2. Créer un **formulaire** spécifique aux demandes de droits
3. Associer une **adresse mail** aux seules fins de la réception des demandes d'exercice de droits
4. **Informer** les personnes concernées de leur droits et des modalités d'exercice de leurs droits
5. Etablir un processus de **collecte des informations** nécessaires pour répondre et centraliser l'envoi des réponses
6. Respecter les **délais** et prévenir les personnes concernées en cas de difficulté de réponse
7. **Réviser** la procédure appliquée sur la base du flux de demandes reçues
8. Etablir au préalable la **liste des traitements** pouvant faire l'objet de demandes d'exercice de droits



L'essentiel

La gestion des réponses aux demandes d'exercice de droits: quel process mettre en place?

Problématiques

Le RGPD instaure de **nouveaux droits** et raccourci les délais de réponse, ce qui oblige les entreprises à définir précisément le processus à suivre pour répondre à ces demandes.

Enjeux

Mettre en place un **processus efficace** permettant de respecter le délai de 1 mois et donner aux personnes des **modalités pratiques** pour qu'elles exercent leurs droits facilement.

Recommandations

- Accuser réception lorsqu'une demande est reçue.
- Dissocier la procédure concernant les clients de celle concernant les salariés.
- Créer un formulaire ou une adresse mail dédiée.

Quel processus de réponse mettre en place ?

Délai de traitement : 1 mois (3 mois en cas de demande complexe)

1. Emission d'un accusé réception à la réception de la demande
2. Qualification de la demande (catégorie de droit exercé)
3. Réalisation de la demande (compilation des données, arrêt des traitements, etc.)
4. Rédaction de la réponse et contrôle du DPO
5. Expédition de la réponse

LES PREUVES DE MISE EN CONFORMITÉ

Utiliser un tableau de suivi

- Nom du demandeur et coordonnées
- Personne en charge de la réponse
- Format de la demande
- Date de réception de la demande
- Date d'accusé réception
- Date d'échéance
- Date de réponse
- Statut de la demande

Utiliser des courriers types de réponse

- Courriers d'accusé de réception
- Courriers de rallongement du délai
- Courriers dédiés au droit d'accès avec consolidation de données
- Courriers de confirmation du traitement des demandes autres que les demandes d'accès.

SECTION 3 :
LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

La sécurité des systèmes d'information

Le niveau de sécurité des systèmes d'information que les entreprises doivent mettre en place dépend de l'exposition aux risques de ces dernières. L'adoption du Cybersecurity Act par l'Union Européenne devrait à terme obliger les organismes à afficher leur niveau de sécurité de manière aussi simple et intelligible que ce qui est pratiqué en matière d'étiquetage alimentaire ou phytosanitaire.

Comment évaluer mon exposition à la sécurité des systèmes d'information ?

Est-ce que je traite des données critiques ?

D'un point de vue RGPD, le risque d'exposition sera plus élevé si vous traitez des données sensibles : données de santé, données génétiques ou biométriques, données philosophiques ou politiques, etc.
Le niveau de risque prend compte aussi du volume de données personnelles traitées par l'entreprise ainsi que de la fréquence d'utilisation des données.

Quel sera l'impact sur mon entreprise en cas de perte de confidentialité des données ?

La divulgation des informations peut n'avoir aucune incidence sur l'entreprise, en particulier lorsque les informations traitées sont publiques. Lorsque les informations divulguées sont uniquement réservées à une utilisation interne et professionnelle, l'impact sera en général assez faible. En revanche, les données accessibles uniquement à un groupe limité de personnes, voire à un groupe très restreint de personnes, doivent bénéficier d'une sécurité renforcée car leur divulgation pourrait avoir un impact très fort sur l'entreprise.

Quel sera l'impact sur mon entreprise en cas de perte d'intégrité des données ?

L'exposition dépendra des impacts résultant de la véracité d'une information ou de sa falsification. Au mieux, l'information peut être fausse sans avoir de conséquences. Dans le pire des cas, la donnée falsifiée peut engendrer des risques de fraude à fort impact financier, voire des impacts de non-conformité réglementaire.

Quel est mon besoin de disponibilité du service et disponibilité des données ?

Les mesures de sécurisation du SI dépendent également de la durée d'indisponibilité du service que vous pouvez accepter. L'exposition ne sera pas la même si le service est indispensable pendant moins d'une semaine ou moins d'une demi-journée.

Comment les données sont-elles stockées ?

Le lieu de stockage a une incidence sur le niveau d'exposition au risque. Ainsi, lorsque le stockage des données s'effectue au sein du SI de l'entreprise l'exposition est moindre que lorsque l'entreprise fait appel à hébergeur tiers cloud.

Comment les données sont-elles transmises ?

Les risques seront différents si les données transitent uniquement sur le réseau d'entreprise et/ou , sur internet, et/ou sur le réseau de vos partenaires. Aussi, le risque sera plus faible si les traitements de données sont effectués par batch (enchaînement automatique d'une suite de commandes), lesquelles alimentent d'autres systèmes en interne, que si ces données font l'objet d'impressions.

Pourquoi mettre en place des mesures de sécurité IT?

Les risques qui ne sont pas couverts par des mesures de sécurisation IT peuvent entraîner des impacts significatifs :

- Impacts financiers
- Impacts d'image
- Impacts sur vos effectifs internes (confiance des salariés)
- Impacts règlementaires, notamment vis-à-vis du RGPD

La gouvernance des systèmes d'information

Renforcer la gouvernance des SI consiste à s'assurer que le dispositif de sécurité répond aux exigences réglementaires et est adapté au risque lié à la donnée manipulée par l'organisation. Elle permet également de s'assurer que les exigences de sécurité déterminées par l'organisation sont bien respectées mais également de la mise à jour des connaissances sur l'évolution des normes et pratiques professionnelles.

Classifier l'information et marquer les documents

Les actions et les niveaux de sécurité seront plus ou moins forts selon la classification des informations concernées. Il est donc nécessaire de définir plusieurs niveaux de confidentialité :

- **Public :** informations publiques, non-confidentielles qui peuvent circuler librement en interne comme en externe
- **Interne :** informations qui peuvent circuler librement dans l'entreprise
- **Restreint :** informations qui ne doivent être communiquées (même à l'intérieur d'une entreprise) qu'aux personnes directement concernées, et n'être manipulées que par des personnes précisément identifiées
- **Confidentiel :** informations dont la divulgation pourrait porter atteinte aux intérêts, à la sécurité ou même à l'existence des personnes concernées

Les documents doivent faire l'objet d'un **marquage.**

Quelles mesures mettre en place pour assurer le respect de la confidentialité ?

Afin d'être en capacité d'apporter la preuve du bon usage des systèmes d'information et afin de prévenir tout usage illicite de ceux-ci, il est recommandé de mettre en place un certain nombre de mesures.

- **Traçabilité :** outils permettant de tracer les activités du système d'information, notamment grâce à des journaux de connexion – logs
- **Filtrage :** outils permettant d'analyser les conditions d'utilisation des moyens informatiques, d'interdire tel ou tel protocole, et de restreindre certaines catégories de sites internet ou d'application
- **Contrôle de l'utilisation des outils informatiques :** contrôler la présence de mots clés dans des documents ou contenus grâce à des outils informatiques

Attention, il est nécessaire que les employés soient **informés** de la mise en place de telles mesures. Cette information peut notamment se faire à travers la charte informatique de l'entreprise.

Quels acteurs doivent être impliqués?

Une multitude d'acteurs d'entreprise doit être impliquée dans un projet de sécurisation IT.

- **Direction des systèmes d'information** (Architectes, Gestion de la donnée, etc.)
- **Responsable de la Sécurité des Systèmes d'Information**
- **Ressources Humaines** (Formation, Contentieux, etc.)
- **Contrôle et Audit Interne**
- **Affaires Juridiques**
- **Délégué à la Protection des Données**

Capitaliser sur la norme ISO27001 dans le cadre d'une mise en conformité RGPD

La sécurité des systèmes d'information est une obligation issue du RGPD. Toutefois, la réglementation **reste vague** en la matière. Ainsi, la norme ISO27001 peut constituer une base solide relative à la sécurité, au même titre que les actions engagées dans le cadre de la Loi de Programmation Militaire.

Comment utiliser la norme ISO27001 pour se mettre en conformité avec le RGPD ?

Le Guide de la sécurité des données personnelles de la CNIL présente 17 chantiers permettant d'assurer la sécurité des données personnelles qui répondent à 7 enjeux :

- Renforcer la protection du réseau IT
- sécuriser les échanges d'informations
- Améliorer la protection des postes de travail et applications mobiles
- Gérer la durée de conservation dans les systèmes d'information
- Mettre en place un dispositif d'anonymisation des données
- Encadrer la sécurité dans le développement et la maintenance informatique
- Accompagner le changement pour les collaborateurs

Un cadrage ISO27001 permet **d'enrichir** les actions liées à ces 17 chantiers ainsi que de **repositionner les priorités.**

Quels chantiers peuvent être mutualisés entre un projet RGPD et un projet ISO 27001?

Si ISO 27001 a un champ d'application plus large car elle ne concerne pas seulement les données personnelles, la norme dispose de plusieurs chantiers communs avec le RGPD qui peuvent être mutualisés :

- Sécurisation IT
- Conservation et suppression des données
- Communication interne et formation
- Gouvernance, politique et procédures
- Gestion des tiers
- Privacy by design
- PIA

Les documents et actions pouvant répondre aux 2 réglementations

Politique de sécurité IT / Politique de protection des données

Plan de traitement des risques / Plan d'action PIA

Formation Sécurisation / Protection des données

Procédure de gestion des incidents / Procédure de violations de données

Méthodologie d'évaluation des risques / Méthodologie PIA

Propriétaires des actifs / Propriétaires des traitements

Programme d'audit ISO27001 / Protection des données

Politique de sécurité des fournisseurs / Procédure de gestion des sous-traitants

La gestion des violations de données à caractère personnel

L'article 33 du RGPD impose aux organismes de notifier à la CNIL toute violation de données à caractère personnel, et dans certains cas, d'en informer également les personnes concernées par les traitements.

Comment qualifier une violation de données personnelles ?

- Perte de **confidentialité** (accès non autorisé ou divulgation)
- Perte **d'intégrité** (modification non désirée)
- Perte de **disponibilité** (disparition des données)

Comment évaluer le risque d'atteinte à la vie privée ?

Le responsable du traitement évalue le risque généré par la violation en s'appuyant sur les critères suivants :

Ainsi, le risque pourra être de quatre ordres : absent, indéfini, présent ou élevé.

Quand doit-on notifier la violation de données ?

Dans le cas où la violation engendre un risque indéfini, présent ou élevé, il est nécessaire de **informer la CNIL** de cette violation. Dans le cas où le risque est élevé, il faut également **notifier les personnes** dont les données ont fait l'objet de la violation.

Cette notification doit avoir lieu dans les **72h** suivant la détection de la violation.

Dans tous les cas, et peu importe le niveau de risque, la violation doit être consignée dans un registre dédié tenu par le DPO.

L'essentiel

La sécurité des systèmes d'information

Problématiques

Le RGPD oblige les entreprises à assurer une sécurité physique et organisationnelle des données personnelles qu'elles traitent. Aussi, le niveau de sécurité doit dépendre de la sensibilité des données traitées.

Enjeux

Mettre en place **des mesures de sécurité suffisantes** malgré un manque de clarté du RGPD en la matière.
Être en capacité de détecter une violation de données personnelles et de la notifier à l'autorité de contrôle.

Recommandations

Capitaliser sur des projets de sécurisation IT d'ores-et-déjà lancés (ISO27001, Loi de programmation militaire, etc.).
Utiliser le dispositif de remontée des incidents pour identifier les violations de données personnelles

Quel processus de réponse mettre en place ?

Délai de traitement : 72h

LES PREUVES DE MISE EN CONFORMITÉ

Procédure de gestion des violations de données

- Description des rôles et responsabilités liés à la gestion des violations de données
- Mise en place d'une échelle d'évaluation des risques afin de déterminer si l'entreprise doit notifier la violation et à qui

Registre des violations de données

Créer un tableau devant être géré par le DPO et comportant les éléments suivants :

- Nature et date de la violation de données
- Catégories et nombre approximatif de personnes et de données concernées
- Mesures de remédiation
- Date de notification ou justification d'absence de notification

SECTION 4 :
LA DÉCLINAISON OPÉRATIONNELLE DU RGPD DANS LES ORGANISMES

Information, transparence et contractualisation : quelles sont vos obligations vis-à-vis des parties prenantes à vos activités ?

Information et transparence

L'article 12 du RGPD précise que « Le responsable de traitement prend des mesures appropriées pour fournir toute information (…) qui concerne le traitement à la personne concernée »

Qui fournit l'information ?

La fourniture de l'information relative au traitement est à la charge du **responsable de traitement.**

En cas de responsabilité conjointe, l'information doit être fournie soit par l'un des deux responsables de traitement soit par chacun des responsables de traitement pour leur périmètre respectif.

En cas de sous-traitance, il est possible de déléguer l'obligation d'information au sous-traitant par le biais du contrat. L'information doit toutefois être donnée au nom du responsable de traitement.

Dans tous les cas, les actions liées à l'information doivent être définies dans le contrat.

Quand fournir l'information ?

La fourniture de l'information dépend du **type de collecte** des données.

En cas de collecte directe, l'information doit être donnée au moment de la collecte (ex : formulaires d'adhésion, formulaire de contact, etc.).

En cas de collecte indirecte, l'information doit être donnée au plus tard 1 mois après la collecte ou lors de la première communication (ex : mailing de prospection commerciale envoyé à partir de coordonnées achetées).

Quelles informations fournir ?

Les personnes concernées doivent être informées des **caractéristiques des traitements et de leurs droits.**

- L'identité du responsable de traitement, les catégories de destinataires des données et les transferts de données hors EEE ;
- Les finalités du traitement, la base légale utilisée, les informations sur un éventuel profilage, sa logique et les conséquences éventuelles ;
- La durée de conservation des données, le caractère obligatoire des réponses et les conséquences en cas d'absence de réponse ;
- Les droit d'accès, rectification, portabilité, opposition, limitation, effacement, ainsi que la possibilité de retirer son consentement et de décider du sort post-mortem de ses données ;
- Un point de contact pour exercer ses droits et la faculté d'introduire une action auprès de la CNIL ;
- En cas de collecte indirecte, la mention doit également comporter les catégories de données obtenues ainsi que leur source.

Un niveau d'information à moduler

Mention allégée	**Quoi ?** La finalité du traitement, le responsable de traitement, les droits et un renvoi vers la Politique. **Quand ?** Lors d'une collecte intervenant pendant la vie du contrat.
Mention classique	**Quoi ?** Toutes les informations relatives au traitement nécessitant la collecte. **Quand ?** Lors de l'entrée en relation avec la personne concernée.
Politique de protection des données	**Quoi ?** Toutes les informations sur l'ensemble des traitements réalisés. **Où ?** Sur le site web de l'organisme ou à disposition dans les locaux.

Contractualisation avec les tiers

Tout organisme doit encadrer ses relations avec les tiers, sous-traitants ou responsables de traitements, intervenant sur des traitements de données. Il doit vérifier que ses sous-traitants présentent des garanties suffisantes. Dans ce cadre, trois chantiers doivent être mis en place : la phase précontractuelle, contractuelle et d'audit.

Quelles sont les qualités de traitement possibles ?

Responsable de traitement : Le responsable de traitement détermine les finalités et les moyens de tout traitement appliqué à des données personnelles. C'est celui pour le compte duquel le traitement est réalisé.

Responsables conjoints : Lorsque plusieurs responsables de traitements déterminent ensemble les finalités et moyens de traitements de données personnelles.

Sous-traitant : Le sous-traitant est un exécutant extérieur qui ne peut réaliser un traitement de données personnelles que sous l'autorité et sur instruction du responsable de traitement.

Attention, un sous-traitant au sens général du terme peut ne pas être sous-traitant mais responsable conjoint en matière de traitement de données personnelles.

Comment qualifier le tiers avec lequel vous contractez ?

La qualification se fait sur la base de quatre critères :

Autonomie : Qui détermine la finalité et les fonctionnalités du traitement ?
Qui détermine la façon dont les données sont intégrées dans le Système d'Information ? Qui met à disposition les ressources techniques / humaines ?

Expertise : Qui détient le rôle traditionnel impliquant le traitement ?

Contrôle : Qui est en charge de la validation finale / du contrôle ? Qui s'assure du respect des obligations vis-à-vis de la règlementation ? Qui effectue un reporting auprès de l'autre partie ?

Transparence : Qui est chargé de la gestion des droits ? A quelle entité appartient la charte graphique apparaissant sur les documents transmis aux clients ?

Comment préserver sa responsabilité en phase précontractuelle ?

Les appels d'offres doivent comporter des critères de sélection :

Les vérifications du respect des mesures peuvent être effectuées via l'envoi d'un questionnaire ou en demandant la communication de certains documents (Exemple : politique de protection des données).

Comment préserver sa responsabilité en phase contractuelle ?

Toutes les interventions de tiers doivent être encadrées par un contrat. De manière générale, un contrat passé avec un responsable conjoint de traitement comportera les obligations de chaque responsable sur son périmètre, tandis qu'un contrat passé avec un sous-traitant comportera les obligations du sous-traitant envers le responsable de traitement.

Comment encadrer les transferts de données en dehors de l'Espace Economique Européen?

L'arbre de décision ci-dessous peut-être utilisé afin d'encadrer ses transferts en dehors de l'EEE.

1. **Le pays dispose-t-il d'une protection adéquate au sens de la commission européenne ?** Si oui, réalisez un contrat classique. Si non, passez à l'étape 2.

2. **Le transfert est-il réalisé intra-groupe ?** Si oui, mettez en place des règles contraignantes d'entreprise (Binding Corporate Rules). Si non, passez à l'étape 3.

3. **Le transfert est-il nécessaire à l'exécution d'un contrat conclu avec la personne concernée ?** Si oui, réalisez un contrat classique. Si non, passez à l'étape 4 .Attention, il faut qu'un lien étroit et important existe entre la personne et la finalité du traitement et qu'il puisse être démontré.

4. **S'assurer de la mise en place de garanties appropriées** Plusieurs garanties sont possibles : recueillir le consentement de la personne concernée, mettre en place des clauses contractuelles types de la commission européenne, recourir à un code de conduite avec engagement contraignant et exécutoire ou à une certification avec engagement contraignant et exécutoire.

L'essentiel

Information, transparence et contractualisation : quelles sont vos obligations vis-à-vis des parties prenantes à vos activités?

Problématiques

Toute personne dont les données sont traitées doit être **informée des activités** portant sur ses données. Aussi, les obligations de chaque entreprise doivent être encadrées afin de préserver leur responsabilité.

Enjeux

Trouver un équilibre relatif à l'effort fourni par l'entreprise dans ses rapports avec l'externe, c'est-à-dire le **bon niveau d'information** à donner pour assurer une bonne compréhension par les personnes concernées et le bon niveau de contractualisation pour préserver sa responsabilité.

Recommandations

- Prioriser les informations essentielles dans les mentions et les contrats à revoir.
- Disposer d'une politique globale accessible sur le site internet et de clausiers dédiés.

LES PREUVES DE MISE EN CONFORMITÉ

Référentiel de mentions

Référentiel regroupant l'ensemble des mentions produites en fonction du support et de la finalité de traitement

Clausier

Clauses contractuelles types pour les contrats de sous-traitance et de responsabilité conjointe

Fichier de notation des-sous-traitants

Tableau de notation des sous-traitants lors des process achats en fonction de leur niveau de conformité

Le privacy by design et by default et l'analyse d'impact : comment anticiper et atténuer les risques ?

L'objectif du privacy by design est de penser la protection des données dès la conception des projets c'est-à-dire de manière préventive et proactive afin d'éviter de nombreux risques liés à la protection des données. Il est complété par le privacy by default, à savoir l'obligation de maximiser la protection des données, et l'analyse d'impacts ayant pour objet l'évaluation et la limitation des risques.

Le Privacy by design et by default

Se poser les bonnes questions

L'objectif est de prouver la prise en compte du RGPD en documentant les éléments ci-dessous :

- **Description générale :** Quelle est la finalité du traitement ? S'agit-il d'un nouveau traitement ? Qui est Responsable de traitement ? D'autres entités sont-elles impliquées ?
- **Description détaillée :** Quel est le nombre de personnes physiques impliquées ? Quelles catégories de personnes physiques sont impliquées ? Quelles sont les catégories de données traitées ? Toutes les données sont-elles nécessaires pour atteindre la finalité du traitement ?
- **Source, stockage et conservation :** Quelle est la source de collecte et comment les données sont-elles collectées ? Par qui, où, et combien de temps les données seront-elles stockées ? Les données utilisées seront-elles transférées ?
- **Sécurité :** Comment la donnée sera-t-elle transférée de la source à la base de données ? Qui aura accès aux données ?

Compléter le registre des traitements

Le nouveau traitement doit être intégré au registre des traitements avec l'ensemble de ses caractéristiques.

L'analyse d'impacts ou PIA

Quand devez-vous réaliser une analyse d'impacts sur la vie privée ?

Un PIA doit être réalisé lorsque le traitement répond à deux critères ou plus listés par le Groupe de travail des autorités de contrôle européennes (cf. Lignes directrices sur la réalisation d'analyses d'impacts).

Concrètement, quels sont les risques sur la vie privée ?

Accès illégitime aux données à caractère personnel

Modification non désirée des données

Disparition des données

L'essentiel

Le privacy by design et by default et l'analyse d'impact : comment anticiper et atténuer les risques?

Problématiques

Toute entreprise doit intégrer dans ses modes projets la protection des données afin de prendre en compte la protection de la vie privée dès la conception des nouveaux produits et services. Le niveau de protection doit être le plus élevé possible.

Enjeux

Protéger la vie privée de manière proactive et préventive en prenant en compte le plus tôt possible les exigences en matière de protection des données.
Anticiper et atténuer les risques pouvant peser sur les données personnelles des clients.

Recommandations

- Intégrer le DPO et le RSSI dans les modes projets
- Rédiger un set documentaire pouvant être utilisé pour chaque projet (ex: procédure pour un nouveau projet)
- Intégrer les plans d'actions issus des PIA dans les projets IT.

Quel processus d'analyse des risques mettre en place ?

1. Analyser les principes fondamentaux (finalité, licéité, nécessité et proportionnalité)
2. Evaluer les mesures de sécurité logiques et physiques
3. Apprécier les risques en fonction de la source, de la menace de la gravité et de la vraisemblance
4. Mettre en place des actions correctives pour limiter les risques
5. Si le risque résiduel demeure élevé, consulter la CNIL

LES PREUVES DE MISE EN CONFORMITÉ

Dossiers projets « Privacy by design »

- Description des caractéristiques du nouveau traitement
- Documentation des points sujets à conformité
- Suivi du plan d'action de mise en conformité

Standards d'entreprise

- Intégrer dans les standards d'entreprise des éléments liés à la protection des données

Dossiers Analyses d'impacts

- Documentation de l'analyse d'impact sur le traitement
- Suivi du plan d'action
- Sign-off du DPO

La valorisation des données personnelles : quels points d'attention ?

La vidéo surveillance sur le lieu de travail

Dans la mesure où une vidéo permet d'identifier directement ou indirectement une personne physique, qui plus est vulnérable, l'utilisation de la vidéo surveillance sur le lieu de travail est particulièrement encadrée.

Les obligations liées à la mise en place de la vidéo surveillance

- Ne pas filmer les employés sur leur poste de travail (hors manipulation de caisse)
- Respecter la vie privée des personnes filmées
- Ne pas filmer les zones de pause ou repos, ni les toilettes et locaux syndicaux
- Sécuriser l'accès à distance aux images

Les règles en matière d'accès et de conservation

L'accès doit être limité à un nombre très restreint de personnes. De plus, la durée de conservation doit être liée à la finalité du traitement et ne doit pas être fixée en fonction de la capacité de stockage (1 mois).

Comment informer les salariés ?

L'information sur le traitement doit être réalisée à deux niveaux.

- Des **panneaux affichés dans les locaux** doivent informer de la finalité du traitement, de la durée de conservation, des modalités d'exercice des droits et des personnes habilitées à visionner les vidéos.
- Le **règlement intérieur** ou **l'intranet** doit informer de l'objet du traitement (finalité et base légale), des données et catégories de personnes concernées, des destinataires des données, de la durée de conservation et des modalités d'exercice de droits.

La gestion des cookies et le consentement

« Les internautes doivent être informés et donner leur consentement préalablement à l'insertion de traceurs. Ils doivent disposer d'une possibilité de choisir de ne pas être tracés lorsqu'ils visitent un site ou utilisent une application.». Cette obligation est imposable aux éditeurs de sites, de système d'exploitation et d'applications, aux régies publicitaires, aux réseaux sociaux ainsi qu'aux éditeurs de solutions de mesures d'audience.

Quels sont les cookies devant obligatoirement faire l'objet d'un consentement?

- Les cookies liés aux opérations relatives à la publicité ciblée
- Les cookies de mesure d'audience
- Les cookies des réseaux sociaux générés notamment par leurs boutons de partage

Quelles sont les conditions de ce consentement ?

Le consentement recueilli doit pouvoir être retiré à tout moment (mécanismes de paramétrage) et ne doit pas conditionner l'accès au sit e internet.

L'acceptation de CGU ne constitue pas une modalité valable de recueil du consentement.

Respecter les durées de conservation

Il est nécessaire de faire apparaître un bandeau d'information et un recueil de consentement tous les 13 mois après la première visite.

Aussi, il faut supprimer les cookies permettant la traçabilité des internautes et les adresses IP au-delà de 13 mois à compter de la première visite.

Il est toujours obligatoire d'informer les personnes via un bandeau d'information, même si le recueil du consentement n'est pas obligatoire. Ce bandeau doit contenir :

- Les finalités des cookies
- La possibilité de s'opposer à ces cookies et de changer les paramètres en cliquant sur un lien présent dans le bandeau
- Le fait que la poursuite de sa navigation vaut accord au dépôts de cookies sur son terminal

Il ne doit pas disparaitre avant que l'internaute ne se rende sur une autre page ou clique sur un élément du site

Actualiser l'information et le consentement

Le consentement et l'information doivent être renouvelés lorsqu'une nouvelle finalité de cookie est mise en place.

La protection des données personnelles et le chat

Lors de la navigation internet et plus particulièrement lors de l'utilisation du chat (messagerie instantanée) les plateformes recueillent les communications ainsi que d'autres informations que les utilisateurs fournissent lorsqu'ils utilisent ces messageries. Cela peut comprendre des informations présentes dans le contenu que les personnes fournissent (par exemple : des métadonnées). Ces données non structurées entrent également dans le champ d'application du RGPD et leur protection demeure une obligation.

Périmètre d'application

Quels sont les organismes concernés par cette obligation ?

Cas de figure 1 : Les **markets place,** plateformes sur Internet mettant en relation des acheteurs et des vendeurs disposant de chats telles que Amazon, etc.;
Cas de figure 2 : Les réseaux sociaux.

Quelles sont les obligations des organismes vis-à-vis des utilisateurs concernant la protection des données?

Informer : les organismes sont dans l'obligation d'informer les utilisateurs:

- Des mesures mises en place afin de garantir la sécurité de leurs échanges;
- De l'utilisation d'outils « professionnels » tels que les API, plugins, etc.;
- Des conditions de stockage d'utilisation et de partage des conversations dans la **Politique d'utilisation des données;**
- Des droits dont ils disposent concernant leurs données personnelles et de la modalité d'exercice de ces derniers.

Collecter: les données personnelles issues du chat, sont, pour les plateformes les traitant, une réelle opportunité pour affiner leur connaissance et les préférences des utilisateurs, prospects ou clients les utilisant. La collecte du consentement constitue l'étape clé afin de procéder au traitement de ces données.

Garantir la sécurité des données personnelles

Comment garantir la sécurité de ces données personnelles?

Les données issues du chat sont des données personnelles à part entière et nécessitent une attention toute particulière. Décryptage des étapes clés à mettre en place:

Respecter les durées de conservation Par exemple, pour un chatbot conçu afin de répondre aux questions ponctuelles d'un utilisateur, des **règles de purge** automatiques mensuelles peuvent être mises en place.
Les données collectées ne doivent pas être conservées au-delà de la durée nécessaire à la finalité du traitement.

Mettre en place des **mesures organisationnelles et techniques spécifiques** aux données collectées.
Pour le recueil de **données sensibles,** comme par exemple, les données de santé, voici des solutions envisageables:

- Un chiffrement des données stockées;
- Un système de blocage de transmission des données sensibles (ex: champ bloquant);
- Un recours à des protocoles d'échanges sécurisés (SFTP, etc.).

Respecter les droits des utilisateurs.

Le consentement doit pouvoir être retiré à tout moment et ne doit pas conditionner l'accès au chat, sa collecte peut se traduire par un message explicite ou une webview.
Les utilisateurs peuvent, dans le cadre de l'exercice de leur droit, exiger à tout moment une restitution des données collectées. Charge à l'organisme de mettre à disposition des utilisateurs la possibilité de télécharger ces informations ou leur historique de conversation.

Prospection commerciale et profilage : quand et pourquoi recueillir le consentement ?

La prospection commerciale

Quand collecter le consentement concernant mes opérations de prospection?

Le traitement des données personnelles à des fins de prospection commerciale ne doit pas toujours faire l'objet d'un **consentement préalable**. Pour déterminer si un consentement doit être recueilli, il faut prendre en compte la **cible de prospection et le canal de diffusion.**

Cas de figure 1: Client (produits analogues)

Le **consentement n'est pas nécessaire,** en revanche, l'organisme doit être en capacité de capter une opposition du contact et de conserver cette information.

Cas de figure 2: Prospect et client (produits non analogues) par téléphone ou courrier

Le consentement à la prospection commerciale sur les canaux **téléphonique** et **courrier papier** n'est pas nécessaire.
En revanche tout comme pour le cas précédent, la personne concernée peut à tout moment exercer son **droit d'opposition.**

Cas de figure 3: Prospect et client (produits non analogues) par voie électronique

Le consentement à la prospection commerciale sur les canaux **e-mail** et **SMS** est obligatoire. Sa collecte doit impérativement avoir lieu avant la réalisation du traitement. Une personne ne peut être contactée que si le responsable de traitement a préalablement collecté son consentement.

Combien de temps le consentement est-il valable ?

3 ans (à compter du dernier contact émanant du prospect avec l'entreprise).

Faut-il collecter le consentement concernant la prospection en B to B?

Non, la collecte du consentement n'est pas nécessaire pour prospecter le représentant d'une personne morale

Le profilage

Qu'est ce que le profilage ?

« Un traitement de profilage a pour objet d'évaluer une personne et de prédire ses réactions et ses préférences. Le profilage est un traitement individualisé». Article 22 du RGPD. Tout traitement de profilage sur des **données sensibles** est interdit, sauf si la personne concernée en est préalablement informée et qu'elle a donné son consentement.

Le process

- Analyse et traitement des données de la personne concernée;
- Établissement d'un profil individualisé ;
- Identification de ses préférences et réactions ;
- Déclenchement d'une décision automatisée.

Quand collecter le consentement concernant mes opérations de profilage? Quelles sont mes obligations?

Cas de figure 1 : Intervention humaine
Lorsqu'un humain intervient dans la prise de décision alors la collecte du consentement n'est pas nécessaire.

Cas de figure 2 : Exécution du contrat ou dispositions légales spécifiques
Lorsque le profilage est une étape nécessaire à la conclusion d'un contrat ou lorsque les décisions sont encadrées par des dispositions légales spécifiques le responsable de traitement doit :

- Informer les personnes lors de la collecte de leurs données ;
- Permettre aux personnes ayant fait l'objet d'une telle décision de contester la décision ou demander de basculer sur un processus géré manuellement.

Cas de figure 3: Aucune des conditions préalables n'est remplie
Dans le cas où aucune de ces cas de figure n'est remplie alors le consentement est à collecter.

L'essentiel

La valorisation des données personnelles : quels points d'attention ?

Problématiques

Pour chaque traitement sur **des données à caractère personnel,** une finalité doit être définie.
Certains traitements doivent répondre à des obligations particulières, et doivent faire l'objet d'une attention certaine.

Enjeux

Adapter les règles générales décrites dans la politique aux cas particuliers issus des activités de valorisation des données.

Recommandations

- Collecter uniquement les données nécessaires au traitement
- Maitriser les données collectées (stockage, transferts, accès, etc.)
- Mettre en place des modes opératoires dédiés à chaque activité de valorisation.

LES PREUVES DE MISE EN CONFORMITÉ

Des fiches pratiques par thématiques

Des fiches pratiques pour chacun des sujets doivent être transmis aux directions concernées et doivent comprendre les obligations à respecter pour réaliser un traitement donné.

Implication du DPO

Comptes rendus de réunion prouvant la participation du DPO à la prise de décisions impactant les données personnelle.

VOS CONTACTS

Sophie Le Goff
Associate Partner Compliance
sophie.le-goff@sia-partners.com

Sandra Bertay
Senior Manager Compliance
sandra.bertay@sia-partners.com

Jeanne Fourcade
Consultante Compliance
jeanne.fourcade@sia-partners.com

Alexandre Noireau
Consultant Compliance
alexandre.noireau@sia-partners.com

À PROPOS DE SIA PARTNERS

Sia Partners réinvente le métier du conseil et apporte un regard innovant et des résultats concrets à ses clients à l'ère du digital. Avec plus de 1 200 consultants dans 15 pays, nous allons générer un chiffre d'affaires annuel de plus de 200 millions d'euros pour l'exercice en cours. Notre présence globale et notre expertise dans plus de 30 secteurs et services nous permettent d'accompagner nos clients dans le monde entier. Nous accompagnons leurs initiatives en stratégie, projets de transformation, stratégie IT et digitale et data science. En tant que pionniers du Consulting 4.0, nous développons des consulting bots et intégrons dans nos solutions la disruption créée par l'intelligence artificielle.

Abou Dabi

Amsterdam

Bruxelles

Casablanca

Charlotte

Denver

Doha

Dubai

Frankfurt

Hamburg

Hong Kong

Houston

Londres

Luxembourg

Lyon

Milan

Montréal

New York

Paris

Riyad

Rome

Seattle

Singapour

Tokyo

Toronto