Tout savoir sur le RGPD

DPO Agency
By PEB

Édito

Depuis le 25 mai 2018, la mise en conformité au RGPD est devenue obligatoire pour toute structure européenne de toute taille et de tout statut juridique, traitant des données personnelles. Cette réglementation est encadrée par la CNIL, Commission Nationale de l'Informatique et des Libertés. Par rapport à la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, le RGPD est une évolution majeure en matière de protection des données personnelles.

L'objectif principal de ce livre blanc est de vous prouver que cette réglementation est un avantage et une opportunité pour votre structure !

Pour se faire, nous mettrons en lumière les objectifs de cette loi, les répercussions sur les données personnelles, les différentes sanctions encourues. Nous vous proposerons une boîte à outils pour vous accompagner dans votre démarche de conformité.

Au-delà de l'amende encourue en cas de non-conformité, ce livre blanc sensibilise à l'opportunité de développement commercial des entreprises et des bénéfices de la mise en conformité du RGPD en Europe.

Le RGPD une opportunité de se démarquer de sa concurrence afin de développer sa clientèle et la confiance des clients !

En tant que Déléguée à la Protection des Données, DPO, externalisée, nombreuses sont les questions que l'on me pose sur le RGPD. C'est pourquoi, j'ai voulu créer ce livre blanc pour aider à la compréhension de cette loi et proposer des outils pratiques, pour répondre de façon concrètes et précises aux interrogations liées à ce règlement.

Bonne lecture !

Sommaire

Les références & liens utiles

La CNIL www.cnil.fr
L'ANSSI www.ssi.gouv.fr·
MOOC www.secnumacademie.gouv.fr

DPO Agency
By PEB

RGPD
dates & chiffres clés

#01

Le RGPD ou Règlement Général sur la Protection des Données de la CNIL est le nouveau cadre européen qui concerne le traitement et la circulation des données à caractère personnel. Il s'agit des informations sur lesquelles les entreprises s'appuient pour proposer des services et des produits.

Ce texte couvre l'ensemble des résidents de l'Union européenne.

Tous les textes de loi précédents sont abrogés par le RGPD.

2 ans se sont écoulés depuis la mise en vigueur de cette loi, le 25 mai 2018.

En seulement un an, les notifications de violations de données sont passées à 2 044 (contre 600 au bout de 4 mois) et les plaintes de 3 797 à + de 11 900 sur la même période :

Une augmentation des réclamations en raison d'une violation des règles relatives à la protection des données personnelles (+32,5 % de plaintes en 2018 par rapport à 2017)

L'origine du RGPD vient du constat fait par la Commission européenne que la législation d'alors, entrée en vigueur en 1995, nécessitait une réactualisation pour tenir compte des évolutions technologiques.

En 2012, Bruxelles a proposé un nouveau règlement, en étalement jusqu'en 2016, avec le 15 décembre 2015, un accord entre le Conseil, le Parlement et la Commission.

Le parcours du texte au niveau européen s'est fait dans un contexte particulier : le 13 mai 2014, la Cour de justice de l'Union européenne rendait son fameux arrêt : celui-ci oblige Google à donner satisfaction aux internautes du territoire qui demandent le retrait de résultats qui les concernent, consacrant ainsi l'existence d'un droit au déréférencement (une sorte de droit à l'oubli « allégé ») sur le net.

Le déploiement du RGPD dans l'espace européen s'est fait en deux temps :

Il y a d'abord eu, le 14 avril 2016, l'adoption définitive du texte par le Parlement, suivi quelques jours plus tard, le 27, de sa promulgation au Journal Officiel.

Cependant, son application ne s'est pas déroulée en même temps : il a été décidé de la décaler de deux ans, au 25 mai 2018.

Ce délai a été fixé pour permettre aux législations nationales et aux entités procédant à la collecte et au traitement des données personnelles de s'y préparer.

Depuis le 25 mai, tout traitement en infraction avec le RGPD peut entraîner des sanctions.

Qui doit se conformer au RGPD ?

#02

Toute entité manipulant des données personnelles concernant des Européens doit se conformer à cette loi, qu'il s'agisse d'une entreprise publique ou privée, d'un sous-traitant, ou même d'une association, d'une école, d'un auto-entrepreneur, d'un indépendant, d'un commerçant.

Attention : le texte ne s'applique pas qu'aux organisations établies sur le territoire national.
Un groupe américain, japonais ou chinois qui collecte et traite des données personnelles européennes doit aussi s'y conformer.
Des géants comme Google, Facebook, Amazon ou encore Uber doivent donc tenir compte des modalités du RGPD s'ils veulent continuer sans risque à fournir des biens et des services à la population européenne.

La taille de l'entreprise, son secteur d'activité, son statut ou son caractère public ou privé n'entre pas en ligne de compte.
Par exemple, une entreprise qui se lance dans de l'e-santé doit être en conformité.

Définition d'une donnée personnelle

#03

Une donnée personnelle (ou donnée à caractère personnel) est une information qui concerne une personne physique, identifiée directement ou indirectement.

Exemples : un nom, une photo, une adresse IP, un numéro de téléphone, une adresse mail, un identifiant de connexion informatique, une adresse postale, une empreinte, un enregistrement vocal, un numéro de sécurité sociale, un enregistrement sur pointeuse ou sur un système de géolocalisation, des coordonnées bancaires, les CV de candidats, les fiches de paie, etc.
Dès lors qu'une entreprise a des clients, des prospects, des sous-traitants, des salariés, des fournisseurs, des partenaires, elle possède des données personnelles.

Certaines données personnelles sont dites « sensibles » , car elles touchent à des informations qui peuvent donner lieu à de la discrimination ou des préjugés :
Une opinion politique, une sensibilité religieuse, un engagement syndical, une appartenance ethnique, une orientation sexuelle, une situation médicale ou des idées philosophiques sont des données sensibles.
Elles ont un cadre particulier, qui interdit toute collecte préalable sans consentement écrit, clair et explicite, et pour des cas précis, validés par la CNIL et dont l'intérêt public est avéré.

Objectifs du RGPD

#04

L'objectif du RGPD est d'être le nouveau texte de référence dans l'Union européenne au sujet des données personnelles.
Une réforme de la législation européenne apparaissait nécessaire au regard de sa vétusté, révélée par l'explosion du numérique, l'apparition de nouveaux usages et la mise en place de nouveaux modèles économiques.
Il s'agit aussi d'harmoniser le cadre juridique européen en matière de protection des données personnelles, afin qu'il n'y ait qu'un seul et même texte de lois qui s'applique parmi l'ensemble des États membres, que ce soit en France, en Allemagne, en Italie ou en Espagne, ainsi que dans la vingtaine d'autres pays de l'Union Européenne.

Avantages pour les clients

L'objectif du RGPD est d'être le nouveau texte de référence dans l'Union européenne au sujet des données personnelles.
Une réforme de la législation européenne apparaissait nécessaire au regard de sa vétusté, révélée par l'explosion du numérique, l'apparition de nouveaux usages et la mise en place de nouveaux modèles économiques.
Il s'agit aussi d'harmoniser le cadre juridique européen en matière de protection des données personnelles : un seul et même texte de lois s'appliquant parmi l'ensemble des États membres, que ce soit en France, en Allemagne, en Italie ou en Espagne, ainsi que dans la vingtaine d'autres pays de l'Union Européenne.

Avantages pour les clients

Du point de vue de l'internaute, le RGPD met en place ou conforte de nombreuses protections.
Par exemple, les entreprises doivent, avant de recueillir des données, obtenir au préalable un consentement écrit, clair et explicite de l'internaute avant tout traitement de données personnelles, ou qu'elles s'assurent que les enfants en dessous d'un certain âge aient bien reçu l'aval de leurs parents avant de s'inscrire sur un réseau social.
Le RGPD inclut aussi une reconnaissance d'un droit à l'oubli pour obtenir le retrait ou l'effacement de données personnelles en cas d'atteinte à la vie privée, le droit à la portabilité des données, pour pouvoir passer d'un réseau social à l'autre, d'un site de streaming à l'autre sans perdre ses informations, le droit d'être informé en cas de piratage des données.

Avantage pour la structure

Être conforme au RGPD permet de prouver son gage de confiance et de qualité à ses clients, salariés, prestataires, etc. Garantit que leurs données personnelles sont protégées et sécurisées, qu'elles seront assurées de ne pas être violées, piratées, et à l'abri d'une cyberattaque. Et si ces cas surviennent, ils nuiront à l'image de marque de la structure et causeront la perte de confiance des clients et partenaires. Outre l'amende de la CNIL qui suivra pour non-conformité au RGPD après les contrôles suite aux réclamations reçues.

Objectifs du RGPD

#04

Bénéfice n°1 I Renforcer la cybersécurité

Le RGPD peut – et doit – inciter à mettre en place des flux opérationnels, respectant les bonnes pratiques de sécurité, diminuant le danger de failles de sécurité et de pertes de données – ainsi que les coûts importants qu'elles peuvent engendrer. La loi exige que les entreprises adoptent des mesures administratives et techniques pour protéger les données personnelles des citoyens de l'UE. Cependant, il est impossible d'assurer seulement l'intégrité et la sécurité de ces données et de laisser le reste de votre environnement IT non conforme.
En réalité, le RGPD vous incite à réévaluer et améliorer toute votre stratégie de cybersécurité.
Avec un contrôle sur l'ensemble de l'infrastructure IT, des flux opérationnels protégeant les données et des procédures de surveillances rationalisées, vous pouvez diminuer de manière significative votre vulnérabilité, mieux comprendre ce qui se passe sur votre réseau et détecter et contrer les cyber-attaques plus rapidement et efficacement.

Bénéfice n°2 I Mieux gérer ses données

Afin de se conformer au RGPD, il faut connaître exactement quelles informations sont concernées dans la structure.
Il n'y a pas uniquement pour cette mise en conformité que la compréhension des données sensibles possédées par une entreprise a de la valeur. Elle peut aussi permettre d'adapter les règles de collecte des données, optimiser leur stockage et améliorer les processus de gestion des données.
En premier lieu, il faut être en mesure d'identifier les fichiers redondants, obsolètes et sans valeur métier. Ce tri dans les données réduira leurs coûts de stockage et de traitement. Et si certains de ces fichiers contiennent des données sensibles – comme les informations personnelles d'un ancien client par exemple, ce risque sera diminué (pourquoi rester responsable de données qui n'ont plus de valeur pour l'entreprise ?).
La réorganisation du stockage sera plus facile, ainsi que l'indexation des données facilitera la recherche. Cela aidera à être en conformité avec le « droit à l'oubli » du RGPD, car l'entreprise pourra trouver et effacer beaucoup plus efficacement les données personnelles d'un individu donné. Les équipes pourront trouver plus rapidement les données dont elles ont besoin, et seront donc elles aussi plus productives et efficaces dans leurs missions quotidiennes

Bénéfice n°3 I Améliorer le ROI marketing

Le RGPD exige que les entreprises, collectivités, associations, etc. recueillent le consentement d'une personne pour traiter ses données personnelles.
En appliquant une règle de consentement et en purgeant les fichiers obsolètes (comme les prospects perdus ou sans suite, les clients perdus...), une base de données surdimensionnée apparaîtra en un fichier qualifié de prospects et clients pertinents qui souhaitent réellement être en relation avec l'entreprise auprès de laquelle ils ont transmis leurs données.

Objectifs du RGPD

#04

Avec ces informations nettoyées, la structure pourra alors créer des messages répondant aux besoins et habitudes spécifiques d'une audience clairement définie, et avec un réel intérêt pour votre activité. Cette approche marketing précise augmentera de manière significative les taux de clic et de conversion, les partages sur les réseaux sociaux, ainsi que le ROI marketing grâce à un usage plus pertinent des budgets et campagnes.

Bénéfice n°4 I Plus grande fidélité et davantage de confiance

La conformité avec le RGPD est une excellente base pour développer des relations de confiance plus fortes avec les clients et le public en général.
Lorsqu'on demande l'accord pour utiliser les données d'une personne, il faut expliquer clairement et précisément l'utilisation qui sera faite de ces données.
Les consommateurs aujourd'hui mieux informés sont conscients de la façon dont leurs données personnelles sont traitées. La transparence et la responsabilité que les entreprises leur démontrent, les encouragent à avoir confiance dans leur marque.
En d'autres termes, se mettre en conformité avec le RGPD permet de montrer que l'entreprise est attentive au respect de la confidentialité de ses clients et prouve son exemplarité en la matière.

Bénéfice n°5 I Être à l'avant-garde d'une nouvelle culture d'entreprise

De nombreuses entreprises acquièrent aujourd'hui des parts de marché en étant « animal-friendly », « eco-friendly » ou « LGBT-friendly». Pourquoi ne pas faire de même avec le respect de la confidentialité des personnes, et être une entreprise « privacy-friendly ». Et se démarquer ainsi de la concurrence ?!

Le RGPD est un pas en avant prometteur vers une nouvelle culture d'entreprise, misée sur le respect et la protection des données confidentielles des clients. Cet état d'esprit pourrait bien devenir la norme, de la même façon que le tri des déchets ou le recyclage des ampoules qui sont devenues des pratiques standard.
À travers la conformité au RGPD, l'entreprise peut devenir un leader en cultivant les valeurs de la sécurité des données auprès des employés et en développant une responsabilité sociale au cœur de son organisation.

Sans vouloir nier que la mise en conformité avec le RGPD est une lourde tâche, complexe et difficile, il est néanmoins important de comprendre les bénéfices qu'elle va apporter. Améliorer la sécurité et la confidentialité des données sensibles va aider à éliminer les failles de sécurité, améliorer la productivité des employés, favoriser des campagnes marketing plus efficaces, développer des relations de confiance avec les clients et se démarquer de la concurrence. Le RGPD est une opportunité pour exceller.

Quelles sanctions ?

#05

Les organisations ont tout intérêt à respecter à la lettre le RGPD car les plafonds des sanctions sont particulièrement élevés : en cas d'infraction, des amendes jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent sont prévues pour l'organisme fautif, sachant que c'est le montant le plus élevé qui est retenu entre les deux cas de figure.

Il convient aussi de noter qu'une société doit veiller à ce que son sous-traitant reste bien en conformité avec cette loi, sous peine d'en subir les conséquences, du fait de sa qualité de responsable du traitement.
Ceci étant, les multinationales ne sont pas nécessairement les plus exposées : si ce sont elles qui risquent les amendes les plus fortes, des juristes et des experts y travaillent déjà à plein temps depuis des mois pour être absolument en conformité avec le RGPD.
Le risque est en revanche plus grand pour les entités plus petites, comme une TPE, une PME, auto-entrepreneur, profession libérale ou une association.

Exemples de sanctions

En France, la première sanction remarquable décidée sous l'égide du RGPD a été prise à l'encontre de Google, le 21 janvier 2019. Saisie par deux associations, une française et une autrichienne, la CNIL estime que l'entreprise américaine commet trois manquements (accessibilité et clarté de l'information, et absence de consentement valable pour la publicité personnalisée).
Google : amendé de 50 millions € pour « manque de transparence, information insatisfaisante et absence de consentement valable pour la personnalisation de la publicité ».

Bien que les GAFAM (dont Google, Facebook et Amazon) soient en ligne de mire de ces condamnations, tous les secteurs sont concernés :

Une société spécialisée dans la promotion immobilière a ainsi été condamnée à 400 000 € d'amende pour « défaut de sécurité des données personnelles et non-respect des durées de conversation » ;

Une société d'installation d'équipement et d'isolation l'a été à hauteur de 500 000 € pour « absence de pertinence, non-adéquation, non pertinence et caractère excessif des données, défaut d'information des personnes, non-respect du droit d'opposition, non coopération avec l'autorité de contrôle, transfert non encadré de données hors de l'UE ».

Si les petites entreprises ou celles de taille moyenne n'ont été que peu concernées pour le moment, il est toutefois à prévoir que la période de tolérance qui leur a été accordée touche à sa fin.
Il est impératif que toutes les entreprises, quelle que soit leur taille et leur statut juridique, se sentent concernées par cette réglementation et se mettent en conformité.

Ailleurs en Europe, des sanctions ont été prononcées dans 11 pays : l'Allemagne, l'Italie, la Pologne, l'Autriche, le Danemark, le Portugal, la Norvège, la Lituanie, la Bulgarie, la Hongrie et Chypre, mais les montants sont beaucoup plus modestes. Ils vont de 9 700 euros (en Autriche) à 400 000 euros (au Portugal).

Quelles sanctions ?

#05

Ailleurs dans le Monde

Si le RGPD a fait l'objet de critiques, notamment du côté des États-Unis, pays qui n'a pas la même vision que l'Europe sur la donnée personnelle, il semble toutefois que le texte ait une certaine influence sur d'autres législateurs.

Notons aussi qu'il existe des projets au niveau des États fédérés américains, comme la Californie et New York. Un texte est même passé l'été 2019 dans le Golden State, siège d'un grand nombre de géants du web. Cependant, son application n'a eu lieu qu'à partir du 1er janvier 2020.

Plus inattendue, la Chine, dont le modèle de développement paraît assez distant des standards occidentaux, serait aussi en réflexion sur le sujet.

Les étapes clés pour sa conformité au RGPD

#06

Pour se mettre en conformité avec le règlement RGPD (Règlement Général sur la Protection de Données personnelles), il est opportun de commencer par examiner les recommandations de l'autorité de tutelle, la CNIL. Elle détient, plus que jamais, le pouvoir de sanctionner et d'infliger de lourdes amendes.
Les étapes obligatoires :
La CNIL souligne que « les entreprises devront assurer une protection optimale des données à chaque instant et être en mesure de la démontrer en documentant leur conformité ».

Voici, en résumé, les 6 étapes recommandées par la haute autorité :

1 - Désigner un « pilote » pour la gouvernance des données personnelles. C'est un « véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne » : le DPO, délégué à la protection des données est le prolongement du « correspondant informatique et libertés », chargé d'organiser les actions à mener. Celui-ci ne peut être ni le chef d'entreprise, ni le responsable informatique sinon, il y aurait conflit d'intérêt, il est recommandé de contacter un DPO externe.

2 – Cartographier les traitements de données personnelles. Il s'agit de « mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez ». Il faut commencer par « recenser de façon précise les traitements de données personnelles. Il est recommandé de constituer un « registre des traitements ». Ce document sera à fournir en cas de contrôle.

3 – Prioriser les étapes à mener : sur la base du « registre de traitements », il faut identifier les actions à mener pour être conforme aux obligations actuelles et à venir. Cette priorisation s'établit « au regard des risques que font peser les traitements sur les droits et les libertés des personnes concernées ».

4 - Gérer les risques et lancer une étude d'impact : pour chacun des traitements de données personnelles «identifiés comme susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées », il faut mener une analyse d'impact sur la protection des données (PIA).

5 – Organiser les procédures internes : « Pour assurer un haut niveau de protection des données personnelles en permanence », il faut mettre en place « des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demande de rectification ou d'accès, modification des données collectées, changement de prestataire) ».

6 – Documenter la conformité : pour prouver la conformité au règlement, il faut « 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 ».

Les 4 étapes à retenir

1. **Évaluation** et **analyse** des écarts + Analyse de la situation => AUDIT DE CONFORMITÉ
2. **Feuille de route** détaillée pour pallier les écarts et répondre aux nouvelles exigences => RAPPORT DE REVUE INITIALE DE CONFORMITÉ **+** PRÉCONISATIONS POUR UNE TOTALE CONFORMITÉ
3. **Test** du plan de prise en charge des incidents, audits et évaluations des processus
4. **Feedback** destiné à améliorer et pérenniser la conformité.
   Actions à mener :
   Identification et classification des données.
   Cartographie des flux de données.
   Analyse des écarts.
   Évaluation des ressources requises pour recruter et former les collaborateurs.
   Estimation des coûts associés aux nouveaux produits et services.
   Prise en compte des services professionnels.
   Déploiement des fonctions de sécurité.
   Mise à jour des processus.
   Maîtrise des risques associés aux tiers.
   Examen des déclarations de confidentialité et des communications associées.
   Définition d'une structure organisationnelle.
   Test du plan de prise en charge des incidents.
   Contrôle des mécanismes d'audit.
   Test des nouveaux processus.
   Évaluation des documents destinés aux clients.
   Préparation à des audits ad hoc.
   Élaboration des programmes de formation et de sensibilisation.
   Mesure.

Conseils d'expert

#07

Dans un premier temps, posez-vous les bonnes questions :

Demandez-vous si vous avez une bonne visibilité sur vos données

Savez-vous si vos données sont exposées ?

Avez-vous prévu des règles de gestion sur vos données ?

Avez-vous mis en œuvre des mesures de sécurité adaptées ?

Pouvez-vous répondre aux requêtes de vos utilisateurs, clients, prospects, salariés... ?

Pouvez-vous prouver votre conformité à la CNIL ?

Êtes-vous sûr de pouvoir rester conforme dans la durée ?

Ne pas oublier que le RGPD prévoit l'obligation de déclarer une faille, entraînant une fuite ou un vol de données personnelles, auprès de l'autorité de contrôle dans les 72 heures suivant l'incident. Le DPO pourra accompagner l'établissement dans la gestion de ces incidents.

Enfin, le DPO devra traiter les demandes d'accès à ses données personnelles, formulées par exemple par un client.

Boîte à outils - RGPD

#08

Guides pratiques, sites web et modèles de documents pour se mettre en conformité avec le Règlement Général sur la Protection des Données (RGPD), sous la surveillance de la CNIL, entré en vigueur le 25 mai 2018.

Pour vous aider à établir des mentions légales de vos sites web.

Outil de gestion de collecte des consentements.

Renforcer la sécurité des données à caractère personnel – ANSSI.

Évaluer le niveau de sécurité des données personnelles de votre organisme – CNIL.

Guide pratique de sensibilisation au RGPD pour petites et moyennes structures.

Boîte à outils RGPD- Modèle de questionnaire interne

#08

Objectifs du questionnaire

La prise en compte du nouveau Règlement Européen sur la Protection des Données (RGPD) et la volonté de se mettre en conformité implique la création d'un registre des traitements de données personnelles.
Une première identification des traitements courants a déjà été réalisée par les porteurs du projet.
Le but de ce questionnaire est de sensibiliser les destinataires à ce nouveau règlement et d'arriver à identifier tous les traitements qui seraient mis éventuellement en œuvre à l'occasion de leur activité personnelle.
Deux points nous intéressent particulièrement concernant un fichier de données à caractère personnel:
La connaissance de son existence,
La durée de conservation des données.

L'identification d'un fichier de données personnelles permet de :

Le lister dans le registre des traitements,
Définir sa finalité,
Définir une durée de vie des données,
Sécuriser selon les règles de l'art par la DSI,
Avoir la capacité de répondre aux droits d'accès ou d'effacement,
Archiver avec cryptage en fin de vie si nécessaire.
La protection des données personnelles est fortement liée à la sécurité du Système d'Information. Les mesures de sécurité qui peuvent être mise en place ne résolvent pas tout, une vigilance collective autour du SI est utile et nécessaire à sa protection.

Nom - Prénom :	**Questionnaire**
Service :	
Fichier de données personnelles - travail quotidien: Données permettant d'identifier une personne de manière directe ou indirecte. Dans le doute, merci de poser la question.	Dans le cadre de votre activité, utilisez-vous des fichiers intégrant des données personnelles autres que ceux qui sont identifiés dans les bases de données ''officielles'' ? Fichiers de contacts personnels (Excel, Word, autre …) OUI – NON Fichiers d'extraction de base de données OUI – NON Fichiers de sauvegarde OUI – NON Fichiers fournis par un tiers (partenaire ou donneur d'ordre) OUI – NON **Si OUI (*):** **Type de données concernées :** **Finalité du fichier :** **Lieu de stockage :**
Fichier de données personnelles - historique ou archive	Avez-vous connaissance de la présence de fichiers conservés à titre de mémoire ou d'archivage ? Fichiers de travail personnel dupliqués OUI – NON Fichiers issus de bases de données obsolètes OUI – NON Fichiers issus d'organisations précédentes OUI – NON **Si OUI (*):** **Type de données concernées :** **Finalité du fichier :** **Lieu de stockage :**
Bonnes pratiques :	Avez-vous identifié des communications ou enregistrements de données qui auraient échappé à la vigilance de la DSI et qui, selon vous, mériterait une attention particulière vis-à-vis de la protection des données personnelles ? Formule réglementaire d'avertissement, clarté de la formule, partage de données avec des tiers, … OUI – NON **Si OUI (*):** **Type de traitement concerné :**
Participation à la conformité :	Avez-vous des remarques ou conseils à formuler concernant la prise en compte de la protection des données personnelles au sein de l'organisme :
Date et signature	

Boîte à outils RGPD -

Exemple de registre

#08

Pour faciliter la tenue du registre, la CNIL propose un modèle de registre de base destiné à répondre aux besoins les plus courants en matière de traitements de données, en particulier des petites structures.
Ce document vise à recenser les traitements de données personnelles mis en œuvre dans votre organisme en tant que responsable de traitement. Centralisé et régulièrement mis à jour, il vous permet de répondre à l'obligation de tenir un registre prévu par le RGPD.
Une fois ce recensement effectué, vous serez en mesure de procéder à l'analyse des traitements de données personnelles à la réglementation.
Composition du document
La page 2 du registre recense les informations communes à toutes vos activités de traitement.
Les coordonnées de votre organisme (ou de son représentant sur le territoire européen si votre organisme n'est pas établi dans l'Union européenne).
Les coordonnées du délégué à la protection des données (DPO) si vous en disposez.
La liste des activités de votre organisme impliquant le traitement de données personnelles.
Pour chaque activité recensée, vous devrez créer et tenir à jour une fiche de registre (page 3 à 6).
Les pages suivantes constituent le modèle de fiche de registre, que vous devrez remplir pour chacune de ces activités.


REGISTRE DES ACTIVITÉS DE TRAITEMENT DE

Activités de l'organisme impliquant le traitement de données personnelles


FICHE DE REGISTRE DE L'ACTIVITÉ

Objectif poursuivis

Catégories de personnes concernées

Catégories de données collectées

REGISTRE DES ACTIVITÉS DE TRAITEMENT D

Cliquez ici. Nom de l'organisme

Coordonnées du responsable de l'organisme *(responsable de traitement ou son représentant si le responsable est situé en dehors de l'UE)*	Nom : Cliquez ici. Prénom : Cliquez ici. Adresse : Cliquez ici. CP : Cliquez ici. Ville : Cliquez ici. Téléphone : Cliquez ici. Adresse de messagerie : Cliquez ici.
Nom et coordonnées du délégué à la protection des données *(si vous avez désigné un DPO)*	Nom : Cliquez ici. Prénom : Cliquez ici. Société (si DPO externe) : Cliquez ici. Adresse : Cliquez ici. CP : Cliquez ici. Ville : Cliquez ici. Téléphone : Cliquez ici. Adresse de messagerie : Cliquez ici.

Activités de l'organisme impliquant le traitement de données personnelles
Listez ici les activités pour lesquelles vous traitez des données personnelles.

Boîte à outils RGPD – Exemple de registre

#08

Activités	Désignation des activités
Activité 1	Cliquez ici. ex. Gestion de la paie
Activité 2	Cliquez ici. ex. Gestion des prospects
Activité 3	Cliquez ici. ex. Gestion des fournisseurs
Activité 4	Cliquez ici. ex. Vente en ligne
Activité 5	Cliquez ici. ex. Sécurisation des locaux
Activité 6	Cliquez ici.
Activité 7	Cliquez ici.
Activité 8	Cliquez ici.

Vous devrez créer et tenir à jour une fiche de registre par activité.
Le modèle de fiche de registre est disponible sur la page suivante, copier / coller autant de fois la sélection qu'il y a d'activité listée.

----> Début de section à copier pour chaque activité listée en page 2 <----

Boîte à outils RGPD – Fiche de registre de l'activité

#08

Cliquez ici. Nom de l'activité

(Créer cette fiche pour chaque activité listée en page 2)

Date de création de la fiche	Cliquez ici pour entrer une date.
Date de dernière mise à jour de la fiche	Cliquez ici pour entrer une date.
Nom du responsable conjoint du traitement *(dans le cas où la responsabilité de ce traitement de donnée est partagée avec un autre organisme)*	Cliquez ici.
Nom du logiciel ou de l'application *(si pertinent)*	Cliquez ici.

Objectifs poursuivis

Décrivez clairement l'objet du traitement de données personnelles et ses fonctionnalités.

Exemple : pour une activité « formation des personnels » : suivi des demandes de formation et des périodes de formation effectuées, organisation des sessions et évaluation des connaissances.

Catégories de personnes concernées

Listez les différents types de personnes dont vous collectez ou utilisez les données.

Exemples : salariés, usagers, clients, prospects, bénéficiaires, etc.

1. 2. 3. 4.

Catégories de données collectées

Cochez et listez les différentes données traitées

☐ État-civil, identité, données d'identification, images *(ex. nom, prénom, adresse, photographie, date et lieu de naissance, etc.)*
☐ Vie personnelle *(ex. habitudes de vie, situation familiale, etc.)*
☐ Vie professionnelle *(ex. CV, situation professionnelle, scolarité, formation, distinctions, diplômes, etc.)*
☐ Informations d'ordre économique et financier *(ex. revenus, situation financière, données bancaires, etc.)*
☐ Données de connexion *(ex. adresse IP, logs, identifiants des terminaux, identifiants de connexion, informations d'horodatage, etc.)*
☐ Données de localisation *(ex. déplacements, données GPS, GSM, ...)*

☐ Internet *(ex. cookies, traceurs, données de navigation, mesures d'audience, ...)*
☐ Autres catégories de données *(précisez)* :

Des données sensibles sont-elles traitées ?

La collecte de certaines données, particulièrement sensibles, est strictement encadrée par le RGPD et requiert une vigilance particulière. Il s'agit des données révélant l'origine prétendument raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale des personnes, des données génétiques et biométriques, des données concernant la santé, la vie sexuelle ou l'orientation sexuelle des personnes, des données relatives aux condamnations pénales ou aux infractions, ainsi que du numéro d'identification national unique (NIR ou numéro de sécurité sociale).

☐ Oui ☐ Non

Si oui, lesquelles ? :

Durées de conservation des catégories de données

Combien de temps conservez-vous ces informations ?

Cliquez ici. Jours, Cliquez ici. Mois, Cliquez ici. Ans, Autre durée : Cliquez ici.

Si vous ne pouvez pas indiquer une durée chiffrée, précisez les critères utilisés pour déterminer le délai d'effacement (par exemple, 3 ans à compter de la fin de la relation contractuelle).

Si les catégories de données ne sont pas soumises aux mêmes durées de conservation, ces différentes durées doivent apparaître dans le registre.

Catégories de destinataires des données

Destinataires internes

(Exemples : entité ou service, catégories de personnes habilitées, direction informatique, etc.)

1. 2.
3. 4.

Organismes externes

(Exemples : filiales, partenaires, etc.)

1. 2.
3. 4.

Sous-traitants

(Exemples : hébergeurs, prestataires et maintenance informatiques, etc.)

1. 2.
3. 4.

Transferts des données hors UE

Des données personnelles sont-elles transmises hors de l'Union européenne ?

☐ Oui ☐ Non

Si oui, vers quel(s) pays :

Dans des situations particulières (transfert vers un pays tiers non couvert par une décision d'adéquation de la Commission européenne, et sans les garanties mentionnées aux articles 46 et47 du RGPD), des garanties spécifiques devront être prévues et documentées dans le registre (article 49 du RGPD). Consultez le site de la CNIL.

Mesures de sécurité

Cochez et décrivez les mesures de sécurité organisationnelles et techniques prévues pour préserver la confidentialité des données.

Le niveau de sécurité doit être adapté aux risques soulevés par le traitement. Les exemples suivants constituent des garanties de base à prévoir et peuvent devoir être complétés.

☐ Contrôle d'accès des utilisateurs

Décrivez les mesures :

☐ Mesures de traçabilité

Précisez la nature des traces *(exemple : journalisation des accès des utilisateurs)*, les données enregistrées *(exemple : identifiant, date et heure de connexion, etc.)* et leur durée de conservation :

☐ Mesures de protection des logiciels (antivirus, mises à jour et correctifs de sécurité, tests, etc.)

Décrivez les mesures :

☐ Sauvegarde des données

Décrivez les modalités :

☐ Chiffrement des données

Décrivez les mesures (*exemple : site accessible en https, utilisation de TLS, etc.)* :

☐ Contrôle des sous-traitants

Décrivez les modalités :

☐ Autres mesures :

----> Fin de section à copier pour chaque activité listée en page 2 <---

Merci d'avoir lu ce livre blanc offert par

DPO Agency
By PEB

Des questions sur le RGPD ? Contactez-nous !

30 min de conseils gratuits !
Prenez rdv directement sur notre agenda digital

Rejoignez notre communauté RGPD pour vous aider !

Suivez-nous sur nos réseaux sociaux