MAI 2018

Tout ce que vous devez savoir sur le RGPD_

Sommaire_

« L'informatique doit être au service de chaque citoyen [...]
Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme ni à la vie privée, ni aux libertés individuelles et publiques ».

La prochaine mise en œuvre du Règlement Général sur la Protection des Données (RGPD), agitée comme un épouvantail par de nombreux acteurs depuis quelques mois, se rapproche à grands pas. Dès le 25 mai 2018, ce Règlement Européen sera applicable en France, prolongeant le texte de loi français, la Loi n°78-17 du 6 janvier 1978, la célèbre « Loi Informatique & Libertés ».

Ce nouveau Règlement vise à poursuivre et garantir ces principes ; et à fournir un cadre lisible pour les acteurs impliqués. Il est plus facile de s'assurer de respecter des bonnes pratiques lorsque celles-ci sont transcrites en directives claires, et unifiées sur l'ensemble de l'Europe.

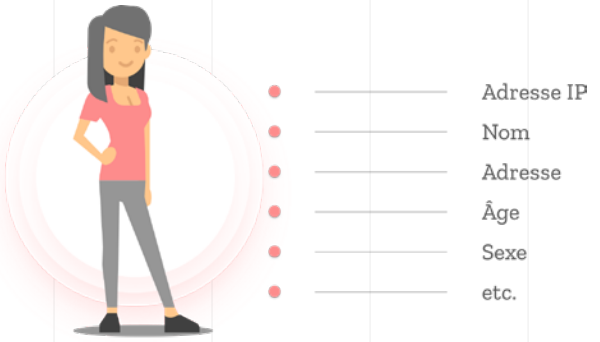
Le texte doit être appréhendé comme tel : un support réglementaire pour valider ses pratiques et méthodes autour de la donnée personnelle.

http://coulc.it/Aj0aG

Le RGDP en un coup d'œil_

RGPD

Les données personnelles_



RGPD

Les droits des personnes_

RGPD

Qu'est-ce qui est impacté ?_

Qu'est-ce qui est impacté ?_

01

Désigner un pilote

02

Inventaire exhaustif des données que vous traitez : registre des traitements

03

Prioriser les actions à mener : feuille de route selon les risques liés à la collecte

04

Gérer les risques (9 critères)

05

Organiser les procédures internes

06

Qu'appelle-t-on « Donnée Personnelle » ?_

D'après l'Art. 2 de la loi « Informatique et libertés »_

« 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 ».

La CNIL considère une personne comme identifiable lorsqu'un fichier comporte des informations permettant indirectement son identification, par l'intermédiaire de son adresse IP, nom, numéro d'immatriculation, numéro de téléphone, photographie, empreinte biométriques... ou encore tout autre ensemble d'informations permettant de discriminer une personne au sein d'une population (lieu de résidence, profession, sexe, âge...).

http://coulc.it/kAejv

Vous comprendrez donc aisément que l'ensemble des données collectées via un dispositif web, un outil de gestion commercial, CRM ou marketing... rentre dans le champ de la « Donnée Personnelle » - **pour faire clair, tout le monde est concerné par le RGPD.**

Que dit le texte ?_

Droits défendus par le texte_

Deux objectifs principaux : d'une part renforcer le droit des personnes dont les données sont traitées, et d'autre part responsabiliser les entreprises qui traitent des données grâce à un mécanisme d'« accountability ».

Droit à l'oubli

Permettant de demander l'effacement des données les concernant.

Droit à la portabilité des données

Consistant à récupérer des données les concernant dans un format structuré, couramment utilisé et lisible par machine.

Droit de limitation

Permettant de demander la suspension du traitement des données (et non la suppression).

Ainsi, les entreprises devront adapter leur système d'information afin de pouvoir stocker les données sans que celles-ci ne fassent l'objet de traitement ou de modification.

http://coulc.it/8fWq7

Responsabilités Obligations_

Respecter le principe de protection des données personnelles et de la vie privée imposées par le Règlement, dès la conception de tout projet (« privacy by design ») et ce, par défaut (« privacy by default ») .

Exemple emblématique :

Notifier toute violation de données à caractère personnel par le responsable de traitement et le sous-traitant aux autorités et aux personnes concernées.

Mise en conformité_

Le Règlement liste six étapes clefs dans la démarche de mise en conformité.

Étape 1
Désigner un pilote

« Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données. Vous pouvez d'ores et déjà désigner un « correspondant informatique et libertés », qui vous donnera un temps d'avance et vous permettra d'organiser les actions à mener. » *cnil.fr*

La désignation d'un délégué à la protection des données n'est pas obligatoire pour les structures privées (à l'opposé des entités publiques), celle-ci dépend de l'activité de l'entreprise vis-à-vis des données personnelles. Si votre activité est fondée sur l'exploitation de données, la question est tranchée : un DPO doit être désigné. Dans le cas contraire, si le traitement et l'exploitation de ces données reste secondaire dans votre activité, représente des petits volumes... il n'y a pas d'obligation.

Toutefois, il est fortement conseillé de désigner un pilote de la procédure de mise en conformité, que celui-ci soit effectivement délégué à la protection des données, ou plus simplement un Correspondant Informatique et Libertés (ou CIL). Dans le second cas, cette nouvelle mission peut être confiée à un de vos collaborateurs.

Le délégué à la protection des données

C'est le principal acteur et gardien de la conformité en matière de protection des données.

Ses missions, telles que mentionnées par cnil.fr :

- **d'informer et de conseiller le responsable de traitement** ou le sous-traitant, ainsi que leurs employés ;
- **de contrôler le respect du règlement** et du droit national en matière de protection des données ;
- **de conseiller l'organisme** sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution ;
- **de coopérer avec l'autorité de contrôle** et d'être le point de contact de celle-ci.

Il est donc responsable de l'ensemble de la conduite de la mise en place des directives du Règlement, et des mises en conformité présentes comme futures.

Il devra donc s'astreindre à une veille pour s'informer des nouvelles obligations et sensibiliser les décideurs sur l'impact de ces nouvelles règles.

Enfin, il pilotera les étapes suivantes de l'adoption du RGPD, à commencer par réaliser l'inventaire des traitements de données de l'entreprise.

cf. Infographie : http://coulc.it/xD7di

Étape 2
Cartographier vos traitements de données personnelles

Dresser un inventaire ; l'idée est de connaître l'étendue des données que votre entreprise traite elle-même, ou traite par l'intermédiaire de ses éventuels sous-traitant. Sans inventaire exhaustif, il sera impossible d'évaluer les impacts du nouveau Règlement. Cet inventaire est désigné par la CNIL sous la dénomination de « registre des traitements ».

Là encore, la Commission nous donne la procédure pour réaliser cet examen, en répondant à une série de questions simples :

Qui ?

- **Inscrivez dans le registre le nom et les coordonnées du responsable** du traitement (et de son représentant légal) et, le cas échéant, du délégué à la protection des données ;
- **Identifiez les responsables des services opérationnels** traitant les données au sein de votre organisme ;
- **Établissez la liste des sous-traitants**.

Quoi ?

- **Identifiez les catégories de données** traitées
- **Identifiez les données susceptibles de soulever des risques** en raison de leur sensibilité particulière (par exemple, les données relatives à la santé ou les infractions)

Pourquoi ?

- **Indiquez la ou les finalités pour lesquelles vous collectez ou traitez ces données** (exemple : gestion de la relation commerciale, gestion RH...).

Où ?

- **Déterminez le lieu** où les données sont hébergées.
- **Indiquez vers quels pays** les données sont éventuellement transférées.

Jusqu'à quand ?

- **Indiquez,** pour chaque catégorie de données, **combien de temps vous les conservez**.

Comment ?

- **Quelles mesures de sécurité sont mises en œuvre** pour minimiser les risques d'accès non autorisés aux données et donc d'impact sur la vie privée des personnes concernées ?

http://coulc.it/sXMG8 · http://coulc.it/vn18L · http://coulc.it/CCOab

Étape 3
Prioriser les actions à mener

Le registre constitué sert également de feuille de route pour les actions à mener. Les priorités de mise en conformité doivent être évaluées selon les risques liées aux données collectées et à leurs traitements.

Points de vigilance :

Relatif au type de données

- origine prétendument raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale,
- santé, orientation sexuelle,
- génétiques ou biométriques,
- infraction ou condamnation pénale,
- concernant des mineurs.

Relatif à l'objet de la collecte/traitement

- la surveillance systématique à grande échelle d'une zone accessible au public ;
- l'évaluation systématique et approfondie d'aspects personnels, y compris le profilage, sur la base de laquelle vous prenez des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative.

Relatif aux éventuels transferts des données hors zone Union européenne

- vérifiez que le pays vers lequel vous transférez les données **est reconnu comme adéquat par la Commission européenne** ;
- dans le cas contraire, **encadrez vos transferts**.

Étape 4
Gérer les risques

Neuf critères de risques liés aux traitements de données sont définis :

1. Évaluation ou notation ;
2. Décision automatisée avec effet juridique ou effet similaire significatif ;
3. Surveillance systématique ;
4. Données sensibles ou données à caractère hautement personnel ;
5. Données personnelles traitées à grande échelle ;
6. Croisement d'ensembles de données ;
7. Données concernant des personnes vulnérables ;
8. Usage innovant ou application de nouvelles solutions technologiques ou organisationnelles ;
9. Exclusion du bénéfice d'un droit, d'un service ou contrat.

Si un traitement rencontre au moins deux critères, il est conseillé de faire une analyse d'impact sur la protection des données (PIA).

http://coulc.it/Tl7lu

Étape 5
Organiser les processus internes

Assurer un haut niveau de protection des données passe par la mise en place de procédures internes, avec pour objectif d'anticiper l'ensemble des aléas de vie des données personnelles : incidents, demande de rectification, modification, changement de prestataire...

- **instituer « la privacy by design »,** soit la protection prise en compte dès la conception d'une application ou d'un traitement. À commencer par les exigences de minimisation de la collecte de données au regard de la finalité, cookies, durée de conservation, mentions d'information, recueil du consentement, sécurité et confidentialité des données...
- **favoriser la sensibilisation des équipes**, mener des actions de formation et de communication ; la protection des données personnelle est l'affaire de chacun et non celle du seul DPO
- **structurer les protocoles réponses aux réclamations et demandes** des personnes quant à l'exercice de leurs droits : droits d'accès, de rectification, d'opposition, droit à la portabilité, retrait du consentement
- **anticiper les violations de données**, prévoir les crises, par exemple la notification à l'autorité de protection des données dans les 72 heures et aux personnes concernées dans les meilleurs délais.

http://coulc.it/P3YxK

Étape 6
Documenter la conformité

La preuve de bonne conformité au Règlement passe par la constitution d'une documentation, qui devra bien entendu être tenue à jour régulièrement.

La documentation sur les traitements de données personnelles :

- registre des traitements
- analyses d'impact sur la protection des données (PIA)
- encadrement des transferts de données hors UE

L'information des personnes

- mentions d'information
- modèles de recueil du consentement des utilisateurs
- procédures mises en place pour l'exercice des droits

Les contrats définissant rôles et responsabilités des différents acteurs

- Les contrats (sous-traitants)
- Les procédures internes en cas de violations de données
- Les preuves de consentement des utilisateurs

http://coulc.it/SD2n

Impacts_

Cookies

L'article 30 du RGPD précise :

« Les personnes physiques peuvent se voir associer [...] des identifiants en ligne tels que des adresses IP et des témoins de connexion (« cookies ») ou d'autres identifiants [...]. Ces identifiants peuvent laisser des traces qui, notamment lorsqu'elles sont combinées aux identifiants uniques et à d'autres informations reçues par les serveurs, peuvent servir à créer des profils de personnes physiques et à identifier ces personnes. »

- **Le consentement implicite n'est plus suffisant.** Fini le tristement célèbre **« en utilisant ce site, vous acceptez notre politique de cookies »**, le consentement doit être donné par une action utilisateur affirmative claire et motivée telle que cocher une case d'acceptation ou régler des préférences dans un menu de configuration dédié aux cookies.

Un site web doit désormais offrir la possibilité d'accepter ou non les cookies.
« donner l'opportunité d'agir avant que les cookies ne soient réglés lors d'une première visite sur un site. »

- **De même, Il doit être aussi facile de retirer son consentement que de le donner**. L'interface de préférences relative aux cookies devra donc rester accessible pendant toute la consultation du site, de façon à permettre à l'usager de modifier son choix dans un sens comme dans l'autre.

Cookies exemptés de consentement

Certains cookies (ou traceurs) strictement nécessaires au fonctionnement du site (on parlera de fourniture d'un service) ne requièrent pas de consentement :

- les cookies de « panier d'achat »
- les cookies « identifiants de session », pour la durée d'une session, ou les cookies persistants limités à quelques heures dans certains cas
- les cookies d'authentification
- les cookies de session créés par un lecteur multimédia
- les cookies persistants de personnalisation de l'interface utilisateur (choix de langue ou de présentation)
- les cookies liés à l'infrastructure (par ex. équilibrage de charge ou « load balancing »)
- ou encore certaines solutions d'analyse statistiques (exemple Xiti qui offre une formule spécifiquement exemptée).
  http://coulc.it/I3SKd

Abonnements aux newsletters

De même que pour les cookies, le texte instaure la règle du consentement préalable et explicite de l'utilisateur avant de l'abonner à toute liste de diffusion marketing ou commerciale.

- **Terminé, la case pré-cochée** « je m'abonne à la newsletter » lorsqu'un utilisateur remplit un formulaire qui n'est pas précisément dédié à cet usage (ouverture de compte, formulaire de contact, candidature, etc)
- **Dans le cas de souscription à des offres commerciales d'entreprises tierces**, une seconde case bien distincte devra être proposée, avec la mention explicite de l'usage à fins de « propositions commerciales de nos partenaires » qui sera fait de l'adresse soumise
- **Détenir un compte client/utilisateur sur un site ou service en ligne ne peut être considéré comme une souscription tacite à une newsletter**
- **L'accès au désabonnement devra lui aussi être proposé de façon simple** et accessible (notamment dans chaque message adressé aux abonnés)
- **L'éditeur de la newsletter devra conserver un historique des abonnements** (horodatage précis, interface utilisée) ainsi que des désabonnements

Toute base de contact, ou d'abonnés, non conforme à ces règles deviendra de facto inutilisable à compter du 25 mai 2018.

Plus que jamais, l'externalisation de la gestion des newsletters, ou le recours à des services dédiés - pour autant que ceux-ci offrent des garanties de conformité à la nouvelle réglementation - sera largement préférable à une solution « maison » qui sera difficile à faire évoluer vers une totale conformité.

Logiciels CRM & RGPD

Les solutions CRM étant par nature gourmandes en données personnelles, les obligations de mise en conformité s'appliquent à celles-ci de la même façon. Même le logiciel CRM est considéré comme un « sous-traitant de données », c'est l'entreprise qui est responsable des données collectées, transmises et enfin exploitées par le CRM.

L'entreprise « cliente » d'une solution CRM ne peut pas se reposer aveuglément sur cette dernière pour sa conformité avec la RGPD, il relève de sa responsabilité de valider la conformité du « sous-traitant de données ».

Le « sous-traitant » devra :

- prouver sa conformité à la réglementation (par les mêmes prérogatives que celles mentionnées plus haut)
- garantir l'intégrité des données récoltées (sécurisation, confidentialité, sûreté face aux attaques ou pannes)
- garantir l'exercice des droits des utilisateurs : modification, suppression des données, etc. tout en tenant un historique de ces opérations.

Il faut retenir que les données transmises à un sous-traitant engagent la responsabilité l'entreprise tout autant que celles traitées en interne, il est donc indispensable d'obtenir toutes les garanties de conformité de la part de l'ensemble des tiers amenés à manipuler ces données.

Phantom IT / Rogue IT

On appelle "Rogue IT", ou "Phantom IT", les systèmes d'information présents dans l'entreprise mais non connus de sa DSI ou de l'autorité sensée en porter l'autorité.

Si il peut paraître évident qu'un projet CRM porté par une équipe dédiée, largement cadré et documenté pourra facilement s'ajuster aux nouvelles règles, ce sera bien moins le cas d'initiatives "pirates" ou "improvisées" : mailing-list improvisées avec une feuille de tableur et un client mail, site web hébergé sur un service grand public en ligne, etc.

L'un des enjeux la mise en conformité est aussi pour l'entreprise sa réappropriation de l'ensemble des traitements de données.

Notifier toute violation de données

Le texte introduit l'obligation de notification à l'autorité de contrôle (en France la CNIL) d'une violation de données à caractère personnel, dans les 72 heures suivant la détection de l'incident.

Par la suite une communication auprès des usagers devra détailler l'ampleur de l'incident, les données perdues ou dérobées, et les actions requises ou planifiées par l'éditeur pour faire face à cette violation.

Conclusion_

Les traitements de données personnelles sont comme les robots chez Asimov :

1_ *un traitement de données ne peut porter atteinte à une donnée personnelle, ni, en restant passif, permettre qu'une donnée personnelle soit exposée au danger ;*

2_ *un traitement de données doit obéir aux ordres qui lui sont donnés par un être humain, sauf si de tels ordres entrent en conflit avec la première loi ;*

3_ *un traitement de données doit protéger son existence tant que cette protection n'entre pas en conflit avec la première ou la deuxième loi.*

Lexique_

- **GRDP** › General Data Protection Regulation
- **RGPD** › Règlement Général sur la Protection des Données
- **DCP** › Données à Caractère Public
- **DPD** › Délégué à la Protection des Données
- **DPO** › Data Protection Officer
- **CIL** › Correspondant Informatique et Libertés
- **CNIL** › Commission nationale de l'informatique et des libertés
- **CRM** › Customer Relationship Management

Ressources utiles_

La CNIL met à disposition une foule de ressources utilitaires :

- **modèles-type de mentions** d'information
- modèles de formulaires de recueil du consentement
- modèle de **registre simplifié**
- information sur les **droits des personnes**
- d**ossiers thématiques à destination des professionnels du marketing et du commerce en ligne**
- **guide** élaboré **à destination des TPE-PME**
- **plan d'accompagnement à destination des startups**

Merci
de votre attention.

AGENCE DE COMMUNICATION_
PARIS & TOULOUSE

06 34 51 38 15
info@couleur-citron.com