Conformité RGPD : comment informer les personnes et assurer la transparence ?

14 mai 2018

Le règlement général sur la protection des données (RGPD), qui entre en application le 25 mai 2018, impose une information **concise, transparente, compréhensible et aisément accessible** des personnes concernées. Cette obligation de transparence est définie aux articles 12, 13 et 14 du RGPD.

L'obligation d'information existe déjà dans la loi Informatique et Libertés. Elle est renforcée par le RGPD : l'information doit être plus complète et plus précise. Elle est par ailleurs assouplie sur les modalités de fourniture et de présentation de cette information.

La transparence permet aux personnes concernées :

- de connaître la raison de la collecte des différentes données les concernant ;
- de comprendre le traitement qui sera fait de leurs données ;
- d'assurer la maîtrise de leurs données, en facilitant l'exercice de leurs droits.

Pour les responsables de traitement, elle contribue à un traitement loyal des données et permet d'instaurer une relation de confiance avec les personnes concernées.

Dans quels cas dois-je informer ?

Vous devez informer les personnes concernées :

- **en cas de collecte directe des données :** lorsque les données sont recueillies directement auprès des personnes (exemples : formulaire, achat en ligne, souscription d'un contrat, ouverture d'un compte bancaire) ou lorsqu'elles sont recueillies via des dispositifs ou des technologies d'observation de l'activité des personnes (exemples : vidéosurveillance, analyse de la navigation sur Internet, géolocalisation et *wifi analytics/tracking* pour la mesure d'audience, etc.) ;
- **en cas de collecte indirecte des données personnelles :** lorsque les données ne sont pas recueuillies directement auprès des personnes (exemples : données récupérées auprès de partenaires commerciaux, de *data brokers*, de sources accessibles au public ou d'autres personnes).

A quels moments dois-je informer ?

1. **Dans le cadre de la collecte :**

- en cas de collecte directe : au moment du recueil des données ;
- en cas de collecte indirecte : dès que possible (notamment lors du 1er contact avec la personne concernée) et, au plus tard, dans le délai d'1 mois (sauf exceptions).

2. **En cas de modification substantielle ou d'événement particulier :**

- exemples : nouvelle finalité, nouveaux destinataires, changement dans les modalités d'exercice des droits, violation de données.

Enfin, une information régulière participe de l'objectif de transparence, en particulier pour les traitements à grande échelle ou de données sensibles. Elle peut être fournie notamment lorsque le responsable de traitement communique avec les personnes

concernées.

Quelles informations dois-je donner ?

1. **Ce qui ne change pas avec le RGPD**

- **Identité et coordonnées** de l'organisme (responsable du traitement de données) ;
- **Finalités** (à quoi vont servir les données collectées) ;
- **Caractère obligatoire ou facultatif du recueil des données** (ce qui suppose une réflexion en amont sur l'utilité de collecter ces données au vu de l'objectif poursuivi – principe de « minimisation » des données) et conséquences pour la personne en cas de non-fourniture des données ;
- **Destinataires ou catégories de destinataires des données** (qui a besoin d'y accéder ou de les recevoir au vu des finalités définies) ;
- **Durée de conservation des données** (ou critères permettant de la déterminer) ;
- **Droits des personnes concernées** (opposition, accès, rectification, effacement ; nouveaux droits RGPD : limitation, portabilité) ;

Selon le cas :

- existence d'un transfert des données vers un pays hors Union européenne (ou vers une organisation internationale) et garanties associées.

2. **Ce qui est nouveau avec le RGPD**

- **Coordonnées du délégué à la protection des données** de l'organisme, s'il a été désigné, ou d'un point de contact sur les questions de protection des données personnelles ;
- **Base juridique** du traitement de données (c'est-à-dire ce qui autorise légalement le traitement : il peut s'agir du consentement des personnes concernées, du respect d'une obligation prévue par un texte, de l'exécution d'un contrat, etc.) ;
- **Droit d'introduire une réclamation** (plainte) auprès de la CNIL ;

Selon le cas :

- l'existence d'une prise de décision automatisée ou d'un profilage, les informations utiles à la compréhension de l'algorithme et de sa logique, ainsi que les conséquences pour la personne concernée.
- le fait que les données sont requises par la réglementation, par un contrat ou en vue de la conclusion d'un contrat ;
- les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers (exemple : prévention de la fraude) ;
- le droit au retrait du consentement à tout moment ;
- la faculté d'accéder aux documents autorisant le transfert de données hors de l'Union européenne (exemples : clauses contractuelles types de la Commission européenne) ;

Informations supplémentaires à donner en cas de collecte indirecte :

- Catégories de données recueillies ;
- Source des données (en indiquant notamment si elles sont issues de sources accessibles au public).

Sous quelle forme ?

Ce que dit le RGPD

La personne concernée par un traitement de données doit recevoir une information délivrée :

de façon concise, transparente, compréhensible et aisément accessible, en

des termes clairs et simples

Vous devez donc :

1. **Veiller à ce que l'information soit compréhensible**

L'information doit être rédigée de la manière la plus claire, précise et simple possible.

- **Utiliser un vocabulaire simple**, faire des phrases courtes et employer un style direct ; éviter les termes juridiques ou techniques, les termes abstraits ou ambigüs et les formules telles que « nous *pourrions* utiliser vos données », « une *possible* utilisation de vos données », « *quelques* données vous concernant sont utilisées », etc.
- **Adapter l'information au public visé** et prêter une attention particulière à l'égard des enfants et des personnes vulnérables. Des vidéos, animations ou dessins animés ou bandes dessinées peuvent être un moyen adapté pour rendre l'information compréhensible.

2. **Concevoir un format lisible d'information**

- **Etre concis.** Il ne faut pas présenter l'information dans une notice d'information composée d'un bloc de 20 pages ou faire des mentions d'information illisibles sous un formulaire de collecte (par exemple un formulaire d'inscription sur un site internet ou un bon de commande).
- **Prioriser les éléments d'information. Sauf cas particuliers, la mise à disposition de l'ensemble des informations en un seul bloc permet difficilement d'atteindre l'objectif de lisibilité et il convient donc de favoriser une approche en plusieurs niveaux.** Prioriser ne signifie pas transmettre une information incomplète aux personnes concernées : il s'agit de mettre en avant les informations essentielles et d'offrir un accès simple et immédiat aux autres informations.
- **Adapter la fourniture d'informations aux situations et aux supports. Une approche combinant différentes modalités d'information peut être suivie, qui tienne compte des spécificités de chaque traitement et permette de fournir les bonnes informations au bon moment.**

Quelles informations prioriser ?

Dans tous les cas :

- l'identité du responsable de traitement,
- les finalités,
- les droits des personnes.

Il peut être nécessaire d'ajouter une information essentielle pour les personnes concernées (exemples : prise de décision automatisée ou mise à disposition de données à des partenaires commerciaux).

Une information en plusieurs niveaux et via différents canaux

Dans un environnement numérique par exemple, **vous pouvez fournir l'information à différentes étapes du parcours utilisateur**. Les informations à prioriser sont données à la personne concernée au moment de la création de son compte, directement sur la page d'inscription. Sur cette même page, un lien renvoie vers une notice d'information complète. Celle-ci doit être également lisible et peut dès lors se présenter sous la forme de menus dépliants.

Exemple d'information de premier niveau sur le téléservice de désignation d'un

délégué à la protection des données (DPO).
Un lien renvoie vers une page permettant d'accéder à l'information détaillée.

La page d'information est constituée de menus dépliant permettant un accès rapide au plan et au détail de l'information en un clic.

La bonne information au bon moment

---

3. **Veiller à l'accessibilité de l'information**

Les personnes ne doivent pas avoir à chercher l'information

- Elles doivent immédiatement voir comment et où y accéder.
- Cette obligation s'applique quel que soit l'environnement (numérique ou autre).
- Les méthodes choisies peuvent varier en fonction du contexte et des modalités d'interaction avec les personnes. **Différents outils et techniques** peuvent ainsi être utilisés pour rendre l'information aisément accessible **selon les environnements ou les technologies** (QR code, message audio, vidéo, panneaux d'affichage, documentation papier, campagne d'information etc.).

Exemples

---

4. **Donner une vision globale sur les traitements de données**

Si vous utilisez différentes modalités d'information ou si vous fournissez de l'information relative à différents traitements, **pensez en complément à centraliser ces informations dans un document unique ou un espace dédié de votre site internet**, pour que les personnes puissent prendre facilement connaissance de l'ensemble de l'information. Si vous optez pour un document unique, assurez-vous qu'il est lisible et compréhensible.

Ces éléments d'information devraient également être distingués clairement des autres clauses ou informations que vous fournissez et qui ne sont pas liées à la protection des données personnelles.

Par exemple, sur un site internet, utilisez un **lien renvoyant directement vers la politique de protection des données**, clairement visible sur chaque page du site, intitulé de manière claire (« Données personnelles » ou « Confidentialité » par exemple).

Pour aller plus loin : le tableau de bord « gérer mes données »

Des outils permettent également aux personnes de **mieux maîtriser l'utilisation de leurs données,** en

leur permettant de gérer leurs préférences et d'exercer leurs droits (« *dashboards* »).

En résumé

Une approche combinant **différentes modalités d'information**, **par étapes complémentaires**, permet d'atteindre l'objectif de transparence.

Il n'y a pas une seule façon de bien informer les personnes. Cette information doit être :

- **adaptée aux situations et aux supports de collecte,**
- **accessible et compréhensible**.

Le RGPD pousse ainsi à la **mise en place de solutions innovantes**.

Conseils de mise en conformité RGPD :

- Mettez à niveau les mentions d'information d'abord sur vos traitements les plus sensibles et sur vos traitements les plus utilisés.
- Si vous avez un site internet, mettez à jour votre politique de protection des données ou créez-en une.
- Appuyez-vous, en les adaptant, sur les exemples de mentions d'information proposés par la CNIL.

Document reference

Lignes directrices du G29

Lignes directrices sur la Transparence (FR)
[PDF-508.54 Ko]
Guidelines on transparency (EN)
[PDF-1.12 Mo]