PROTECTION DES DONNÉES EN ACTION

10 Fiches Pratiques pour devenir un as de la conformité RGPD

MDP
DATA PROTECTION

Réalisé et Edité par

DATA PROTECTION

Editeur de solutions SaaS Legal-Tech

Notre ADN : Des compétences à la convergence de plusieurs métiers : juridique, technologie IA, marketing, et sécurité.

Notre promesse :

- Simplifier la vie de nos clients dans leur conformité
- Faire du réglementaire, un avantage compétitif et non une contrainte.

Table des matières

PREAMBULE

La gestion d'une entreprise soulève inévitablement des questions essentielles qui touchent à la fois à la sécurité, à la responsabilité et à la confiance. À l'ère numérique, où l'information est une ressource aussi précieuse que vulnérable, il est crucial de prendre en compte les préoccupations suivantes :

- Suis-je suffisamment protégé sur le plan informatique ?
- Quelles seraient les retombées d'une cyberattaque ?
- Suis-je en conformité avec le RGPD ?
- ...et bien d'autres.

Les interrogations soulevées sont nombreuses et complexes, allant de la gestion des données personnelles à la responsabilité éthique. Se préoccuper de ces aspects n'est pas seulement le signe d'une entreprise responsable, mais aussi d'une entreprise qui reconnaît que son activité est indissociablement liée à la protection et au respect des données et plus globalement, de son capital informationnel.

Le RGPD en Perspective

Le Règlement Général sur la Protection des Données (RGPD) représente une étape majeure dans la protection des données personnelles. Ce règlement européen encadre les traitements réalisés au sein de l'Espace Économique Européen mais aussi ceux qui concernent les données personnelles des citoyens européens. Evolution d'une législation qui tente d'épouser son temps, le cadre établi par le RGPD va au-delà d'une simple réglementation : il établit un équilibre entre l'innovation, la responsabilité et la préservation des droits individuels. Depuis son entrée en vigueur en 2018, le RGPD a permis de :

→ **Renforcement des Droits Individuels :** Le RGPD reconnaît la valeur des données personnelles et octroie aux individus un

contrôle accru sur leur utilisation. Il consacre également des dispositions spécifiques pour protéger les données des mineurs.

→ **Sensibilisation et Responsabilisation :** Le RGPD n'est pas seulement destiné aux experts en conformité ou au grandes entreprises. Il concerne l'ensemble des acteurs impliqués dans le traitement des données. Il suscite une prise de conscience collective de l'importance de la protection des données tout au long de leur cycle de vie.

→ **Collaboration Européenne :** Le RGPD transcende les frontières nationales en encourageant une coopération étroite entre les autorités de protection des données européennes. Cette collaboration renforce la crédibilité de la régulation et garantit une application cohérente et efficace du règlement.

→ **Pouvoirs de Sanction :** Le RGPD confère aux autorités de protection des données des pouvoirs de sanction renforcés. Cela assure que les entreprises qui négligent leurs responsabilités en matière de protection des données sont tenues responsables de manière adéquate.

Quelques chiffres

Pour mieux appréhender l'impact et la nécessité du RGPD, il est instructif de se pencher sur les données concrètes. Dans son rapport annuel d'activité pour l'année 2022, la Commission Nationale de l'Informatique et des Libertés (CNIL) offre un aperçu saisissant :

En 2022, la CNIL a démontré sa préoccupation constante pour la protection des droits individuels et la conformité avec le RGPD :

- **Traitement des Plaintes :** La réduction du nombre de plaintes déposées témoigne d'une prise de conscience croissante des enjeux liés à la protection des données. Cependant, la persistance d'une activité significative souligne l'importance continue du respect des obligations en matière de protection des données.

- **Contrôles Actifs :** Les 340 contrôles effectués par la CNIL en 2023 témoignent de son engagement à surveiller et à garantir la conformité des entreprises. Une attention particulière est accordée aux plaintes, ce qui renforce la dimension proactive de la régulation.
- **Sanctions et Mises en Demeure :** Les 42 sanctions et 168 mises en demeure imposées par la CNIL en 2023 soulignent son rôle crucial dans l'application du RGPD. Ces mesures ne visent pas simplement la répression, mais aussi l'éducation et la prévention.
- **Impact Financier :** Les amendes cumulées approchant les 100 millions d'euros montrent que les conséquences d'une non-conformité peuvent être substantielles. Cela met en évidence l'importance d'investir dans la conformité pour éviter des coûts potentiels plus élevés.

Le voyage vers une conformité et une prise en compte des principe du RGPD par les équipes métiers peut sembler complexe, mais est essentiel pour bâtir des bases solides en matière de protection des données. Ce livret de formation vise à vous guider dans cette démarche, en vous fournissant les connaissances et les outils nécessaires pour naviguer dans ce paysage réglementaire en constante évolution et assurer les bases d'une protection de vos données.

L'état des lieux de la cybersécurité

La cybersécurité constitue un enjeu majeur et décisif de la survie d'une entreprise, avec des implications financières et opérationnelles considérables à l'échelle mondiale.

Dans l'univers numérique, chaque individu utilisant un outil numérique ou même un objet connecté peut représenter un point vulnérable dans le réseau de cybersécurité qui s'étend à travers le cyberespace. L'essor des interactions numériques a été accompagné d'une croissance fulgurante des attaques de piratage.

Quelques données chiffrées du rapport du Sénat de 2021 suffisent pour mettre en lumière l'ampleur de cette tendance :

- Dès 2021, le coût de la cybercriminalité atteint **les 6 000 milliards** de dollars par an, en hausse par rapport aux 3 000 milliards enregistrés en 2015, affectant tous les secteurs économiques,
- Si le cyber risque était un pays, il serait la **3ème** économie mondiale,
- En 2020, **43%** des PME ont fait face à des incidents de cybersécurité, illustrant la portée généralisée de la menace,
- Sur la même années **16%** des attaques mettent en péril l'existence même d'une entreprise.

Une intégration croissante mais inégale du risque Cyber

Les criminels du cyberespace ne choisissent pas leurs cibles au hasard. Lorsqu'une entreprise renforce sa sécurité, les cybercriminels ajustent leurs tactiques en ciblant des maillons plus faibles de la chaîne, comme les fournisseurs ou les sous-traitants.

Les grandes entreprises et les ETI (Entreprises de Taille Intermédiaire) ont un budget permettant de mettre en place défenses plus robustes. Les stratégies de sauvegarde efficace et de reconstruction des systèmes ont également réduit l'efficacité de bloquer les systèmes et de demander une rançon en échange. Cependant, cette amélioration des défenses des grandes entreprises a eu pour conséquence de diriger l'attention des cybercriminels vers les PME plus vulnérables. Cette délocalisation du risque vers des partenaires, sous-traitants ou clients, finit par affaiblir, de fil en aiguille, la sécurité des grandes entreprises.

La surface d'attaque s'agrandit avec l'accès distant aux systèmes, augmentant les points d'entrée et potentiellement provoquant un "effet domino" catastrophique. La cybersécurité requiert donc une approche globale, impliquant tous les acteurs de la chaîne de valeur.

Le Rôle Crucial de la Sensibilisation et de la Collaboration

Le maillon faible dans la chaîne de la cybersécurité est souvent le salarié lui-même, pouvant devenir un vecteur d'attaque involontaire. La sensibilisation à la cybersécurité est cruciale, mais elle n'est pas toujours intégrée pleinement dans la culture d'entreprise. Une approche fragmentée et hiérarchisée du management entrave souvent la coopération qui est nécessaire. Une culture partagée doit impliquer tous les niveaux hiérarchiques, avec une présence active des dirigeants et du management pour instaurer un environnement de sécurité. La lutte contre les menaces cybernétiques nécessite une hygiène numérique intégrée, constante et des pratiques de sécurité rigoureuses de la part de chacun.

Défis et Solutions pour les PME

La pénurie mondiale d'expertise en cybersécurité est exacerbée par le manque de ressources humaines accessibles pour les TPE et PME. De plus, ces entreprises ne perçoivent pas toujours l'importance cruciale de sécuriser l'information. L'augmentation des budgets ne suffit pas face à la sophistication grandissante des menaces et des technique.

La cybersécurité nécessite une approche holistique, une sensibilisation continue et une collaboration étendue. Les entreprises, quel que soit leur taille, doivent comprendre que la protection des données ne concerne pas seulement les systèmes, mais aussi les individus qui les utilisent

PILOTER VOTRE PROJET AVEC LA CHECKLIST

Nous vous avons préparé une Check-list pour le RGPD qui récapitule les étapes importantes à suivre pour assurer la conformité au Règlement Général sur la Protection des Données.

Cette check-list est une ressource de base pour vous guider dans votre démarche mais chaque entreprise est unique !II peut donc être nécessaire d'adapter cette liste en fonction de vos besoins spécifiques.

Sensibilisation et Engagement

- **Sensibilisation des Équipes :** Informer et sensibiliser les employés sur les principes et les exigences du **RGPD.**
- **Désignation d'un DPO** : Désigner un Délégué à la Protection des Données si nécessaire.
- **Désigner un relai RGPD en charge du dossier**

Identification des Données Personnelles

- **Inventaire des Données :** Identifier et inventorier les données personnelles traitées, stockées ou collectées ainsi que les service concernés
- **Apporter une attention particulière Profilage et Décisions Automatisées :** assurer l'information des personnes et l'opposition à ce mécanisme

Définition des Finalités et Bases Légales

- **Finalités du Traitement :** Définir clairement les finalités pour lesquelles les données sont collectées et traitées**.**
- **Bases Légales :** Identifier les bases légales (consentement, contrat, intérêt légitime, etc.) justifiant le traitement.

Informations aux Personnes Concernées

- **Politique de Confidentialité :** Mettre à jour et publier une politique de confidentialité transparente et compréhensible.
- **Droit à l'Information :** Informer les personnes concernées sur la collecte, l'utilisation et le traitement de leurs données.
- **Éducation des Utilisateurs :** Fournir des informations aux utilisateurs sur leurs droits en matière de protection des données et comment les exercer.

Consentement

- **Recueil du Consentement :** Obtenir un consentement clair et explicite lorsque requis, et enregistrer le consentement obtenu.
- **Consentement Parental pour les mineurs :** Obtenir le consentement parental pour le traitement des données des mineurs en dessous de l'âge de consentement locale.

Droits des Personnes Concernées

- **Droit d'Accès :** Mettre en place un processus pour répondre aux demandes d'accès des personnes concernées.
- **Droit à l'Oubli :** Définir des procédures pour effacer les données personnelles à la demande.
- **Droit de Portabilité :** Permettre la portabilité des données lorsque demandé.

Sécurité et Protection des Données

- **Mesures Techniques et Organisationnelles :** Mettre en place des mesures de sécurité pour protéger les données contre les atteintes.
- **Gestion des Violations de Données :** Élaborer un plan pour gérer les violations de données et les notifier selon les délais prescrits

Sous-Traitance et Transferts

- **Évaluation des Sous-Traitants :** Vérifier régulièrement que vos sous-traitants maintiennent également la conformité au RGPD.
- **Contrats avec les Sous-Traitants : Mettre en place des contrats avec les sous-traitants incluant les obligations de protection des données.**
- **Transferts de Données Hors UE :** Appliquer des mécanismes appropriés pour garantir la conformité lors de transferts hors de l'UE.

Analyse d'Impact sur la Protection des Données (AIPD)

- **Réalisation de l'AIPD :** Effectuer des analyses d'impact pour les traitements à risque élevé et mettre en place des mesures d'atténuation.

Registre des Activités de Traitement

- **Tenue du Registre :** Maintenir un registre des activités de traitement conformément à l'Article 30 du RGPD.
- **Formation Continue :** Assurer une formation continue des équipes sur les exigences du RGPD.

- **Évaluation Régulière :** Réévaluer régulièrement les mesures prises pour assurer la conformité continue.

Conformité du site internet et gestion des cookies et Technologies Similaires

- **Politique de Cookies :** Mettre en place une politique de cookies détaillant les cookies utilisés sur votre site web.
- **Consentement pour les Cookies :** Obtenir le consentement explicite des utilisateurs pour l'utilisation de cookies, sauf pour les cookies strictement nécessaires.

Gestion des Demandes des Autorités de Contrôle

- **Réponse aux Autorités de Contrôle :** Mettre en place des procédures pour répondre aux demandes et aux enquêtes des autorités de contrôle.

Amélioration continue

- **Mise en place de procédures de revues périodiques :** Effectuer des revues internes régulières pour évaluer la conformité continue et identifier les zones à améliorer.
- **Exigences Spécifiques du Secteur :** Si votre secteur a des exigences spécifiques en matière de protection des données (ex. : santé, finance), assurez-vous de les respecter.

LES 10 FICHES PRATIQUES DU RGPD

1. Clarification des Responsabilités et des Obligations

L'objectif de ce premier point est de revenir sur les obligations consacrées par le RGPD et les différentes responsabilités qu'il englobe.

- **Mettre en place et maintenir à jour une documentation**

Au vu du RGPD, les éléments documentaires englobent toutes les preuves de conformité. Cela implique la création et la mise à jour d'un registre des activités de traitement, d'un registre des sous-traitants, ainsi que la compilation de tous les documents liés à l'information des personnes (article 12 à 14) , tels que les notifications d'information et les politiques de confidentialité. Les responsables de traitement doivent, comme énoncé par l'article 5, être en mesure de démontrer leurs conformité.

- **Sécurité des Données**

L'article 32 prévoit la mise en place des mesures techniques et organisationnelles appropriées pour protéger les données personnelles contre la perte, l'accès non autorisé, la divulgation, etc.

- **Respecter les Notions de Privacy "by design et by default"**

L'Article 25 du RGPD appelle les organisations à intégrer des mesures techniques et organisationnelles appropriées tout au long du processus et ce, dès la conception des processus et par défaut dans les produits et services.

- **Assurer la Conformité des Sous-Traitants**

Mandatée par l'article 28 du RGPD, l'obligation d'assurer la conformité des sous-traitants garantit la protection des données à chaque étape de leur cycle de vie, particulièrement lors de leur transfert à un sous-traitant qui les traite pour le compte du responsable de traitement. L'existence de garanties adéquates en termes de mesures techniques et organisationnelles satisfait aux prescriptions du règlement, tout en préservant les droits des personnes concernées.

- **Garantir les Droits des Personnes concernées**

Les personnes dont les données sont traitées possèdent des droits personnels, que l'on retrouve aux articles 12 à 22 du RGPD : droit à l'information, droit à la rectification, droit d'accès, droit d'opposition, droit à l'effacement, droit à la portabilité et droit à la limitation du traitement. Il est crucial de leur procurer les moyens appropriés pour une exercice efficace de ces droits, en anticipant l'intégration d'outils techniques au sein des systèmes informatiques en vue d'une gestion optimisée.

- **Notifier les Incidents de Violation de Données**

Prévue aux articles 33 et 34 du RGPD, cette obligation prévoit qu'en cas de violation de données personnelles pouvant engendrer un risque pour les droits et libertés des individus, les organisations doivent notifier les autorités de contrôle et, dans certains cas, les personnes concernées.

- **Réaliser les Analyses d'Impact à la Protection des Données**

Consacrées aux articles 35 et 36 du texte, Les analyses d'impact sur la protection des données sont des outils essentiels de conformité. Elles

évaluent l'impact sur la protection des données en cas de traitements à risque élevé pour les droits et libertés des individus.

- **Transferts Internationaux de Données**

Les transferts de données personnelles hors de l'Union européenne sont soumis à des règles strictes pour garantir un niveau adéquat de protection. Les articles 44 à 50 précisent le cadre de ces transferts.

- **Nomination d'un Délégué à la Protection des Données**

Les articles 37 à 39 prévoient dans certains cas, la désignation obligatoire d'un DPO chargé de superviser la conformité en conseillant et en accompagnant les organisations et les métiers.

- **Et bien d'autres..**

Il est essentiel de souligner que cette liste n'est pas limitative, et que les obligations spécifiques peuvent différer en fonction de la nature du traitement et du rôle de l'entité impliquée. D'autres devoirs et principes guident les traitements de données, tels que l'exigence de consentement valide, le principe de réduction des données, la limitation des objectifs, les autorisations parentales pour les mineurs, les notifications préalables pour certaines activités de traitement, et bien d'autres encore.

2. Cartographie des Systèmes d'Information

Il est essentiel de reconnaître que la sécurité des systèmes d'information (SI) s'étend bien au-delà du numérique pour englober également le système d'information physique. Les deux aspects, numérique et physique, sont étroitement liés et interdépendants dans la protection globale d'une organisation. Prendre en compte à la fois les aspects numériques et physiques du SI permet de garantir une protection complète contre les menaces et les vulnérabilités, tout en assurant la continuité des opérations. Une approche holistique permet de minimiser les risques liés à la sécurité des données, d'assurer la confidentialité et l'intégrité des informations, ainsi que de préserver la disponibilité des services.

La présente section a pour objectif de fournir une démarche de cartographie des systèmes d'information. cette permet de visualiser l'ensemble des flux de données au sein de l'organisation, de comprendre comment les données circulent et sont traitées, ainsi que de déterminer les points de vulnérabilité potentiels.

Systèmes d'information numériques

- **Identification des Réseaux** : Il existe quatre catégories distinctes de réseaux informatiques en fonction de leur envergure (nombre de machines) et de leur portée :

- Le réseau personnel (PAN : Personal Area Network), couvrant une courte distance entre les machines ;
- Le réseau local (LAN : Local Area Network), adapté à un site d'entreprise ;
- Le réseau métropolitain (MAN : Metropolitan Area Network), étendu à l'échelle d'une ville ;

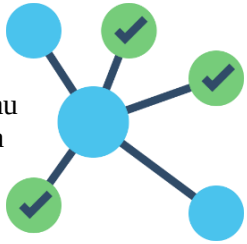
- Le réseau étendu (WAN : Wide Area Network), englobant une grande zone géographique, généralement à l'échelle d'un pays ou d'un continent.

- **Identification des Mesures de Sécurité** : Pare-feu, antivirus, VPN (Virtual Private Network), NAS (Stockage en Réseau) et outils de sauvegarde, ainsi que les gestionnaires de mots de passe, sont des exemples de dispositifs de sécurité à prendre en compte.

- **Identification des Outils d'Administration :** Toutes les opérations d'installation, de suppression, de modification et de configuration d'un système participant au SI qui peuvent altérer son fonctionnement ou sa sécurité sont incluses. Un exemple d'outil est l'Active Directory (AD) qui permet de gérer les droits d'accès, les configurations et les autorisations au sein du système d'information.

- **Identification des Périphériques** : Des postes informatiques aux imprimantes et scanners, mais aussi tout ce qui compose l'internet des objets, chaque élément de mon réseau peut présenter un risque pour mon entreprise. Les identifier permet de les sécuriser et de les maintenir à jour pour atténuer les risques liés à la cybersécurité.

- **Identification des Logiciels (Locaux ou Web)** :Il est nécessaire de vérifier l'authenticité et l'origine des logiciels utilisés. Par ailleurs, la mise à jour constante des logiciels est essentielle pour réduire les risques. Il est crucial d'identifier les logiciels qui ne reçoivent plus de mises à jour afin de prendre des mesures. Les logiciels en mode web (SAAS) présentent également des risques en termes d'accès au réseau et aux données. Il convient de vérifier la sécurité proposée par l'éditeur et sa conformité à la réglementation**.**



- **Identification des Serveurs** : Les serveurs jouent fréquemment un rôle essentiel dans le système. La sécurisation, l'accès restreint et la

protection optimale de ces dispositifs sont primordiaux. La sécurisation physique et logique des serveurs permet de garantir la continuité des opérations.

Systèmes d'Informations Physiques

La gestion des systèmes d'information ne se limite pas uniquement à l'environnement numérique, mais englobe également le domaine physique où des données sensibles peuvent être en circulation. Cette approche holistique garantit la protection complète des informations confidentielles et assure la conformité aux réglementations telles que le RGPD.

- **Identification des Mesures de Cloisonnement**: L'accès aux informations physiques, telles que les fiches de paie et les contrats de travail, est également encadré par le RGPD. En identifiant les documents en circulation au sein de votre organisation et en les classant, vous pouvez déterminer les droits d'accès nécessaires et mettre en place des mesures appropriées. Cela peut inclure des mesures telles que des armoires verrouillées, la gestion des clés et des accès restreints.

- **Identification des Mesures de Minimisation**: Le RGPD interdit la collecte d'informations personnelles sans finalités spécifiques. Une procédure d'analyse des documents et des applications est essentielle pour déterminer les données réellement nécessaires, évitant ainsi la collecte inutile.

- **Identification des Mesures d'Anonymisation et de Pseudonymisation**: Pour certains traitements, il peut ne pas être nécessaire d'identifier les personnes concernées. L'anonymisation et la pseudonymisation des données sont des techniques permettant de respecter les principes de proportionnalité et de minimisation des risques.

- **Formations et Sensibilisation des Utilisateurs**: L'élément humain est l'une des principales sources de risques en matière de protection des données. Pour atténuer ces risques et intégrer les équipes dans un effort collectif de sécurisation, la sensibilisation et la formation des collaborateurs aux bonnes pratiques et aux obligations réglementaires sont cruciales.

- **Identification des Mentions d'Informations :** La transparence dans le traitement des données personnelles est imposée par le RGPD. Cela nécessite des documents tels que les politiques de confidentialité, les chartes d'utilisation des systèmes d'information, les clauses de sous-traitance et bien d'autres, pour informer les individus sur la manière dont leurs données sont traitées.

- **Identification des Mesures de Contrôles et de Qualité**: Certaines réglementations, y compris les normes ISO et certifications, peuvent avoir un impact direct ou indirect sur le RGPD. Identifier les éléments permettant de justifier ou d'améliorer ces aspects est nécessaire pour garantir la conformité et la qualité.

- **Identification des Fournisseurs de Système d'Information :** L'accès aux informations et aux systèmes d'information doit être réglementé par des contrats spécifiques, définissant clairement les limites d'action des fournisseurs. Aucun fournisseur ne devrait avoir accès à votre système d'information sans avoir accepté préalablement les dispositions légales et contractuelles.

La combinaison de mesures physiques et numériques dans la gestion des systèmes d'information assure une protection holistique des données et renforce la confiance dans le traitement responsable des informations.

Sécurisation du SI suivant les données et le risque associé

La cartographie des systèmes d'information se révèle être une étape stratégique cruciale pour la gestion efficiente des données. En offrant une vue globale cohérente de l'écosystème numérique de l'organisation, elle permet de déterminer les emplacements de stockage, de traitement et d'échange des données, offrant ainsi la possibilité de repérer les zones de vulnérabilités potentielles et d'instaurer des mesures de sécurité adaptées aux menaces, qui s'inscrit elles même dans un processus d'amélioration continue.

Également, l'identification des zones abritant les données les plus vulnérables permet la mise en place de précautions de sécurité préventives pour réduire le risque d'atteinte à la confidentialité des données et de cyberattaques. En ce sens, les données les plus sensibles ou stratégique doivent impérativement bénéficier de mesures de sécurité supplémentaire. Par exemple, le serveur doit être physiquement protégé (salle fermé à clefs, protection contre les incendies..), mais aussi informatiquement parlant : le chiffrement permet de sécuriser les données sur le serveur et de limiter les risques en cas d'accès non autorisé.

Ainsi, la gestion des systèmes d'information physiques et numériques inclus l'évaluation de la résilience des systèmes d'information via des test d'intrusion par exemple, la mise en place des plan de communication en cas d'incident, de plan de reprise d'activité et de plan de continuité d'activité, ou encore, la gestion efficace des sauvegarde.

A noter qu'une une norme internationale dédiée à la sécurité de l'information existe, il s'agit de la norme ISO 27001. Elle définit les meilleures pratiques et les exigences pour établir, mettre en œuvre, exploiter, surveiller, réviser, maintenir et améliorer un système de gestion de la sécurité de l'information (SGSI) au sein d'une organisation.

3 Identification et gestion des relations de sous-traitance

La sous-traitance des données

Lorsqu'un traitement de données personnelles doit être réalisé pour le compte d'un responsable du traitement, celui-ci engage des sous-traitants qui doivent garantir la mise en place de mesures techniques et organisationnelles adéquates, conformes aux exigences du RGPD et assurant la protection des droits des personnes concernées.

Dans la pratique : L'entité qui fait appel à des services de sous-traitance pour le traitement de données doit s'assurer que le sous-traitant choisi est également en conformité avec la réglementation. Cette phase d'évaluation, qui peut inclure des audits ou des questionnaires de sécurité est primordiale, dans la mesure où le responsable de traitement est juridiquement responsable de ses sous-traitants.

Comment procéder ?

1. **Établir un contrat clair :** Le responsable du traitement et le sous-traitant doivent signer un contrat contenant diverses mentions obligatoires énumérées dans l'article 28.3 du RGPD. Celui-ci doit également spécifier clairement les engagements en matière de sécurité des données, les obligations en cas de violation de données, les procédures de gestion des incidents, ainsi que les responsabilités en matière de protection des droits des personnes concernées. Le contrat devrait préciser Le contrat doit également clairement définir les responsabilités. Des mentions concernant la sous-traitance ultérieur ainsi que les transferts internationaux de données doivent également être prévues.

2. **Documenter l'activité de sous-traitance :** Le sous-traitant doit mettre à disposition du responsable du traitement toutes les informations nécessaires pour prouver qu'il respecte ses obligations.

Il est essentiel que le sous-traitant présente des garanties suffisantes :

- Il doit proposer des solutions et des outils qui assurent le respect de la confidentialité des données personnelles.
- Il doit avoir mis en place les mesures techniques et organisationnelles qui permettent de garantir la sécurité des données

Le sous-traitant joue également un rôle d'assistance et de conseil envers le responsable du traitement :

- Il doit alerter le responsable du traitement si une instruction qu'il reçoit semble enfreindre la réglementation.
- Il est tenu d'aider le responsable du traitement dans le traitement des demandes d'exercice des droits des personnes concernées.

La sécurité des données est un aspect crucial :

- Le responsable du traitement doit choisir un sous-traitant qui offre des garanties de sécurité suffisantes.
- Le sous-traitant doit mettre en place un niveau de sécurité approprié en fonction de la nature des données collectées pour le compte du responsable du traitement (article 32 du RGPD).

En cas de violation de données, le sous-traitant a également l'obligation d'assister le responsable du traitement dans ses obligations de notification

à l'autorité de protection des données (CNIL en France) et de communication à la personne concernée, le cas échéant.

L'amélioration continue :

La relation avec un sous-traitant ne se limite pas à la signature du contrat initial. Il est recommandé de mettre en place des mécanismes d'amélioration et de vérification continue pour s'assurer que le sous-traitant respecte les engagements contractuels et maintient un niveau adéquat de sécurité des données.

Le cas particulier des prestataires du SI

Dans le contexte de la sous-traitance, les prestataires du système d'information (SI) occupent une place spécifique en raison de l'accès qu'ils ont à des parties essentielles de votre infrastructure technologique et de l'impact direct sur la sécurité des données personnelles. Leur rôle est crucial pour le bon fonctionnement et la sécurité de vos opérations, ce qui requiert une attention particulière lors de l'élaboration de contrats et de la mise en œuvre de garantie. En établissant des contrats soignés, en assurant la transparence, en surveillant la conformité et en collaborant activement, vous garantirez la sécurité et la protection adéquate des données personnelles ainsi qu'une gestion des risques efficace.

4 Identification des caractéristiques du traitement

Dans le cadre de la rédaction du registre de traitement, le RGPD exige la mise en place d'une base légale claire pour chaque traitement de données personnelles. Cette base légale justifie le traitement en fonction de la situation spécifique. Parallèlement, les finalités définissent les objectifs poursuivis par la collecte et le traitement de ces données.

Identification des Bases Légales

Chaque traitement de données doit reposer sur une base légale. Les bases légales peuvent inclure le consentement de la personne concernée, l'exécution d'un contrat, l'obligation légale, la protection des intérêts vitaux, l'exécution d'une mission d'intérêt public ou l'exercice d'une autorité publique, ainsi que des intérêts légitimes poursuivis par le responsable du traitement ou un tiers. Si le consentement est requis comme base légale, celui-ci doit répondre doit spécifique, libre, éclairé et non équivoque.

A noter que pour une catégorie spécifique de données, dites données particulières le teste prévoit des bases légales spécifiques, au vue de la nature délicate des données. Le RGPD (Règlement général sur la protection des données) établit des bases légales spécifiques pour le traitement de ces données sensibles.

Identification des Finalités et des sous finalités

Les finalités déterminent la raison d'être du traitements Elles doivent être en accord avec les missions et les activités de l'organisme. Par exemple, elles peuvent inclure la gestion des relations avec les clients, la fourniture de services, la gestion des ressources humaines, la communication marketing, la sécurité des biens et des personnes, etc.

Les finalités délimitent l'acticité de traitement. Celles -ci doivent être compatibles les unes avec les autres, c'est pour cela que nous avons un approche plus particulière. Nous considérons que le traitement suit une finalité principale, et que l'ensemble des sous finalités représentent finalement les différentes étapes, les différents processus métiers qui permettent de répondre à la finalité principale.

5. Gestion et Référencement des Périodes de Conservation

La durée de conservation des données personnelles est un aspect crucial de la conformité au RGPD. Le responsable du traitement doit déterminer une période appropriée pendant laquelle les données seront conservées en fonction de l'objectif initial de leur collecte. Cette étape est essentielle pour éviter une conservation excessive et pour garantir le respect des droits des personnes concernées.

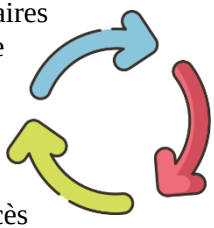
Cycle de Vie de la Donnée Personnelle

Le cycle de vie de la donnée personnelle peut être divisé en différentes phases, chacune ayant des implications spécifiques en matière de conservation :

Phase 1 : Conservation en Base Active

Pendant cette phase, les données personnelles sont activement utilisées pour atteindre l'objectif initial de leur collecte. Il s'agit de la période nécessaire à la réalisation de la finalité du traitement. Par exemple, les données peuvent être stockées dans des systèmes tels que les CRM ou les ERP et être facilement accessibles dans l'environnement de travail immédiat.

Phase 2 : Archivage Intermédiaire



Lorsque les données personnelles ne sont plus nécessaires pour atteindre l'objectif initial, elles entrent dans cette phase. Les données peuvent encore avoir une valeur administrative, par exemple pour gérer d'éventuels litiges ou pour répondre à des obligations légales spécifiques. Pendant cette période, les données doivent être conservées dans des conditions de sécurité et d'accès

contrôlé, en prévoyant des consultations ponctuelles et justifiées par des personnes spécifiquement autorisées.

Phase 3 : Archivage Définitif

Certaines données personnelles peuvent avoir une valeur historique, juridique ou scientifique et peuvent être archivées de manière permanente. Ces données doivent être traitées avec soin et stockées dans des conditions qui garantissent leur intégrité et leur accessibilité à long terme.

Facteurs à Considérer pour Déterminer les Durées de Conservation

Plusieurs facteurs doivent être pris en compte pour déterminer la durée de conservation appropriée des données personnelles :

- **Objectif Initial :** La finalité pour laquelle les données ont été collectées détermine en grande partie la durée de conservation. Les données ne doivent être conservées que tant que cet objectif est valide.
- **Obligations Légales :** Les obligations légales spécifiques concernant la conservation des données, telles que les périodes de conservation imposées par la loi, doivent être respectées.
- **Risques Juridiques :** Les risques de litiges ou de contentieux doivent être pris en compte. Les données nécessaires pour la défense juridique doivent être conservées en conséquence.
- **Intérêts des Personnes Concernées :** Les droits et les préférences des personnes concernées doivent être pris en compte. Les données ne doivent pas être conservées plus longtemps que nécessaire par rapport à leurs attentes.
- **Évolution Technologique :** Les évolutions technologiques peuvent influencer la manière dont les données sont stockées et rendues accessibles. Il convient de garantir que les données restent exploitables malgré les changements technologiques.

Documentation et Transparence

Il est essentiel de documenter les périodes de conservation pour chaque type de données et de s'assurer que ces informations sont claires et transparentes pour les personnes concernées. Les politiques de conservation doivent être accessibles dans les politiques de confidentialité et autres communications liées à la protection des données.

Réévaluation et Mise à Jour

Les durées de conservation doivent être régulièrement réévaluées pour s'assurer qu'elles restent appropriées en fonction de l'évolution des objectifs, des obligations légales et des risques. Les données doivent être supprimées ou anonymisées une fois qu'elles ne sont plus nécessaires aux fins initiales pour lesquelles elles ont été collectées.

6. Mise en Place des Droits des personnes Concernés

Le RGPD accorde aux personnes concernées un ensemble de droits puissants pour contrôler leurs données personnelles. En tant que responsable du traitement, il est de votre devoir de garantir que ces droits sont respectés et que les personnes concernées peuvent exercer leurs droits de manière transparente et efficace.

Droits des Personnes Concernées Conformément au RGPD

1. Droit d'Accès : Les personnes concernées ont le droit de demander et d'obtenir des informations sur les données personnelles que vous traitez à leur sujet. Vous devez fournir des détails sur les finalités du traitement, les catégories de données traitées, les destinataires et la durée de conservation.

2. Droit de Rectification : Les personnes concernées peuvent demander la correction de données personnelles inexactes ou incomplètes.

3. Droit à l'Oubli : Aussi appelé droit à l'effacement, les personnes concernées peuvent demander la suppression de leurs données personnelles lorsque celles-ci ne sont plus nécessaires aux fins pour lesquelles elles ont été collectées, lorsque le consentement est retiré ou lorsque le traitement est illégal.

4. Droit de Restriction du Traitement : Les personnes concernées peuvent demander la suspension temporaire du traitement de leurs données dans des situations spécifiques, par exemple, lorsque l'exactitude des données est contestée.

5. Droit à la Portabilité des Données : Les personnes concernées ont le droit de recevoir les données personnelles qu'elles ont fournies dans un

format structuré et couramment utilisé, et de les transmettre à un autre responsable du traitement si nécessaire.

6. Droit d'Opposition : Les personnes concernées peuvent s'opposer au traitement de leurs données personnelles, notamment pour le marketing direct ou lorsque le traitement est basé sur l'intérêt légitime du responsable du traitement.

7. Prise de Décision Automatisée et Profilage : Les personnes concernées ont le droit de ne pas être soumises à une décision basée uniquement sur un traitement automatisé, y compris le profilage, si cette décision produit des effets juridiques ou affecte significativement la personne.

Mise en Œuvre des Droits

Transparence : Informez les personnes concernées de l'existence de ces droits, de la manière dont elles peuvent les exercer et de la procédure à suivre.

Procédures Internes : Établissez des procédures internes pour répondre aux demandes des personnes concernées et pour assurer une gestion efficace et sécurisée de leurs droits.

Délais de Réponse : Respectez les délais légaux pour répondre aux demandes des personnes concernées (généralement dans un délai d'un mois).

Identité de la Personne Concernée : Vérifiez l'identité de la personne concernée pour éviter toute divulgation non autorisée de données.

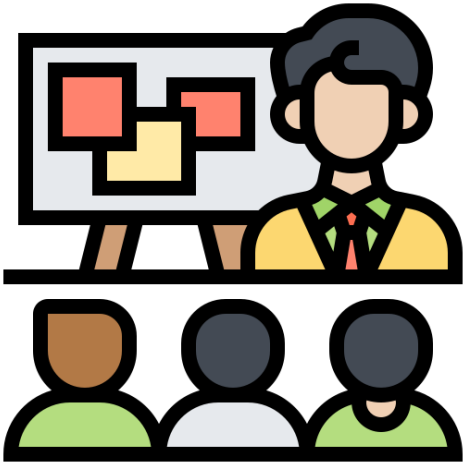
Réponses Complètes : Fournissez des réponses complètes et transparentes aux demandes, en expliquant les mesures prises.

Collaboration avec le Délégué à la Protection des Données (DPD) : Si désigné, travaillez en collaboration avec le DPD pour garantir la conformité avec les droits des personnes concernées.

Sensibilisation et Formation

Il est crucial que les membres de votre équipe comprennent les droits des personnes concernées et soient formés pour répondre efficacement aux demandes. La sensibilisation à la protection des données et à la confidentialité devrait être intégrée dans la culture organisationnelle.

En mettant en place des procédures solides, en garantissant la transparence et en répondant de manière adéquate et respectueuse aux demandes des personnes concernées, vous démontrez votre engagement envers la protection des données et contribuez à renforcer la confiance des personnes dans la manière dont vous traitez leurs informations personnelles.



7. Identification et Gestion des Transferts au-delà de l'Union Européenne

Avec la globalisation des échanges et l'utilisation croissante des nouvelles technologies, le transfert de données personnelles hors de l'Union européenne (UE) et de l'Espace Économique Européen (EEE) est devenu courant. Cependant, il est impératif d'assurer un niveau de protection des données équivalent à celui offert par le RGPD lors de ces transferts. Pour cela, différentes mesures et outils juridiques sont à disposition.

Transfert de Données en Dehors de l'UE/EEE : Implications

Lorsque des données personnelles sont transférées en dehors de l'UE/EEE, il peut y avoir des risques pour la protection des données, car les lois sur la protection des données peuvent varier d'un pays à l'autre. Les données peuvent être soumises à des réglementations moins strictes, ce qui peut compromettre la confidentialité et la sécurité des données personnelles.

Mécanismes Juridiques pour Assurer un Niveau de Protection Adéquat

Plusieurs mécanismes juridiques sont disponibles pour garantir un niveau de protection adéquat lors des transferts de données hors de l'UE/EEE :

1. Décision d'Adéquation : La Commission européenne peut déterminer qu'un pays tiers assure un niveau de protection adéquat des données, ce qui permet des transferts sans mesures supplémentaires.

2. Clauses Contractuelles Types (CCT) : Des clauses contractuelles types approuvées par la Commission européenne peuvent être incluses dans les contrats entre le responsable du traitement et le sous-traitant ou entre des parties qui transfèrent des données.

3. Règles d'Entreprise Contraignantes (BCR) : Les BCR sont des règles internes de protection des données adoptées par un groupe d'entreprises et approuvées par l'autorité de contrôle compétente.

4. Mécanismes de Certification : Des mécanismes de certification peuvent être utilisés pour démontrer que le transfert respecte les normes de protection des données.

5. Clause de Dérogation : Le transfert peut également être autorisé dans des situations spécifiques, par exemple lorsque la personne concernée a donné son consentement explicite et informé.

Évaluation des Risques et Mesures de Protection Supplémentaires

Lorsque vous envisagez de transférer des données en dehors de l'UE/EEE, il est essentiel d'effectuer une évaluation des risques pour déterminer si le pays de destination assure un niveau adéquat de protection des données. Si des risques subsistent, des mesures de protection supplémentaires doivent être mises en place.

1. Analyse de Risque : Évaluez les risques associés au pays de destination, y compris les lois locales sur la protection des données et la sécurité.

2. Mesures Supplémentaires : En fonction des résultats de l'analyse de risque, des mesures de protection supplémentaires, telles que le chiffrement, peuvent être mises en place pour renforcer la sécurité des données.

3. Consultation de l'Autorité de Contrôle : Si des risques subsistent malgré les mesures prises, consultez l'autorité de contrôle compétente avant d'effectuer le transfert.

Documentation et Transparence

Documentez soigneusement les transferts de données hors de l'UE/EEE, en indiquant les mécanismes juridiques utilisés, les mesures de protection mises en place et les résultats de l'analyse de risque. Informez également les personnes concernées sur les transferts de leurs données et les mesures de protection appliquées.

Conformité Continue

Assurez-vous que les transferts de données hors de l'UE/EEE sont régulièrement réévalués pour garantir leur conformité continue avec les mécanismes juridiques et les mesures de protection.

8. Établissement et Actualisation du Registre des Traitements

L'article 30 du RGPD impose à chaque responsable du traitement, ainsi qu'au représentant du responsable du traitement le cas échéant, de tenir un registre des activités de traitement effectuées sous leur responsabilité. Ce registre joue un rôle crucial dans la démonstration de la conformité aux obligations du RGPD et dans la garantie de la transparence dans le traitement des données personnelles.

Éléments à Documenter dans le Registre des Activités de Traitement
Chaque registre des activités de traitement doit contenir une série d'éléments clés pour chaque traitement de données personnelles :

Nom et Coordonnées des Intervenants : Identifiez les responsables du traitement, les sous-traitants éventuels et, le cas échéant, le représentant du responsable du traitement.
Finalités et Sous-Finalités des Traitements : Précisez l'objectif global du traitement, ainsi que les objectifs spécifiques qui s'y rattachent.
Typologies de Données Traitées : Indiquez les catégories de données personnelles traitées, telles que les données d'identification, les données de contact, les données sensibles, etc.
Durées de Conservation : Précisez la période pendant laquelle les données seront conservées, en fonction de l'objectif initial de la collecte.
Source des Données : Indiquez la provenance des données personnelles, que ce soit directement auprès de la personne concernée ou auprès d'autres sources.
Catégories des Personnes Concernées : Identifiez les catégories de personnes concernées par le traitement, par exemple, les clients, les employés, les fournisseurs, etc.
Catégories des Destinataires (Sous-Traitants) : Listez les catégories de destinataires auxquels les données peuvent être divulguées, notamment les sous-traitants impliqués.

Mesures Techniques et Organisationnelles : Décrivez les mesures mises en place pour garantir la sécurité et la protection des données.

Transferts Hors de l'UE/EEE : Mentionnez les transferts de données personnelles hors de l'Union européenne ou de l'Espace Économique Européen, ainsi que les mesures de protection mises en place.

Fondements Juridiques : Indiquez les bases légales qui justifient le traitement des données, telles que le consentement, l'exécution d'un contrat ou l'intérêt légitime.

Dans notre logiciel

Chaque traitement de données personnelles est lié à une fiche de traitement détaillée. Pour établir ces fiches de traitement, il est nécessaire de compléter les étapes d'identification précédemment mentionnées (de 1.1 à 1.6), telles que la définition des finalités, la détermination des bases légales, la gestion des durées de conservation, etc.

Conformité Continue et Facilitation des Contrôles

La tenue d'un registre des activités de traitement offre plusieurs avantages, notamment :
Conformité : Il facilite la démonstration de la conformité aux obligations du RGPD en fournissant une vue complète des traitements de données personnelles.
Contrôles et Audits : Il permet de faciliter les contrôles par les autorités de contrôle et les audits internes en fournissant des informations transparentes et précises.
Gestion des Risques : Il contribue à identifier et à gérer les risques liés au traitement des données personnelles.

9. Réalisation d'Analyses d'Impact sur la Protection des Données (PIA)

L'Analyse d'Impact sur la Protection des Données (AIPD), également connue sous le nom d'Évaluation d'Impact sur la Vie Privée (PIA), est un outil essentiel pour garantir la conformité au RGPD et pour préserver le respect de la vie privée. L'AIPD vise à identifier et à atténuer les risques associés au traitement des données personnelles, en particulier lorsque ces traitements présentent un risque élevé pour les droits et libertés des personnes concernées.

Obligation de Réalisation de l'AIPD

L'AIPD est obligatoire dans les cas suivants :

1. **Le traitement envisagé figure dans la liste** des types d'opérations de traitement pour lesquelles la CNIL a déterminé qu'une analyse d'impact relative à la protection des données est obligatoire.
2. L**e traitement remplit au moins deux des neuf critères** énoncés dans les lignes directrices du Groupe de Travail de l'Article 29 (G29) :

    - Évaluation/Scoring (y compris le profilage).
    - Décision automatique avec effet légal ou similaire.
    - Surveillance systématique.
    - Collecte de données sensibles ou données à caractère hautement personnel.
    - Collecte de données personnelles à grande échelle.
    - Croisement de données.
    - Personnes vulnérables (patients, personnes âgées, enfants, etc.).
    - Usage innovant (utilisation d'une nouvelle technologie).

- Exclusion du bénéfice d'un droit/contrat.

Objectifs de l'AIPD

L'objectif principal de l'AIPD est d'identifier et d'évaluer les risques pour les droits et libertés des personnes concernées liés au traitement des données personnelles. Une fois ces risques identifiés, des mesures d'atténuation appropriées peuvent être mises en place pour réduire ces risques à un niveau acceptable.

Outil de Réalisation des AIPD

La CNIL met à disposition un outil pour faciliter la réalisation des AIPD. Cet outil permet aux responsables du traitement d'évaluer les risques associés à un traitement de données personnelles et de déterminer les mesures nécessaires pour assurer la protection des droits et libertés des personnes concernées.

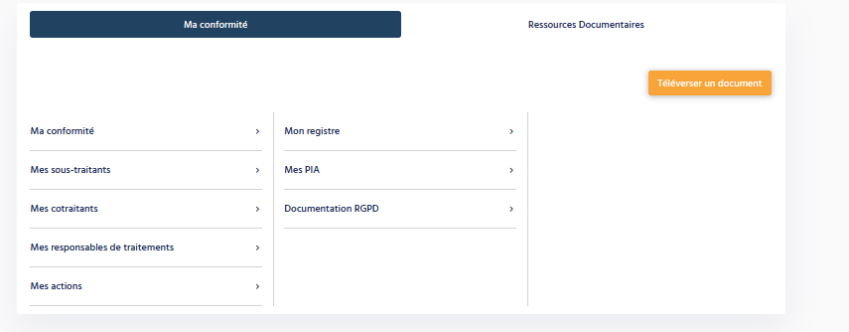
L'outil de réalisation des AIPD peut être téléchargé via le lien suivant : [Lien vers l'outil PIA de la CNIL]

Intégration des Résultats de l'AIPD

Les résultats de l'AIPD doivent être documentés et intégrés dans le registre des activités de traitement. Ils doivent également être pris en compte lors de la conception du traitement et dans la mise en œuvre de mesures de protection des données.

10. Documentation des Processus

Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu.



GLOSSAIRE

Autorité de contrôle : Une autorité publique indépendante chargée de superviser et d'assurer la mise en œuvre du RGPD dans un État membre de l'UE.

Bases légales du traitement : Les motifs juridiques qui justifient le traitement des données à caractère personnel, tels que le consentement, l'exécution d'un contrat, l'intérêt légitime, etc.

Consentement : L'expression volontaire, spécifique, éclairée et univoque de la personne concernée par laquelle elle accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant soient traitées.

Délégué à la protection des données (DPO) : La personne chargée de superviser la conformité au RGPD au sein d'une organisation et d'agir en tant que point de contact pour les questions de protection des données.

Destinataire : La personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers.

Données à caractère personnel sensibles : Les données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques, l'appartenance syndicale, la santé ou la vie sexuelle d'une personne.

Informatique et libertés : La notion de protection des données et de respect de la vie privée qui est au cœur du RGPD.

Limitation du traitement : Le marquage de données à caractère personnel conservées, en vue de limiter leur traitement futur.

Portabilité des données : Le droit des personnes concernées de transférer leurs données personnelles d'un responsable du traitement à un autre, dans un format lisible par machine.

Privacy by Default (Protection des données par défaut) : Le principe selon lequel les paramètres de protection des données les plus élevés doivent être automatiquement activés sans intervention de l'utilisateur.

Privacy by Design (Protection des données dès la conception) : Une approche de développement qui intègre dès le début les principes de protection des

données pour garantir que les données à caractère personnel sont traitées de manière sécurisée et conforme au RGPD.

Privacy Impact Assessment (PIA) : Une évaluation de l'impact sur la protection des données pour identifier et atténuer les risques liés à un traitement spécifique de données.

Profilage : Toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique.

Responsabilité conjointe du traitement : Lorsque deux ou plusieurs responsables du traitement déterminent conjointement les finalités et les moyens du traitement.

Responsable du traitement : La personne physique ou morale, l'autorité publique, le service ou un autre organisme qui détermine les finalités et les moyens du traitement.

Sous-traitant : 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.

Traitement : Toute opération ou tout ensemble d'opérations effectuées sur des données à caractère personnel.

Transfert de données hors de l'UE : Le mouvement de données à caractère personnel en dehors de l'Union européenne vers des pays tiers qui ne sont pas considérés comme assurant un niveau adéquat de protection des données.

Violation de données à caractère personnel : Une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel.

Violation du droit à la protection des données : Toute infraction aux dispositions du RGPD pouvant entraîner des sanctions.


MDP
DATA PROTECTION