Le RGPD
et ses applications en SSTI

Présanse | Réunion d'information

Journée d'étude du 15 mars 2018

AXESS Solutions Santé
Digital & Business Experts

Erwan TREHIOU
Avocat

présanse
PRÉVENTION ET SANTÉ AU TRAVAIL

PRESENTATION

Aurélie TRACOL

Ingénieur Qualité | Responsable de la sécurité des données depuis 2016

- Resp. Qualité & Resp. Support pendant 20 ans chez un éditeur dans le domaine de la Santé (certification ISO 9001)
- Lead implementer ISO 27001 (nov. 2017)

Maître Erwan TREHIOU

Avocat

- Droit des contrats
- Droit des affaires
- Droit de la consommation
- Droit du numérique

SOMMAIRE

1 Le RGPD

1. Introduction

- Généralités
- Quelques définitions
- Pourquoi ?
- Qu'est-ce qui change ?

1 LE RGPD Introduction / Généralités

- Nouveau texte de référence européen en matière de **protection des données à caractère personnel**

GDPR : General Data Protection Regulation

RGPD : Règlement Général sur la Protection des Données

- Remplace la Directive CE 95/46 du 24 octobre 1995

- Applicable à partir du **25 mai 2018**

- Concerne toutes les entités **situées dans l'Union européenne** ou **proposant des services dans l'Union européenne** qui traitent des données à caractère personnel, **même manuellement**.

Exceptions :

- *activité strictement personnelle ou domestique*
- *traitements concernant la sécurité nationale ou de l'Union européenne*

1 LE RGPD Introduction / Quelques définitions

Donnée à caractère personnel

« toute information se rapportant à une personne physique identifiée ou qui peut être identifiée, ***directement ou indirectement****, notamment par référence :*

- ***à un identifiant, tel***
  - *qu'un nom,*
  - *un numéro d'identification,*
  - *des données de localisation,*
  - *un identifiant en ligne,*
- ***ou à un ou plusieurs éléments spécifiques propres à son identité :***
  - *physique,*
  - *physiologique,*
  - *génétique,*
  - *psychique,*
  - *économique,*
  - *culturelle,*
  - *ou sociale. »*

1 LE RGPD Introduction / Quelques définitions (suite)

Donnée à caractère personnel sensible

Elles concernent :

- *l'origine raciale ou ethnique,*
- *les opinions politiques,*
- *les convictions religieuses ou philosophiques ou l'appartenance syndicale,*
- *les données génétiques,*
- *les données biométriques aux fins d'identifier une personne physique de manière unique,*
- *les **données concernant la santé**,*
- *les données concernant la vie sexuelle ou l'orientation sexuelle.*

Données concernant la santé

*« Données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, **y compris la prestation de services de soins de santé**, qui révèlent des informations sur l'état de santé de cette personne. »*

Sauf cas particuliers, le traitement des données sensibles est interdit.

1 LE RGPD Introduction / Quelques définitions (suite)

Traitement

*« toute opération ou tout ensemble d'opérations **effectuées ou non à l'aide de procédés automatisés** et appliquées à des données ou des ensembles de données à caractère personnel, telles que :*

- *la collecte,*
- *l'enregistrement,*
- *l'organisation,*
- *la structuration,*
- ***la conservation,***
- *l'adaptation ou la modification,*
- *l'extraction,*
- *la consultation,*
- *l'utilisation,*
- *la communication par transmission,*
- *la diffusion ou toute autre forme de mise à disposition,*
- *le rapprochement ou l'interconnexion,*
- *la limitation,*
- *l'effacement ou la destruction. »*

1 LE RGPD Introduction / Quelques définitions (suite)

Responsable du traitement

« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, ***détermine les finalités et les moyens du traitement****. »*

1 LE RGPD Introduction / Pourquoi ?

Bref historique

• **1995 Europe** : approbation des principes de la vie privée et de la protection des données personnelles

Directive » nécessité de la transposer dans la législation de chaque pays

» 28 lois différentes !!!

- difficile à appliquer au niveau international
- protection des consommateurs inégale selon les pays
- peu efficace auprès des grandes entreprises comme Google ou Facebook

Ancienneté des règles, mal adaptées aux nouveaux développements (IoT, applications mobiles, cloud…) **» nécessité d'une nouvelle règlementation**

• **2016 GDPR** (99 articles) adopté par le Parlement européen

Règlement » effet direct dans chaque loi nationale

• **2018 (25 mai) Entrée en vigueur du GDPR** dans chaque pays membre

1 LE RGPD Introduction / Qu'est-ce qui change ?

- **Renforcer les droits des personnes** (création d'un droit à la portabilité des données personnelles, personnes mineures…)

- **Responsabiliser les entités** (resp. de traitement et sous-traitants)

- Rendre les **sanctions vraiment dissuasives**

(20 000 000 € ou 4 % du CA annuel mondial : **le + élevé des 2** !)

1 Le RGPD

2. Les grands principes

- Accountability
- Coresponsabilité des sous-traitants
- Privacy by design / default
- Analyse d'impact sur la vie privée
- Désignation d'un DPO
- Signalement des violations
- Nouveaux droits des personnes

1 LE RGPD Les grands principes

Logique de responsabilisation

« Accountability »

- Prendre toutes les mesures pour garantir la conformité des traitements
  - » **être en mesure de le démontrer à tout moment** (registre de l'ensemble des traitements)
- Le responsable du traitement est un acteur économique responsable
  - » (mesures techniques et organisationnelles pour garantir le respect de la réglementation)

Coresponsabilité des sous-traitants

- Engagement contractuel (protection, alerte le cas échéant)
- Solidairement responsables

1 LE RGPD Les grands principes

Protection de la vie privée dès la conception

« Privacy by design »

- Protection de la vie privée dès la conception d'un service / produit
  - » (et tout au long du cycle de vie des données)

Protection de la vie privée par défaut au + haut niveau

« Privacy by default »

Nativement niveau de protection le + élevé

- Seules les **données nécessaires à la finalité** poursuivie seront traitées
- **Consentement explicite et éclairé** des personnes concernées
- **Durée limitée**
- **Gestion des habilitations**

1 LE RGPD Les grands principes

Analyse d'impact sur la vie privée

« PIA : Privacy Impact Assessment »

- Analyse des risques si **risque élevé pour les droits et libertés**
  - » (collecte massive de données sensibles)

Désignation d'un Délégué à la Protection des Données

« DPO : Data Protection Officer »

Obligatoire pour les SSTI car :

- Traitement **à grande échelle de données sensibles ou condamnations**

1 LE RGPD Les grands principes

Signalement des violations de données personnelles

- Signalement à la CNIL et à la personne concernée si risque élevé pour les droits et libertés.

Nouveaux droits des personnes

- Droit d'information renforcé (consentement pour une finalité précise)
- Droit à l'oubli consacré (effacement et pas simple déréférencement)
- Droit à la limitation des traitements
- Droit à la portabilité des données (format structuré et lisible)

2 Ses applications en SSTI

1. Qui est concerné ?
2. Mise en conformité

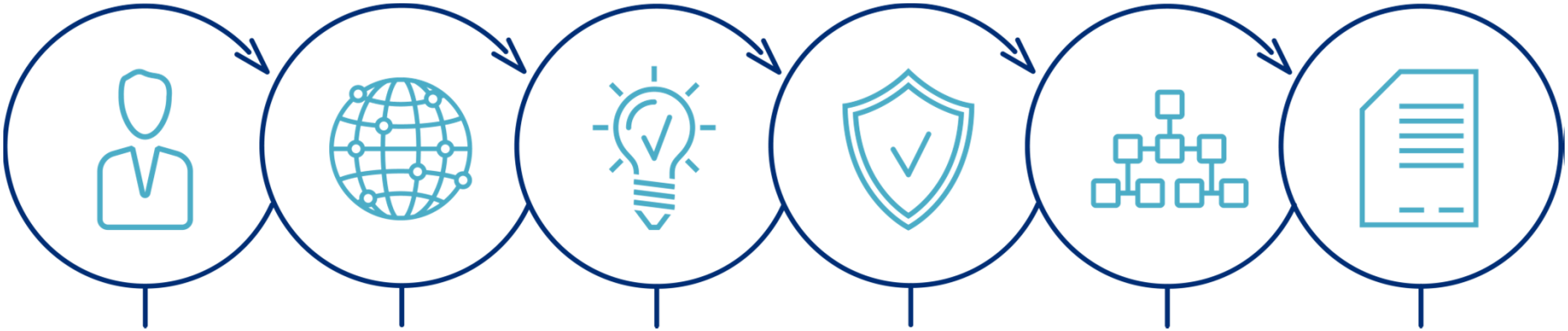
2 SES APPLICATIONS SSTI : Qui est concerné ?

- Equipe Santé Travail
- Service ressources humaines
- Service de la gestion de la relation adhérent
- Service comptabilité
- Services techniques (informatique, logistique, …)
- Service juridique
- Service communication
- …

» Impact sur tout le SSTI

2 SES APPLICATIONS SSTI : Mise en conformité

La CNIL a organisé la mise en conformité en 6 étapes



1. Désigner un Délégué à la Protection des Données
2. Cartographier les traitements de données personnelles
3. Prioriser les actions
4. Gérer les risques
5. Organiser les processus internes
6. Documenter la conformité

2 SES APPLICATIONS SSTI : Mise en conformité

1 Désigner un pilote

Les SSTI doivent obligatoirement nommer un **Délégué à la Protection des Données** (ou DPO, Data Protection Officer) car ils traitent « à grande échelle » des données sensibles.

C'est le successeur du Correspondant Informatique et Libertés.

Son profil :

- Appétence pour la partie **juridique**
- Compétences **techniques/informatiques**
- Bon **communiquant**

2 SES APPLICATIONS SSTI : Mise en conformité

1 Désigner un pilote (suite)

Son rôle :

- **Informer et conseiller** le responsable de traitement ou le sous-traitant ainsi que leurs employés.

- **Contrôler le respect du règlement** et du droit national en matière de protection des données.

- **Conseiller le SSTI** sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution.

- **Coopérer avec l'autorité de contrôle** et être le point de contact de celle-ci.

Le DPO peut être **externe** au SST et peut être **mutualisé**.

2 SES APPLICATIONS SSTI : Mise en conformité

2 Cartographier vos traitements de données personnelles

Tenir un registre des traitements pour être à tout moment en mesure de répondre aux questions suivantes :

- **Qui ? »** Responsable du traitement, responsable du service traitant les données, sous-traitant éventuel…
- **Quoi ? »** Catégorie de données traitées (données de santé ou non)
- **Pourquoi ? »** Finalité (exemples gestion RH, gestion de dossier Santé au Travail…)
- **Où ? »** Lieu de stockage
- **Jusqu'à quand ? »** Durée de conservation (ou moyen de calcul)
- **Comment ? »** Mesures de sécurité pour minimiser les risques

2 SES APPLICATIONS SSTI : Mise en conformité

3 Prioriser les actions

Pour chaque traitement, identifier les actions à mener pour être conforme aux obligations actuelles et à venir et les prioriser au regard des risques pesant sur les droits et libertés des personnes concernées :

- **Minimisation »** Supprimer toutes les données à caractère personnel qui ne sont pas indispensables à la finalité du traitement …
- **Base juridique à identifier »** Exemples : consentement, intérêt légitime, contrat, obligation légale…
- **Mentions d'information à réviser »** Clarifier l'information des personnes (transparence)
- **Information des sous-traitants et conformité des contrats »** Coresponsabilité des sous-traitants, obligation de sécurité, confidentialité
- **Modalités d'exercice des droits des personnes à prévoir »** Droits d'accès, de rectification, portabilité, retrait du consentement…
- **Mesures de sécurité à vérifier »** Audits…

2 SES APPLICATIONS SSTI : Mise en conformité

4 Gérer les risques

Pour les « collectes massives » de données de santé (susceptibles d'engendrer des risques élevée pour les droits et libertés des personnes concernées), une **analyse d'impact sur la vie privée** (PIA, Privacy Impact Assessment) doit être faite.

Elle contient :

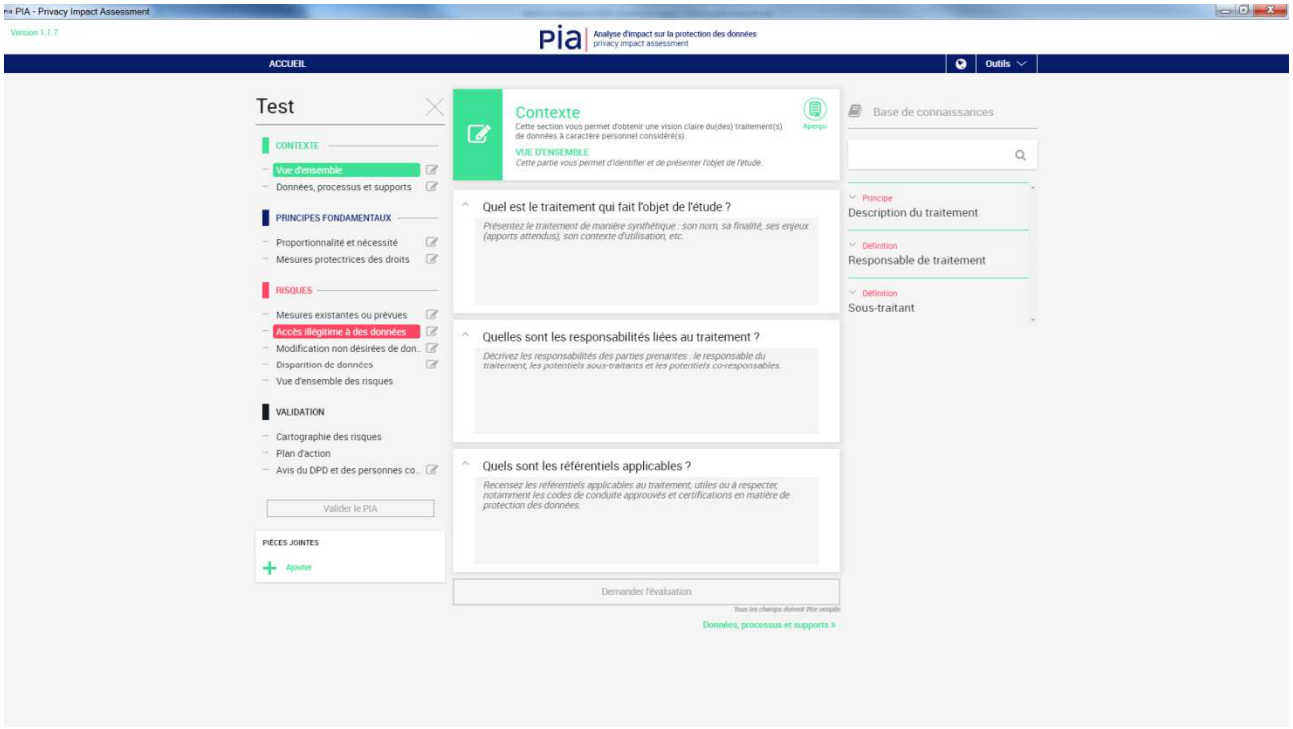
- Une **description du traitement** et de ses **finalités**.
- Une **évaluation de la nécessité** et de la **proportionnalité** du traitement.
- Une **appréciation des risques** sur les droits et libertés des personnes concernées.
- Les **mesures envisagées** pour traiter ces risques et se conformer au règlement.

2 SES APPLICATIONS SSTI : Mise en conformité

4 Gérer les risques (suite)

Il existe des outils facilitant l'analyse d'impact sur la vie privée :

- outil EBIOS (méthode d'analyse de risques)
- outil spécifique de la CNIL nommé « PIA » :



2 SES APPLICATIONS SSTI : Mise en conformité

5 Organiser les processus

Des processus internes doivent être décrits pour protéger les données en permanence en tenant compte d'événements non prévus (faille de sécurité, changement de prestataire, gestion des demandes d'accès, modification des données collectées…).

Il convient de :

- **Prendre en compte** la protection des données dès la conception d'une application ou d'un traitement (minimisation, durée de conservation, mentions d'information, recueil du consentement, sécurité des données, rôle des acteurs).

- **Sensibiliser et organiser** la remontée d'information (plan de formation et de communication auprès des collaborateurs).

- **Traiter** les demandes des personnes concernée en définissant les acteurs et les modalités (voie électronique ?).

- **Anticiper** les violations de données (notification à la CNIL dans les 72H et aux personnes concernées dans les meilleurs délais).

2 SES APPLICATIONS SSTI : Mise en conformité

6 Documenter la conformité

La conformité du SSTI doit être prouvée à tout moment. Pour cela, un dossier documentaire doit être construit, comportant :

- **La documentation sur les traitements :**
  - » des traitements
  - » analyses d'impact sur la vie privée
- **L'information des personnes :**
  - » mentions d'information
  - » modèles de recueil du consentement des personnes concernées
  - » procédures mises en place pour l'exercice du droits des personnes
- **Les contrats et responsabilités des acteurs :**
  - » et les modalités

3 Focus

1. **Le sous-traitant**
2. **La gestion de la conformité des contrats**
3. **Garantir le *Privacy by design***
4. **L'analyse d'impact sur la protection des données**

3 FOCUS n°1 Le sous-traitant

Définition du sous-traitant

- Article 4 § 8 : le sous-traitant est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

- Il s'agit d'une personne juridique distincte du responsable de traitement (client).

Responsabilité du sous-traitant

Un sous-traitant n'est tenu pour responsable du dommage causé par le traitement que :

1) s'il n'a pas respecté les obligations prévues par le RGPD qui incombent spécifiquement aux sous-traitants, ou
2) s'il a agi en-dehors des instructions licites du responsable du traitement ou contrairement à celles-ci.

» Il y a une co-responsabilité et non pas un transfert de responsabilité.

3 FOCUS n°1 Le sous-traitant

Exigences du sous-traitant

- Le sous-traitant doit *« présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée »*.

- Le responsable du traitement doit donc définir un socle de base prenant en compte les éléments suivants :

    - les opérations de traitement confiées au prestataire
    - la sécurité technique des services
    - la maturité du prestataire sur la question de la protection des données personnelles

3 FOCUS n°1 Le sous-traitant

Problématique : comment sécuriser son régime de sous-traitance ?

➢ 1ère étape : sécuriser le contrat de sous-traitance

Le RGPD impose au responsable du traitement de signer avec chacun de ses sous-traitants un contrat écrit (papier ou électronique), avec des clauses obligatoires :

- l'objet du traitement
- la durée du traitement
- la nature et la finalité du traitement
- le type de données à caractère personnel
- les catégories de personnes concernées
- les obligations et les droits du responsable du traitement

3 FOCUS n°1 Le sous-traitant

Problématique : comment sécuriser son régime de sous-traitance ? (suite)

➢ 1ère étape : sécuriser le contrat de sous-traitance (suite)

Le contrat doit également prévoir que le sous-traitant :

- ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement,
- veille à ce que les personnes autorisées à traiter les données à caractère personnel respectent la confidentialité,
- prenne toutes les mesures requises en matière de sécurité des traitements,
- aide le responsable du traitement au respect du RGPD.

» Le sous-traitant met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations et permettre la réalisation d'audits.

3 FOCUS n°1 Le sous-traitant

Problématique : comment sécuriser son régime de sous-traitance ? (suite)

➢ 1ère étape : sécuriser le contrat de sous-traitance (suite)

Il convient, pour tout recours à un sous-traitant :

- d'évaluer le niveau de risque du sous-traitant,
- de négocier les clauses contractuelles adaptées au niveau de risque.

3 FOCUS n°1 Le sous-traitant

Problématique : comment sécuriser son régime de sous-traitance ? (suite)

➢ 2ème étape : gérer la chaine de sous-traitance dans son ensemble

Il convient pour cela de :

- gérer le sous-traitant de premier rang sur le plan opérationnel,
- établir une matrice de sous-traitance,
- mettre en place une revue annuelle de la sous-traitance,
- gérer les sous-traitants de second rang.

3 FOCUS n°1 Le sous-traitant

Problématique : comment sécuriser son régime de sous-traitance ? (suite)

➢ 3ème étape : sécuriser les sous-traitants déjà existants

Il convient pour cela de :

- répertorier les sous-traitants actuels,
- leur attribuer un niveau de risque,
- mettre en conformité le contrat de sous-traitance.

3 FOCUS n°2 La gestion de la conformité des contrats

Le contrat permet de gérer :

- les engagements des prestataires professionnels
- la collaboration des entreprises clientes
- la répartition des tâches
- les responsabilités liées
- la protection des données

» Le contrat est un point essentiel de toute activité économique : la question de la mise en conformité d'un organisme avec les dispositions du RGPD implique la mise en conformité des contrats.

3 FOCUS n°2 La gestion de la conformité des contrats

Problématique : comment mettre en conformité les contrats ?

➢ D'une manière générale, il convient d'adapter les contrats :

- avec les sous-traitants
- avec les prestataires informatiques/technologiques (achat de logiciels, de solutions informatiques complexes
- dans les appels d'offres, qu'ils soient privés ou publics
- avec les personnes concernées

➢ Cette adaptation se fait par :

- l'insertion de clauses spécifiques à la protection des données (finalités des traitements, durée de conservation, exigences de coopération, modalité de notification des violations de données, mesures d'urgence…)
- le renforcement de l'information des personnes concernées, via des documents contractuels
- la vérification des garanties apportées par les partenaires (*Privacy by design* des logiciels, sécurité des infrastructures d'hébergement, confidentialité des traitements effectués par les préposés)

3 FOCUS n°2 La gestion de la conformité des contrats

» Il convient d'attacher une attention toute particulière à la rédaction des contrats, qui permettront de répartir concrètement les responsabilités de chacun et de démontrer une volonté de mise en conformité aux dispositions du RGPD.

» Il n'existe pour autant pas de clauses types puisque les clauses doivent être adaptées à chaque situation.

3 FOCUS n°3 Garantir le *Privacy by design*

Définition

- Article 25 § 1 RGPD : « *Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques, le responsable du traitement met en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences du présent règlement et de protéger les droits de la personne concernée ».*

» Le *privacy by design* est donc le fait pour le responsable du traitement de mettre en place un ensemble de mesures de sécurité en amont de la création de son produit, de son service et de la réalisation de ses traitements.

» Il y a une exigence de proportionnalité entre les finalités des traitements et les risques liés, et les mesures à mettre en place.

3 FOCUS n°3 Garantir le *Privacy by design*

Les principes de mise en conformité

- Etre proactif, et non réactif, être préventif, et non correctif
- Protection par défaut *(Privacy by default)*
- Protection de la vie privée intégrée dès la conception (coexistence entre protection et innovation)
- Conciliation des intérêts
- Sécurité de bout en bout, durant tout le cycle de la vie de la donnée
- Visibilité et transparence assurées par le responsable du traitement (obligation d'information)
- Respect de la vie privée des utilisateurs

3 FOCUS n°3 Garantir le *Privacy by design*

La garantie du Privacy by design en pratique

- Minimisation de la collecte (proportionnalité entre les données qu'il entend collecter et les finalités des traitements)
- Dissimulation des données et de leurs interdépendances
- Séparation des données
- Agrégat des données
- Information des personnes
- Contrôle de la personne sur les données
- Mise en œuvre d'une politique de confidentialité
- Preuve de la conformité (accountability)

3 FOCUS n°4 L'analyse d'impact sur la protection des données

Définition

- Le RGPD en tant que tel ne définit pas formellement la notion d'analyse d'impact sur la protection des données : il en détaille cependant le contenu et son rôle.

- En principe, il s'agit d'une analyse préalable effectuée par le responsable du traitement, à réaliser avant que les traitements soient mis en place ou modifiés de façon substantielle.

- L'analyse d'impact a pour objet de :

    - décrire les traitements réalisés par l'organisme sur des données personnelles,
    - évaluer la nécessité et la proportionnalité de ces traitements,
    - gérer les risques sur les droits et libertés des personnes physiques qui en résultent (détermination des mesures à prendre en compte).

- Tous les traitements ne sont pas concernés : requièrent une analyse d'impact les traitements « susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques ».

3 FOCUS n°4 L'analyse d'impact sur la protection des données

Traitement nécessitant une analyse d'impact

- Le RGPD lui-même fournit des exemples de traitements nécessitant une analyse d'impact :

  - l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, fondée sur un traitement automatisé, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;

  - traitement à grande échelle de catégories particulières de données ou de données à caractère personnel relatives à des condamnations pénales et à des infractions ;

  - la surveillance systématique à grande échelle d'une zone accessible au public.

3 FOCUS n°4 L'analyse d'impact sur la protection des données

Traitement nécessitant une analyse d'impact

- Plusieurs critères doivent être pris en compte :
  - Évaluation et notation
  - Prise de décision ayant des effets juridiques
  - Surveillance systématique
  - Données sensibles
  - Traitement à grande échelle
  - Séries de données assemblées et combinées
  - Données concernant les personnes vulnérables
  - Recours à de nouvelles technologies
  - Transfert des données en-dehors de l'UE
  - Traitement privant d'un droit, d'un service ou d'un contrat

» Plus il y a de critères, plus il est probable que le traitement présente un risque élevé pour les droits et les libertés des personnes concernées, et que par conséquent une analyse d'impact soit nécessaire.

3 FOCUS n°4 L'analyse d'impact sur la protection des données

Réalisation de l'analyse d'impact

- L'analyse d'impact doit être effectuée avant la mise en place du traitement, le plus tôt possible.
- L'analyse d'impact doit être mise à jour tout au long de la conception du traitement.
- Le responsable du traitement doit réaliser l'analyse d'impact : il peut faire appel à des tiers (ex : sous-traitant), mais c'est lui qui engage sa responsabilité sur la conformité de l'analyse.
- Consultations : DPO / Personnes concernées.

3 FOCUS n°4 L'analyse d'impact sur la protection des données

Méthodologie de réalisation

Le RGPD prévoit qu'une analyse d'impact doit au moins comporter :

- une description des opérations de traitement envisagées et des finalités de traitement ;
- une évaluation de la nécessité et de la proportionnalité des opérations envisagées ;
- une évaluation des risques pour les droits et libertés des personnes concernées ;
- les mesures envisagées pour aborder les risques et établir le respect du RGPD.

3 FOCUS n°4 L'analyse d'impact sur la protection des données

Conseils pratiques

- Le cadre est assez souple
- Il existe des modèles (G29, CNIL)
- Norme ISO/EIC 29134
- Prise en compte des codes de conduite édictés par des associations ou des organismes professionnels
- Guides CNIL
- Développement par la CNIL d'un outil en ligne permettant de réaliser une analyse d'impact

Conclusion

Opportunités :

- **Pas supplémentaire** vers la protection des données personnelles.
- Santé au travail, la protection de la vie privée : **droits fondamentaux.**
- Renforce la position des SSTI **comme tiers de confiance.**

Mise en conformité réussie si :

1. **vous êtes convaincu** que le RGPD permettra de **renforcer les SSTI** et de **pérenniser leur indépendance et leur rôle,**
2. **vous organisez cette transition** (6 étapes CNIL par exemple),
3. **vous communiquez** avec conviction et **sensibilisez** tous vos collaborateurs,
4. **vous suivez** cette démarche **dans le temps** avec une **volonté d'amélioration continue.**

Merci de votre attention !

Avez-vous des questions ?

Aurélie TRACOL
1 rue Mozart
26000 VALENCE
04.75.82.00.80 – P. 7018
aurelie.tracol@axess.fr

Erwan TREHIOU - Avocat
8 rue Beccaria
38000 GRENOBLE
04.76.43.94.71
contact@trehiou-conseils.fr