UNIVERSITÉ de Picardie Jules Verne

Guide pratique de sensibilisation au RGPD

Mise en œuvre de dispositifs de protection des données

UPJV

Le guide pratique de sensibilisation au RGPD a pour objectif de sensibiliser les personnels à la mise en œuvre de leurs propres dispositifs de protection des données, dont ils sont seuls et entièrement responsables.

AVANT-PROPOS

Les données sont omniprésentes et au cœur de la Recherche. Bien gérées et sécurisées, elles permettent de gagner en efficacité, de personnaliser et de conforter la relation avec les participants à la recherche. Pour s'adapter aux enjeux du numérique et garantir une meilleure maîtrise des données personnelles, une nouvelle réglementation européenne, le Règlement Général sur la Protection des Données (RGPD), est entré en application le 25 mai 2018. Il renforce les droits des personnes et responsabilise davantage les organismes publics et privés qui traitent leurs données.

Un des changements majeurs consiste en la suppression de la plupart des obligations déclaratives auprès de la CNIL (déclarations, autorisations) au profit d'une logique d'auto-responsabilité. Les responsables de traitements devront donc veiller eux-même au respect de la réglementation tout au long du cycle de vie de la donnée (collecte, traitement, archivage, suppression).

Ce guide vous propose des clés de compréhension pratiques pour engager au sein de vos travaux une démarche de conformité au RGPD, et les faire progresser dans leur maturité numérique.

Ce guide ne répondra pour autant pas nécessairement aux besoins spécifiques de chaque recherche, seul un aperçu des principales réflexions à mener et actions à mettre en œuvre est abordé. Le site de la CNIL dispose de nombreux contenus pour ceux qui souhaiteront accéder à une documentation plus technique et plus complète.

Le contexte juridique s'adapte pour suivre les évolutions des technologies et de nos sociétés (usages accrus du numérique…). Ce nouveau règlement européen s'inscrit dans la continuité de la Loi française « Informatique et Libertés » de 1978 et renforce le contrôle par les citoyens de l'utilisation qui peut être faite des données les concernant. Il harmonise les règles en Europe en offrant un cadre juridique unique. Les mêmes obligations sont imposées aux entreprises établies hors de l'Union européenne, dès lors qu'elles utilisent les données personnelles de résidents européens. En tant que chercheur, ces nouvelles obligations vous inciteront notamment à plus de transparence dans vos relations avec vos interlocuteurs. Faire comprendre la manière dont vous utilisez leurs données personnelles et leur donner la possibilité de les maîtriser, renforcera la confiance et favorisera donc votre activité.

QUI EST CONCERNÉ PAR LE RGPD ?

Tout organisme quels que soient sa taille, son pays d'implantation et son activité, peut être concerné. En effet, le RGPD s'applique à toute organisation, publique et privée, qui traite des données personnelles pour son compte ou non, dès lors :

• qu'elle est établie sur le territoire de l'Union européenne ;

• que son activité cible directement des résidents européens.

Par exemple, un organisme établi en France, qui réalise une étude en dehors de l'Union européenne doit respecter le RGPD. De même, un organisme en dehors de l'Union européenne, réalisant une étude en France doit respecter le RGPD.

Le RGPD concerne aussi les sous-traitants qui traitent des données personnelles pour le compte d'autres organismes ou de personnes.

Ainsi, si vous traitez ou collectez des données pour le compte d'une autre entité (entreprise, collectivité, association), vous avez des obligations spécifiques pour garantir la protection des données qui vous sont confiées.

QU'EST-CE QU'UNE DONNÉE PERSONNELLE ?

Une « donnée personnelle » est « toute information se rapportant à une personne physique identifiée ou identifiable » (Cf Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, article 2).

Une personne peut être identifiée :

• directement (exemple : nom, prénom) ;

• indirectement (exemple : par un identifiant (n° client), un numéro (de téléphone), une donnée biométrique, plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :

• à partir d'une seule donnée (exemple : numéro de sécurité sociale, ADN)

• à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour, abonnée à tel magazine et militant dans telle association).

QU'EST-CE QU'UN TRAITEMENT DE DONNÉES PERSONNELLES ?

Un « traitement de données personnelles » est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement).

Par contre, un fichier ne contenant que des coordonnées d'entreprises (par exemple, entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un email de contact générique « compagnieA@email.fr ») n'est pas un traitement de données personnelles.

Un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

Un traitement de données doit avoir un objectif, une finalité, c'est-à-dire que vous ne pouvez pas collecter ou traiter des données personnelles simplement au cas où cela vous serait utile un jour. À chaque traitement de données doit être assigné un but, qui doit bien évidemment être légal et légitime au regard de votre activité professionnelle.

Le RGPD renforce l'obligation d'information et de transparence à l'égard des personnes dont vous traitez les données (clients, collaborateurs, etc.).

QUI EST RESPONSABLE DE TRAITEMENT ?

Le responsable de traitement est la personne physique ou morale qui seule ou conjointement, détermine les finalités et les moyens du traitement.

QU'EST-CE QU'UN SOUS-TRAITANT ?

Le RGPD reconnaît le rôle des sous-traitants dans le traitement de données personnelles, et leur impose des obligations particulières.

Le sous-traitant est la personne physique ou morale qui traite des données personnelles pour le compte d'un autre organisme ou d'une autre personne (le « responsable de traitement »), dans le cadre d'un service ou d'une prestation.

Vous êtes concerné, en qualité de responsable de traitement, si vous choisissez de confier la gestion de vos données personnelles à des prestataires qui seront vos sous-traitants.

Vous êtes concerné, en qualité de sous-traitant, si votre entreprise traite des données personnelles sur instruction et pour le compte d'un autre organisme dans le cadre d'un service ou d'une prestation.

TRANSFÉRER DES DONNÉES HORS DE L'UE

Avec la globalisation des échanges et l'utilisation croissante des nouvelles technologies, le nombre de transferts de données hors de France ne cesse de croître. Or, le transfert de données hors de l'Union européenne (UE) et de l'Espace Economique Européen (EEE) est possible, à condition d'assurer un niveau de protection des données suffisant et approprié. Ces transferts doivent être encadrés en utilisant différents outils juridiques. Par ailleurs, tout transfert doit faire l'objet du consentement explicite de la personne concernée.

QUELS OUTILS POUR ENCADRER LES TRANSFERTS DE DONNÉES HORS EEE ?

Les transferts hors UE peuvent être fondés sur :

- une décision d'adéquation de la Commission européenne concernant certains pays assurant un niveau de protection adéquat ;

- des clauses contractuelles types (CCT) de la Commission européenne ;

- des règles internes d'entreprises (BCR) ;

- des clauses contractuelles spécifiques (considérées comme conformes aux modèles de clauses de la Commission européenne) ;

Avec le RGPD, les transferts peuvent également être encadrés par :

- des clauses contractuelles types adoptées par une autorité de contrôle et approuvées par la Commission européenne ;

- un code de conduite approuvé (comportant l'engagement contraignant et exécutoire pris par les destinataires hors UE d'appliquer les garanties appropriées) ;

- un mécanisme de certification approuvé (comportant l'engagement contraignant et exécutoire pris par les destinataires hors UE d'appliquer les garanties appropriées) ;

- un arrangement administratif ou un texte juridiquement contraignant et exécutoire pris pour permettre la coopération entre autorités publiques (Mémorandum of Understanding dit MOU ou MMOU, convention internationale…).

QU'EST-CE QUE LE BOUCLIER DE PROTECTION DES DONNÉES UE – ÉTATS - UNIS ?

Le Bouclier de Protection des Données, mieux connu sous le nom de « Privacy Shield », est un mécanisme d'auto-certification pour les entreprises établies aux États-Unis qui a été reconnu par la Commission européenne comme offrant un niveau de protection adéquat aux données à caractère personnel transférées par une entité européenne vers des entreprises établies aux États-Unis. Ce mécanisme est par conséquent considéré comme offrant des garanties juridiques pour de tels transferts de données.

QUELLES SONT LES ENTREPRISES AMÉRICAINES QUI PEUVENT BÉNÉFICIER DU BOUCLIER DE PROTECTION DES DONNÉES UE – ÉTATS-UNIS ?

Afin de pouvoir s'auto-certifier au Bouclier de Protection des Données, une entreprise établie aux États-Unis doit être soumise aux pouvoirs de contrôle et d'exécution de la Commission Fédérale du Commerce (« FTC ») ou du Département des Transports américain (« DoT »). D'autres autorités habilitées par la loi pourraient également rejoindre le dispositif à l'avenir.

Cela signifie par exemple, que les organismes à but non lucratif, les banques, les sociétés d'assurances et les fournisseurs de services de télécommunication (s'agissant des services fournis au public) ne relèvent pas de la compétence de la FTC ou du DoT et ne peuvent donc pas adhérer au Bouclier de Protection des Données.

Le Bouclier de Protection des Données s'applique à tout type de données à caractère personnel transférées par une entité depuis l'UE aux États-Unis, notamment des données commerciales, de santé ou de ressources humaines à condition que la société destinataire au États-Unis ait adhéré au dispositif.

QUELLES ACTIONS CONVIENT-IL D'ENTREPRENDRE AVANT DE TRANSFÉRER DES DONNÉES À CARACTÈRE PERSONNEL VERS UNE SOCIÉTÉ ÉTABLIE AUX ÉTATS-UNIS QUI A ADHÈRE OU DÉCLARE AVOIR ADHÉRÉ AU BOUCLIER DE PROTECTION DES DONNÉES ?

Avant de transférer des données à caractère personnel auprès d'une entreprise établie aux États-Unis qui déclare être certifiée au Bouclier de Protection des Données, les entreprises européennes doivent s'assurer que la société américaine dispose d'une certification active (les certifications doivent être renouvelées tous les ans) et que la certification couvre les données en question (plus particulièrement : les données RH, les données non-RH respectivement).

Afin de vérifier si une certification est active et applicable, les sociétés européennes doivent consulter la Liste du Bouclier de Protection de Données qui est publiée sur le site du Département du Commerce américain

LE DELÉGUÉ À LA PROTECTION DES DONNÉES (DPD)

Avec une fonction située au cœur de la conformité au règlement européen sur la protection des données (RGPD), le délégué à la protection des données (DPD) conseille et accompagne les organismes qui le désignent dans leur conformité.

En tant que conseiller de la conformité en matière de protection des données au sein de l'Université, le DPD est principalement chargé :

- d'informer et de conseiller l'organisme ;
- de contrôler le respect du règlement et du droit national en matière de protection des données ;
- de conseiller l'organisme sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;
- être contacté par les personnes concernées pour toute question ;
- de coopérer avec la CNIL et d'être son point de contact.

RESPECTEZ LES DROITS DES PERSONNES

Informez les personnes

À chaque fois que vous collectez des données personnelles, le support utilisé (formulaire, questionnaire, etc.) doit comporter des mentions d'information.

Vérifiez que l'information comporte notamment les éléments suivants :

- Les coordonnées du responsable de traitement (vous) ;
- L'adresse contact.cnil@u-picardie.fr ;
- Pourquoi vous collectez les données (« la ou les finalités ») ;

- Ce qui vous autorise à traiter ces données (le « fondement juridique » : il peut s'agir du consentement de la personne concernée, de l'exécution d'un contrat, du respect d'une obligation légale qui s'impose à vous…) ;

- Qui a accès aux données (indiquez les destinataires des données ou des catégories de destinataires: les services internes compétents, un prestataire, etc.) ;

- Combien de temps vous les conservez (exemple : « 2 ans après la fin de la recherche ou de la publication ») ;

- Les modalités selon lesquelles les personnes concernées peuvent exercer leurs droits, retrait du consentement, droit d'accès, de suppression…(par un message sur une adresse email dédiée, par un courrier postal à un service identifié) ;

- Si vous transférez des données hors de l'Union européenne (précisez le pays et l'encadrement juridique qui maintient le niveau de protection des données).

- Le droit d'exercer directement une réclamation auprès de la CNIL si la personne n'a pu exercer ses droits auprès de l'UPJV.

Si le risque zéro n'existe pas en informatique, vous devez prendre les mesures nécessaires pour garantir au mieux la sécurité des données.

Vous êtes en effet tenu d'assurer la sécurité des données personnelles que vous détenez.

SÉCURISEZ VOS DONNÉES

Garantissez l'intégrité de votre patrimoine de données en minimisant les risques de pertes de données ou de piratage. Les mesures à prendre, informatiques ou physiques, dépendent de la sensibilité des données que vous traitez et des risques qui pèsent sur les personnes en cas d'incident.

Différentes actions doivent être mises en place : mises à jour de vos antivirus et logiciels, changement régulier des mots de passe et utilisation de mots de passe complexes, ou chiffrement de vos données dans certaines situations. Il faut éviter les supports de stockages non sécurisés. En cas de perte ou vol d'un outil informatique, il sera plus difficile pour un tiers d'y accéder. Les failles de sécurité ont également des conséquences pour ceux qui vous ont confié des données personnelles. Ayez à l'esprit les conséquences pour les personnes de la perte, la divulgation, la modification non souhaitée de leurs données, et prenez les mesures nécessaires pour minimiser ces risques.

Pour évaluer le niveau de sécurité des données personnelles, voici quelques questions à se poser :

• les comptes utilisateurs internes et externes sont-ils protégés par des mots de passe d'une complexité suffisante ?

• les accès aux locaux sont-ils sécurisés ?

• des profils distincts sont-ils créés selon les besoins des utilisateurs pour accéder aux données ?

• avez-vous mis en place une procédure de sauvegarde et de récupération des données en cas d'incident ?

TRAITEMENTS DE DONNÉES À RISQUE, ÊTES-VOUS CONCERNÉ ?

L'article 9 du RGPD en donne la définition et pose l'interdiction de traiter les données dites « **sensibles** ».

Sont notamment concernées les données :

• révélant l'origine prétendument raciale ou ethnique ;

• portant sur les opinions politiques, philosophiques ou religieuses ;

• relatives à l'appartenance syndicale ;

• concernant la santé ou l'orientation sexuelle ;

• génétiques ou biométriques.

L'article 9.2 prévoit cependant quelques exceptions à cette interdiction :

- La personne concernée a donné son consentement ;

- Le traitement est réalisé en matière de droit du travail (RH), de sécurité sociale... ;

- Le traitement porte sur des données qui sont manifestement rendues publiques par la personne concernée ;

- Le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail ;

- Le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique ;

- Le traitement est nécessaire à des fins archivistiques dans l'intérêt public, des fins de recherche scientifiques ou historiques ou à des fins statistiques.

LES PRINCIPES CLÉS DE TOUT TRAITEMENT

Licéité :

Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie:

- la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;

- le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;

- le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;

- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;

- le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Loyauté et transparence :

Les données doivent être traitées de manière licite, loyale et transparente au regard de la personne concernée (mentions d'informations détaillées, claires et précises).

Le principe de finalité du traitement :

Les données personnelles ne peuvent être recueillies et traitées que pour un objectif déterminé explicite et légitime.

Cette finalité doit être déterminée avant la collecte de données. Il est interdit de collecter des données « au cas où ».

Lesdites données ne pourront pas être réutilisées ultérieurement pour une autre recherche sans obtenir le consentement écrit des personnes concernées. De plus, ces données ne peuvent être réutilisées que sous certaines conditions :

- Les données doivent être anonymes ou anonymisées ;

- Faire mention d'une réutilisation des données dans le formulaire de consentement.

Le principe de proportionnalité et de minimisation :

Seules les informations adéquates, pertinentes et nécessaires à la finalité de la recherche peuvent faire l'objet d'un traitement. Inutile de collecter des informations qui ne sont pas indispensables à la réalisation de l'étude. Si possible, se passer de données personnelles.

Le principe d'une durée de conservation limitée des données :

Une durée de conservation doit être établie en fonction de la finalité de chaque traitement. Il peut y avoir différentes durées pour différentes données pour un même traitement. Une fois le traitement réalisé et les résultats obtenus, inutile de conserver les données personnelles (anonymisez vos données). Seuls les éléments probatoires nécessaires ou les données anonymes peuvent être conservées plus longuement (sauf obligation légales de conservation ou d'archivage).

Les principes de sécurité et de confidentialité :

Les données collectées ne peuvent être consultées que par les personnes habilitées à y accéder en raison de leurs missions dans le cadre du traitement.

Il est nécessaire de prendre toutes les mesures de protection nécessaires, physiques et logicielles, pour en garantir la confidentialité et éviter toute divulgation d'information volontaire ou involontaire.

Plus les données sont sensibles plus la sécurité et la confidentialité doivent être importantes.

LES QUESTIONS À SE POSER SUR LA BASE DE CES PRINCIPES

Apportez les ajustements nécessaires aux traitements de données envisagées dans le cadre de vos travaux de recherche, en vous posant les bonnes questions :

- La finalité (l'objectif) de la recherche est-elle clairement définie ?

- Les données que vous envisagez de collecter sont-elles toutes strictement nécessaires par rapport au sujet de votre recherche ?

- Avez-vous prévu, lorsque votre recherche sera terminée, une durée à l'issue de laquelle les données seront archivées anonymement ou supprimées ?

- Les personnes concernées seront-elles informées avant le début de la recherche.

- Comment la personne concernée pourra-t-elle exercer ses droits (droit d'accès, d'opposition, de suppression…) ?

- Les mesures mises en place seront-elles suffisantes pour préserver la sécurité des données ?

LES QUESTIONS AUXQUELLES VOUS DEVEZ RÉPONDRE PRÉCISÉMENT DANS LA NOTICE D'INFORMATION À DESTINATION DES PERSONNES CONCERNÉES

- Pourquoi cette recherche ? Dans quel cadre ?

- Quel est l'objectif de cette recherche ? (indiquez l'objectif réel !)

- Comment va se dérouler cette recherche (description du protocole, tests, entretiens, durée…) ?

- Qui peut participer ou non ?

- Concernant les données (pourquoi ce type de données, quel traitement sera réalisé, anonyme ou non…)

- Quels sont les droits des personnes (accès, rectification, suppression, retrait du consentement…) ?