#NOTES D'EXPERTS

Règlement Européen de Protection des Données et Relations institutionnelles

RGPD

23/05/2018

Règlement européen 2016/679 du 27 avril 2016, relatif à la protection des données physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Les règles relatives à la protection des données personnelles se renforcent. Le règlement européen RGPD instaure de nouvelles obligations à la charge des entreprises et de nouveaux droits pour chaque citoyen. Il entre en vigueur le 25 mai 2018. Ce texte offre aux citoyens européens une plus grande maitrise du traitement de leurs données personnelles et exige plus de transparence de la part des sociétés sur leur collecte et utilisation de ces données.

Le RGDP s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux **traitements non automatisés de données à caractère personnel** contenues ou appelées à figurer dans des fichiers

Côté consommateur, le RGPD vise à mieux protéger les droits des personnes vis-à-vis de leurs données : droit à l'oubli, portabilité des données.

La responsabilité et le rôle des entreprises
Toutes les entreprises sont désormais redevables d'une obligation de mise en conformité, sous peine de sanctions pouvant aller jusqu'à 4% du Chiffre d'affaire annuel.
Les entreprises doivent désormais justifier de l'existence et de la fiabilité de leurs procédures relatives à la collecte, l'usage, la protection, le stockage, l'anonymisation ou encore la suppression des données à caractère personnel. Elles doivent pouvoir à tout moment démontrer le respect des obligations du règlement.

La CNIL est l'organisme diffuseur en France. Ses agents assermentés effectueront les contrôles de la documentation et des ordinateurs.

- Le RGPD permet d'alléger les formalités des entreprises auprès de la CNIL. Pour prouver sa conformité au règlement, il n'est désormais plus utile de réaliser une déclaration spécifique (hormis quelques domaines particuliers)

- Chaque entreprise et chaque service doit désormais constituer et regrouper la documentation nécessaire.

- Le renforcement de la responsabilité des entreprises s'inscrit dans le temps. Les entreprises doivent désormais assurer une protection optimale des données permanente et dynamique.

- La désignation d'un pilote appelé DPO (Data Protection Officer) est conseillée.

L'Assemblée nationale a adopté définitivement le 14 mai dernier à une large majorité le projet de loi renforçant la protection des données personnelles, texte d'application du droit européen. L'ensemble des groupes, à l'exception des communistes et des insoumis qui se sont abstenus, ont approuvé cette révision de la loi fondatrice Informatique et libertés de 1978.

Celle-ci était rendue nécessaire par l'entrée en vigueur le 25 mai du *« paquet européen de protection des données »,* qui comprend notamment le Règlement général sur la protection des données personnelles (RGPD).

Ce texte donne la possibilité aux ONG d'organiser des actions de groupe fédérant des milliers d'internautes pour attaquer les entreprises fautives. Certaines comptent d'ailleurs déposer une action de groupe contre les Gafam (Google, Apple, Facebook, Amazon et Microsoft) dès le 25 mai, date d'entrée en vigueur du nouveau RGPD, en estimant qu'ils conditionnent l'accès à leurs services à ce consentement à l'exploitation des données.

Navigateurs et moteurs de recherche par défaut

La rapporteure Paula Forteza (LREM), ancienne d'Etalab - service de Matignon chargé de coordonner l'ouverture des données publiques - qui a dénoncé une *« stratégie de chantage »* de ces Gafam, s'est félicitée *« de ces initiatives de la société civile qui font vivre les droits, contrôles et voies de recours mis en place par le texte ».*

Assemblée et Sénat n'avaient pu se mettre d'accord sur une version commune, ayant des divergences notamment sur l'exonération de sanction pour les collectivités territoriales.

Lors de cette dernière lecture, les députés ont adopté un amendement pour s'assurer que Google et Apple ne puissent imposer leurs navigateurs et moteurs de recherche par défaut sur les smartphones, tablettes et PC. Cette mesure, défendue depuis de longs mois par Eric Bothorel (LREM) et soutenue à l'unanimité, vise à empêcher que *« des contrats passés par des entreprises puissent à la fois imposer une application préinstallée et interdire qu'un choix alternatif protégeant mieux les données personnelles des utilisateurs soit proposé lors de la configuration initiale de leur terminal ».* Le secrétaire d'État au numérique Mounir Mahjoubi a adopté un *« regard très ouvert »* sur cet amendement, *« qui n'est pas l'avènement de la lutte finale contre les plateformes »* mais *« un premier pas vers la régulation collective. »*

Cette note aborde la question spécifique des données détenues dans le cadre de missions de relations institutionnelles. Il sera intéressant d'analyser les conditions des données détenues en interne pour anticiper les éventuels contrôles HATVP.

LES DONNEES PERSONNELLES

Définitions
(Loi n° 78-17 du 6 janvier 1978 – version à jour RGDP) :

- ✓ Constitue **une donnée à caractère personnel** toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. Les coordonnées professionnelles sont des datas personnelles ; le mot personnel signifie que cela s'attache à une personne et non que ce soit privé.

- ✓ Constitue **un traitement de données à caractère personnel** toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

- ✓ Constitue **un fichier de données à caractère personnel**, tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.

Obligation de consentement
(Loi n° 78-17 du 6 janvier 1978 – version à jour RGDP) :

- Le traitement de données à caractère personnel doit avoir reçu le consentement de la personne concernée
- Le consentement est **"préalable" à la collecte des données**.et doit comprendre le droit d'accès et de rectification
- Loi muette quant à la manière de prouver l'acquisition du consentement, **recours à l'écrit est conseillé mais interdiction d'une case pré-cochée.**

Obligations imposées par le traitement
(Loi n° 78-17 du 6 janvier 1978 – version à jour RGDP) :

- Cartographier les traitements des données personnelles est l'étape la plus importante. Elle permet de se rendre compte des actions à mener. La tenue d'un registre des traitements est la première étape permettant de prouver la conformité au règlement.
  - Les données sont collectées et traitées de manière loyale et licite ;
  - Pour des finalités déterminées, explicites et légitimes ;
  - Elles sont exactes, complètes et, si nécessaire, mises à jour ;

- Les données recueillies doivent être recentrées au **maximum sur l'essentiel**. Il faut donc éviter de collecter et conserver des données que l'entreprise n'utilise pas.
  - Les données sont adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et de leurs traitements ultérieurs ;

- Le règlement impose de fixer une durée de conservation des données collectées.
  - Les données sont conservées sous une forme permettant l'identification des personnes concernées pendant une durée qui n'excède pas la durée nécessaire aux finalités pour lesquelles elles sont collectées et traitée.
  - Cela impose qu'une date de collecte ou de création de fiche

- Il importe également que les données soient bien sécurisées, que seules les personnes ayant besoin d'y accéder y accède.

- La co-responsabilité avec les sous-traitants induit désormais de revoir tous ses contrats et notamment du fait que les données sont bien sécurisées mais également qu'elles ne soient pas gérées hors d'Europe.

LA SPECIFICITE DES RELATIONS INSTITUTIONNELLES

Toutes les directions et métiers sont concernés dès lors qu'ils manipulent des données personnelles (fichiers clients, fichiers salariés, prospects, fournisseurs, cartographies de cibles spécifiques...)

La collecte d'informations pour établir un fichier de contacts et d'institutionnels notamment est un traitement de données à caractère personnel.

Les règles s'appliquent lorsque les données sont collectées, utilisées et conservées.

Il peut s'agir de la gestion de clients, de prospects et de salariés.

Et dans le cas spécifique des Relations institutionnelles

- La gestion de fichier d'élus, de la société civile, de représentants de l'administration, d'experts...

- L'organisation d'événements, d'étude, de démarches de sensibilisation et dialogue et donc d'invitations, de confirmation, de gestion des participants …

On peut dire que l'utilisation des données personnelles pour inviter des personnes, pour informer… est possible dès lors que l'on utilise des données qui sont publiques telles que les coordonnées professionnelles mais que l'on prévoit toujours pour l'intéressé l'accès à ses données, les corrections éventuelles, leur restriction d'usage ou leur destruction

Cela impose et notamment dans le cas de fichiers ou de cartographies ou de bases de données internes de ne pas acquérir, constituer, conserver, commercialiser des données contenant des appréciations ou des jugements.

Cependant le droit européen de la liberté d'expression précise que certaines données peuvent être conservées et sauvegardées. Ainsi il est possible qu'une déclaration d'une personnalité ne soit pas automatiquement supprimée si l'intérêt public à la garder prévaut.

Il faut préciser cependant :

- Site de l'Assemblée Nationale :
  Il est rappelé que l'article 26 de la loi du 6 janvier 1978 « Informatique et libertés » prohibe toute collecte massive de ces adresses, à l'insu de leurs détenteurs, pour procéder à l'envoi massif de messages non désirés, quel que soit l'objet des messages diffusés.

- Site du Sénat :
  La liberté d'accès aux données à caractère personnel contenues dans les documents parlementaires n'emporte pas une liberté d'exploitation de ces données. Conformément aux dispositions de la « loi Informatique et Libertés », toute personne souhaitant collecter et réutiliser les informations diffusées sur ce site doit se conformer aux obligations lui incombant en sa qualité de responsable de traitement.

Interdiction de collecte des opinions politiques, philosophiques SAUF si les données ont été rendues publiques par la personne concernée
(Loi n° 78-17 du 6 janvier 1978 – version à jour RGDP) :

- Il est interdit de collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.
- **Exception, les traitements portant sur des données à caractère personnel rendues publiques par la personne concernée**

- Le consentement reste obligatoire en cas de traitement de ces données à caractère personnel rendues publiques par la personne concernée.
  CE, ss-sect. 10, 30 déc. 2015, n° 376845 : Il résulte de cette définition que le nom et les coordonnées des personnes physiques, telles que leurs adresses et leurs numéros de téléphone, constituent des informations relatives à une personne physique identifiée et, par suite, des données à caractère personnel au sens des dispositions de la loi du 6 janvier 1978. Dès lors, que ces données soient des coordonnées professionnelles des personnes physiques en cause, et qu'elles soient le cas échéant par ailleurs, est sans incidence à cet égard ; c'est donc à bon droit, que la Commission nationale de l'informatique et des libertés les a qualifiées de données à caractère personnel.
  - Pas de distinction vie privée et vie professionnelle
  - **Consentement obligatoire même si les données sont rendues publiques sur internet**

Fin de l'obligation de déclaration auprès de la CNIL du fichier, mais des outils de conformité :

- Site de l'Assemblée Nationale :
  En application de l'article 16, sont **également interdites la constitution de systèmes d'envoi automatisé de messages, la création de bases de données réunissant les adresses électroniques des députés** et la mise en place de traitements automatisés d'informations nominatives concernant les députés qui **ne seraient pas conforme au RGPD.**

- Cependant, l'un des axes du nouveau règlement est de **responsabiliser les acteurs traitant des données**. Alors que la directive de 1995 reposait en grande partie sur la notion de « formalités préalables » (déclaration, autorisations), le règlement européen repose sur une logique de conformité, dont les acteurs sont responsables, sous le contrôle et avec l'accompagnement du régulateur.

- La protection des données **dès la conception et par défaut**

- Mettre en place des mesures de protection des données appropriées et démontrer cette conformité à tout moment

Cela signifie pour les données détenues par les entreprises :

- La nécessité de faire des tests de sécurité régulièrement
- La mise en place d'une procédure qui permette de rétablir la continuité du service en cas d'atteinte à la fiabilité des données
- De notifier les risques éventuels sur la sécurité de vos données à la CNIL par l'intermédiaire du DPO.

Le lien avec la loi SAPIN 2 et déclaration HATVP.

Dans le cadre de l'activité de Représentation d'intérêts, les entreprises doivent désormais s'inscrire sur le site de la HATVP et y intégrer un certain nombre de données intégrant les actions de représentation d'intérêts.

Le répertoire HATVP
Sont enregistrés au répertoire les personnes exerçant une activité de représentation d'intérêts au nom de la personne morale.
Il importe dans ce cas de recueillir l'avis écrit des personnes concernées.

Le rapport d'activité AGORA:
Le rapport d'activité est structuré en fonction des questions sur lesquelles ont porté les actions de représentation d'intérêts.
Le rapport n'est pas nominatif ; il ne précise pas le nom des décideurs rencontrés, sollicités mais uniquement les catégories de responsables publics.
Une colonne facultative dite « observations » pourrait intégrer des données diverses dont des noms de personnes. Si tel est le souhait de l'organisme, il importe dans ce cas de respecter les règles du RGPD.

En cas de contrôle :
Afin de préparer le rapport d'activité et de se prémunir en cas de contrôle, il est fortement recommandé en interne de constituer un tableau détaillé intégrant les noms et fonctions des personnes rencontrées, à leur initiative ou pas. Mais également de sauvegarder « les preuves » de ces contacts : mail et notes envoyées, compte-rendu de RV…
Ces données devant être conservées dans une période de 5 ans.
Il s'agit bien de la gestion de fichiers. Ces fichiers doivent être impérativement réalisés sous contrôle du DPO. Ils peuvent dans certains cas être considérés comme données à risque.
Certaines données ne devant pas être transmises en externe, Il s'agit également de faire respecter les règles du secret des affaires.

LES ETAPES DE LA MISE EN PLACE DU RGPD

Ces étapes suggérées par la CNIL s'appliquent à toutes directions détenant des données

Les points clés de la conformité d'un traitement de données personnelles

Pour prouver sa conformité au règlement, il importe de constituer et regrouper la documentation nécessaire. Ces actions de conformité devant être réactualisées et réexaminées régulièrement.

Afin de piloter la gouvernance des données personnelles, il est conseillé de désigner un DPO qui a une mission de contrôle et de conseil en interne. La désignation peut se faire en ligne sur le site de la CNIL.

- **Le registre des traitements** ; il comprend les différents traitements de données personnelles, les catégories de données personnelles traitées, les objectifs poursuivis par les opérations de traitements de données, les acteurs internes et externes qui traitent ces données. Il importe de préciser les flux, l'origine et la destination des données.
  Il importe de préciser les process suivants : collecte, enregistrement, organisation, structuration, conservation, extraction, consultation, communication, transmission, diffusion.
  Et de répondre aux questions suivantes : Qui, quoi, pourquoi, Où, jusque quand, comment ?

  - ETAPE 1 : La tenue d'un registre des traitements mis en œuvre : Etablir une cartographie du traitement des données personnelles

- **L'information des personnes** ; il s'agit de compiler les mentions d'information diffusées en externe, les modèles de recueil de consentement des personnes concernées, les procédures mises en place.

  - ETAPE 2 : Points d'attention – Documenter les risques
    Seules les données strictement nécessaires à la poursuite de vos objectifs sont collectées et traitées.
    Il faut repenser le droit d'accès, de rectification, d'opposition, d'effacement, de portabilité, de limitation de traitement.

  - Identifier la base juridique du traitement (par exemple : consentement de la personne, intérêt légitime, contrat, obligation légale)
  - Réviser les mentions d'information afin qu'elles soient conformes aux exigences du règlement (articles 12, 13 et 14 du règlement)
  - Vérifier que les sous-traitants connaissent leurs nouvelles obligations et leurs responsabilités et notamment de l'existence de clauses contractuelles rappelant les obligations du sous-traitant en matière de sécurité, de confidentialité et de protection des données personnelles traitées.
  - Prévoir les modalités d'exercice des droits des personnes concernées (droit d'accès, de rectification, droit à la portabilité, retrait du consentement...)
  - Vérifiez les mesures de sécurité mises en place.

- **Les contrats** et particulièrement les contrats avec les sous-traitants, les procédures internes en cas de violation des données, et éventuellement les preuves de consentements.

  - ETAPE 3 : Mettre en place des procédures internes qui garantissent 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

- **Documentation de la conformité**
  - ETAPE 4 : Les éléments suivants doivent être disponibles :
  - Le registre des traitements (ETAPE 1)
  - Les mentions d'information (ETAPE 2)
  - Les modèles de recueil du consentement des personnes concernées (ETAPE 2)
  - Les procédures mises en place pour l'exercice des droits (ETAPE 2)
  - Les contrats avec les sous-traitants (ETAPE 2)
  - Les procédures internes en cas de violations de données (ETAPE 3). Il importe de conserver les listes d'opposition.
  - Les preuves que les personnes concernées ont donné leur consentement lorsque le traitement de leurs données repose sur cette base (ETALAB)

ANNEXE/ **RECOMMANDATIONS ET MODELES**

De façon générale, chaque message mail doit proposer systématiquement une possibilité de désinscription. Une fois la désinscription demandée, l'effacement des données doit s'effectuer dans les plus courts délais. Il importe de répercuter l'action de désinscription ou d'opposition au responsable du traitement. Celui-ci devant conserver la trace de toutes les personnes ayant demandé le désabonnement.

Formules suggérées bas de mail en nombre ou envoi de lettres groupées

- *Vous disposez d'un droit d'accès, de rectification et d'opposition aux données vous concernant, que vous pouvez exercer en contactant adresse mail.*

Ou

- *Conformément à l'article 32 de la loi 78-17, vous pouvez exercer votre droit d'accès et de rectification aux données vous concernant, ou vous désinscrire en contactant adresse mail*

Un mailing en nombre signifie le fait de faire un envoi non personnalisé à plusieurs personnes ; Dans le cas d'un publipostage personnalisé, on pourrait entendre mais sous toute réserve selon les cas qu'il s'agit d'envois nominatifs.

Les bas de mail dans le cas d'un mailing en nombre/ mentions obligatoires

Lors d'un envoi de mail il n'y a pas de collecte de données, donc les seules mentions obligatoires sont :

– L'identité et les coordonnées de l'expéditeur
– Le lien de désabonnement
– Les mentions Cnil concernant les droits : accès / rectification / modification de données

Exemple

Ce courrier électronique est envoyé par XXXX. Si vous ne souhaitez plus recevoir d'informations de notre part, il vous suffit d'adresser un courriel à adresse mail

Vous disposez d'un droit d'accès, de rectification et d'opposition aux données vous concernant, que vous pouvez exercer en contactant adresse mail

Les formulaires liés à la collecte de données sur site internet ou par mailing

Pour la collecte de données personnelles, voici les informations obligatoires à mentionner :

– L'identité du responsable du traitement
– La finalité de l'utilisation des données : démarches de Dialogue / événement/ prospection commerciale. Il importe de désormais préciser si le nom de la personne sera agrégé dans une liste transmise aux participants.
– La finalité du traitement des données ; la direction, le responsable…
– Les droits conférés par la loi aux consommateurs (à savoir le droit d'accès, de rectification, et d'opposition), ainsi qu'un mail de contact.
– Le nouveau texte impose désormais de faire figurer dans ces « mentions CNIL » la durée de conservation des données collectées ou les critères utilisés permettant de déterminer cette durée.

Exemple *:*

Les informations recueillies sur ce formulaire sont enregistrées dans un fichier informatisé par XXX pour permettre de vous adresser des contenus adaptés à vos enjeux. Elles sont conservées pendant ???? et sont destinées à ???? organisées par XXX.
Conformément à l'article 32 de la loi 78-17, vous pouvez exercer votre droit d'accès et de rectification aux données vous concernant, ou vous désinscrire en contactant adresse mail

Lors d'utilisation de fichiers qui n'ont pas été collectées par vous-mêmes

Le « vendeur » doit préciser par écrit et sur la facture en cas de vente

- que les adresses électroniques utilisées ont été collectées de manière régulière

- que la finalité de la collecte a été précisée (mention2)
- que l'utilisateur doit préciser lors de chaque utilisation les données légales (mention1)

Vous devez demander précisément par écrit au nouvel utilisateur du fichier de bien préciser les données légales.

Votre adresse mail est enregistrée dans un fichier informatisé conformément à notre politique de confidentialité. En indiquant votre adresse mail, vous acceptez de recevoir nos offres personnalisées. Vous pouvez vous désinscrire à tout moment en nous adressant un mail et à adresse mail
Ou selon les cas ;
Par notre intermédiaire, *vous pouvez être amené à recevoir des mails d'autres sociétés ou associations.*
Si vous ne le souhaitez pas, il vous suffit de le préciser adresse mail

Dans le cas de prospection commerciale

Il est formellement déconseillé de faire de la prospection électronique à partir d'adresses de courriers électroniques collectées dans les espaces publics de l'internet (site web, annuaire, forum discussion, …)
Il importe d'utiliser exclusivement les adresses de courriers électroniques collectées de manière loyale.
Il n'est pas nécessaire d'obtenir l'accord du destinataire lorsque :

- L'adresse électronique est de type générique (par ex : info@…, contact@…, commande@…)
- Le professionnel a été informé lorsqu'il a communiqué son adresse électronique de la possibilité de s'opposer gratuitement à toute utilisation commerciale de ses coordonnées :
    - L'objet de la sollicitation doit être en rapport avec les fonctions exercées à titre professionnel par le destinataire du message
    - Dans tous ces cas de figure, la CNIL recommande que le droit d'opposition puisse s'exercer directement à partir du formulaire de collecte par l'apposition d'une case à cocher ou d'un mail à envoyer

En validant mon inscription, j'accepte que les informations recueillies sur ce formulaire soient enregistrées afin de rendre le service/de livrer le produit et traitées conformément à notre Politique de confidentialité.
***[ ]** En cochant la case, vous acceptez de recevoir des propositions commerciales.*

Les sites internet

Pour les pages web accessibles d'un simple « clic » ; il faut s'assurer que le lien de désinscription fonctionne.
Une fois la désinscription demandée par l'internaute, l'effacement de ses données doit s'effectuer dans les plus courts délais.
Enfin, indiquez sur la page de désinscription le nom et les coordonnées du responsable du traitement et du propriétaire du fichier source s'il est différent du responsable du traitement.
Répercutez l'action de désinscription ou d'opposition au responsable du traitement

L'envoi de lettres d'information

S'assurer de l'inscription préalable de la personne sur l'envoi de telles lettres et de sa possibilité de pouvoir se désabonner à tout moment, notamment lors de l'envoi de chaque lettre d'information.
Utiliser toujours le système de destinataires multiples cachés afin de ne pas transmettre les données personnelles à des destinataires qui pourraient être malveillants et sans délégation d'autorisation des personnes concernées

Votre adresse mail est enregistrée dans un fichier informatisé conformément à notre politique de confidentialité. Vous pouvez vous désinscrire à tout moment en nous adressant un mail et à adresse mail