E-Book - DataFactory

Avril 2017

NOVENCIA

General Data Protection Regulation

« Le compte à rebours est lancé »

25 mai 2018

Transformez le changement en opportunité !

www.NOVENCIA.com - 21 rue de la banque 75002 Paris

INTRODUCTION

300 000 tweets, 15 millions de SMS, 200 millions d'e-mails chaque minute à travers le monde… Sans compter les milliards de données générées par les objets connectés et celles collectées lorsque nous naviguons sur le Web ou que nous passons des commandes sur les sites marchands. Aujourd'hui, la donnée est au centre de toutes les attentions. En moins de cinq ans, elle est devenue un actif clé de l'entreprise et les qualificatifs ne manquent pas : « Or noir », « pétrole du XXIème siècle »… Désormais, de nombreuses entreprises innovantes fondent leur modèle économique sur l'exploitation de ces fameuses données personnelles.

Mais pour le citoyen, évoquer la notion de donnée personnelle, c'est une toute autre histoire. Pour le citoyen, c'est évoquer la notion de confidentialité, de libre circulation des informations personnelles. Depuis la loi Informatique et Libertés du 6 janvier 1978, les principes de licéité de la collecte de données personnelles sont posés : proportionnalité des données collectées par rapport à la finalité du traitement, loyauté de la collecte, droit d'opposition des personnes concernées, interdiction de principe de la collecte de données sensibles.

Avec l'arrivée du réglement du 14 avril 2016, plus connu sous le nom de GDPR pour General Data Protection Regulation, le devoir d'information des personnes a été renforcé, rendant, dans certains cas, le consentement obligatoire. Désormais, c'est aux entreprises qu'incombe la responsabilité de la manipulation des informations, depuis la localisation des données sensibles sur le réseau jusqu'à la gestion des accès, le stockage et la sécurité.

C'est un chantier lourd que les entreprises doivent, dès à présent, prendre à bras le corps, car il ne leur reste plus que quelques mois avant l'injonction de mise en conformité. Mais au-delà de la contrainte réglementaire, les entreprises doivent comprendre que le GDPR est une véritable opportunité, un tremplin vers une gouvernance des données gagnant-gagnant. Car si la data est le nouvel or noir, la confiance est une nouvelle monnaie d'échange !

La directive de 1995 (95/46/CE) sur les données personnelles est morte !
Vive le GDPR !

Sommaire

LE GRAND « DATA MÉNAGE »

Le General Data Protection Regulation (GDPR), est un réglement européen (2016/679) adopté en avril 2016 et qui sera applicable le 25 mai 2018. Ce texte à effet direct, c'est à dire qu'il n'y a pas besoin de loi nationale pour le transposer, a pour objectif l'amélioration de la protection et de la confidentialité des informations personnelles identifiables.

Dans un monde numérique de téléphones intelligents, de médias sociaux, de services bancaires sur internet et de transferts mondiaux, l'adoption de ce réglement doit permettre à l'Europe de s'adapter aux nouvelles réalités du numérique. Au niveau local, elle oblige les entreprises à procéder à un grand « Data Ménage » dans les données qu'elles ont librement collectées et stockées jusqu'à présent. Car, à l'avenir, les entreprises devront accorder une attention toute particulière aux données dites « sensibles ». Car ce sont elles, au regard du réglement, qui présentent des risques particuliers d'atteinte aux droits et libertés.

Pour un grand nombre de professionnels, cette réglementation arrive au bon moment. *« Course à la digitalisation, intelligence artificielle, machine learning, robotisation, IoT. Avec l'émergence de l'économie collaborative et de celle des plateformes, nous devons établir une vraie relation de confiance entre le consommateur et les différentes entreprises qui utilisent les données. »*, estime **Philippe Deljurie, X-PM partners.**
D'un point de vue juridique, *« cette réglementation est équilibrée car elle protège les intérêts des individus tout en protégeant l'innovation. Avec ce texte de 200 pages, on a une convergence d'intérêts contradictoires qui sont l'émergence de la société européenne numérique et l'émergence d'un citoyen européen. Le GDPR est donc une grande avancée en terme d'uniformisation et de simplification des droits sur la protection des données sur quasiment toute la surface de la planète. »*, souligne **Maître Lipskier.** En effet, le réglement offre un cadre légal uniforme dans tous les pays membres, ce qui évitera les disparités qui peuvent résulter des lois de transposition nationales.

Le champ d'application du réglement est donc sans limite. Où qu'elle soit, même hors UE, toute entreprise doit s'y soumettre dès l'instant où les données traitées sont relatives à une offre de biens ou de services ou à des personnes qui sont dans l'Union européenne.

Ce nouveau champ d'application permet également de réguler les pratiques d'entreprises étrangères, qui sans ouvrir d'établissement sur le territoire de l'Union, ciblent pourtant un marché européen.

« Ce texte est incomplet. De plus, il présente pas moins de 50 exceptions nationales. À moins d'un an de la mise en conformité au 25 mai 2018 nous ne disposons pas de l'information nécessaire pour mettre en œuvre la totalité des opérations de mise en conformité. C'est un réglement complexe à mettre en œuvre dans un laps de temps très court. À mon sens, c'est un vrai sujet d'inquiétude. »

Paul-Olivier Gibert, Dirigeant chez Digital & Ethics et Président de l'AFCDP (Association française des Correspondants à la protection des Données à caractère personnel)

Qu’est-ce qu’une donnée personnelle ?

Toute information relative à une personne physique identifiée ou qui peut être identifiée directement ou indirectement par référence à un identifiant tel que le nom, un numéro d’identification, une donnée de localisation, un identifiant en ligne, une adresse IP, etc.

Qu’est-ce qu’une donnée sensible ?

Les données sensibles sont celles qui font apparaître, directement ou indirectement, les origines raciales, ethniques, les opinions politiques, philosophiques ou religieuses, l’appartenance syndicale des personnes, ou celles relatives à la santé ou à la vie sexuelle.

Par principe, la collecte et le traitement de ces données sont interdits.

Cependant, dans la mesure où la finalité du traitement l’exige, ne sont pas soumis à cette interdiction :

- Les traitements pour lesquels la personne concernée a donné son consentement exprès.
- Les traitements justifiés par un intérêt public après autorisation de la CNIL ou décret en Conseil d’Etat.

La collecte et le traitement de ces données doivent, dans ces hypothèses, être justifiés au cas par cas, au regard des objectifs recherchés.

Qu’est-ce qu’un traitement ?

C’est une opération ou un ensemble d’opérations efféctués sur des données à caractère personnel quel que soit le procédé, automatisé ou non. Un traitement est notamment constitué de la collecte, l’enregistrement, l’extraction, l’organisation, le stockage, la modification, la consultation, l’utilisation, la diffusion, l’effacement ou la destruction, etc.

VERS UNE EUROPE NUMÉRIQUE, LES GRANDS CHANGEMENTS DU GDPR

À partir du 25 mai 2018, toutes les entreprises ou organisations localisées au sein d'un pays membre de l'UE, mais également situées hors UE sont concernées par la mise en conformité dès lors qu'elles collectent, traitent ou stockent des données à caractère personnel (DCP). Et si une entreprise fait appel à un sous-traitant, elle doit s'assurer que ce dernier sera en mesure de respecter le GDPR.

Le principe d'accountability

Jusqu'à présent, les responsables de traitement étaient soumis à un système déclaratif ou d'autorisation préalable à la mise en place de traitements de données auprès des autorités de contrôle (la CNIL en France). Avec la mise en place du nouveau réglement, *« on a une bascule. On passe d'un régime déclaratif hérité de la directive de 1995 à une démarche responsable (accountability), selon laquelle un responsable de traitement devra démontrer à son autorité de contrôle qu'il se conforme à ses obligations »*, explique **Paul-olivier Gibert, président de l'AFCDP**.

En pratique, le « principe de responsabilité » est en fait une « obligation de rendre compte ». Il implique que le responsable d'un traitement de données personnelles adopte des mesures techniques et organisationnelles garantissant le respect de la réglementation. Selon **Maître Lipskier** « c'est un des grands bouleversements du nouveau réglement. Celui de passer d'*une responsabilité a posteriori à une responsabilité a priori. Cette responsabilité impacte toutes les entreprises. Elles doivent toutes, dès à présent, se préparer et s'adapter à rapporter la preuve de la conformité de leurs traitements de données aux principes posés par le Réglement ».*

Concrètement, cela implique que chaque organisme devra édicter une politique de protection des données personnelles sur-mesure selon le traitement auquel il procède. En effet, le G29 (Groupe de travail réunissant les 29 autorités indépendantes européennes de protection des données) précise que la mise en pratique du principe d'« Accountability » suppose une analyse au « cas par cas ».

« Le GDPR n'est pas un réglement qui donne réponse à tout. Il donne des orientations, vous explique qu'il faut mettre en place des mesures techniques et organisationnelles. C'est donc à l'entreprise d'interpréter le réglement et de définir un référentiel. Ce référentiel reprendra donc l'ensemble de vos règles par rapport aux points de conformité du réglement. »

Thierry Brun, GDPR Ambassador Software Segment Leader – IBM Europe

« Dès le départ, il est essentiel de mener un certain nombre d'investigations en interne pour faire un état des lieux des données que l'entreprise possède. Ce n'est qu'en passant par une parfaite connaissance de la donnée qu'on pourra par la suite identifier quels services innovants pourront en découler. »

Arnaud Zilliox, fondateur NOVENCIA Group

MESURES TECHNIQUES ET ORGANISATIONNELLES, DE QUOI PARLE-T-ON ?

En pratique, pour garantir le respect du réglement, plusieurs éléments factuels devront être pris en compte : la nature du traitement mis en œuvre, le contexte, la portée et la finalité. Il convient donc d'évaluer les risques pour les droits et libertés des personnes.

PRIVACY BY DESIGN

Cette approche consiste pour une entreprise à développer des produits et des services en prenant en compte, dès leur conception et tout au long de leur cycle de vie, les aspects liés à la protection de la vie privée et des données à caractère personnel. (Article 25)
L'implémentation d'une approche privacy by design constitue ainsi un gage supplémentaire de qualité et de confiance pour l'entreprise quant au traitement des données à caractère personnel des clients mais également des salariés, partenaires, prestataires.

PRIVACY BY DEFAULT

Cette approche signifie que les paramètres les plus contraignants en matière de protection des données sont automatiquement appliqués lorsqu'un client acquiert un nouveau produit ou service. Concrètement, il n'incombe plus aux clients et aux utilisateurs d'ajuster manuellement leurs paramètres de confidentialité.

La **pseudonymisation et le cryptage** (article 4) permettent de ne plus pouvoir associer des données à une personne physique précise sans avoir recours à des informations supplémentaires.

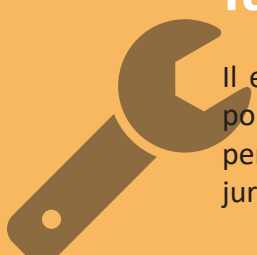
La **minimisation des données** (article 5-1), qui consiste à ne traiter que des données adéquates, pertinentes et limitées à la finalité du traitement.

La **disponibilité** des données et l'accès à celles-ci en cas d'incident (fuite, violation).

La capacité de **tester, analyser et évaluer** l'efficacité des mesures de sécurité.

> ***« L'enjeu de la réglementation, c'est plutôt d'adopter un code de bonne conduite. Il s'agit de mettre en place des pratiques et des process autour de la donnée personnelle. C'est ce que demande le GDPR, des solutions qui correspondent à des situations. »***
>
> Cyril Lefevre, Business Solution Manager – Data Management chez SAS

Comment l'entreprise peut faire face à ces exigences ?



Il est d'ores et déjà possible de faire un état des lieux des différentes politiques internes à l'entreprise en lien avec la protection des données personnelles. Un audit peut également être réalisé par des experts juridiques et techniques.

LA SÉCURITÉ DES DONNÉES

La sécurité des données personnelles devra être assurée par le responsable de traitement mais aussi par le sous-traitant. Leur objectif commun est ainsi d'assurer la confidentialité, l'intégrité, la disponibilité et surtout la notion nouvelle de *« résilience des systèmes et des services de traitement des données ».*

Avec l'arrivée du GDPR, l'enjeu est double : technique et juridique.

Technique tout d'abord, car avec la démultiplication des traitements se pose la question de la sécurité des données et plus largement du rôle des acteurs du cloud. Selon **Thierry Guenoun, Directeur Europe Moyen Orient et Afrique pour Appdome**, qui collabore régulièrement avec des acteurs du secteur *« On peut partir du principe que ces entreprises sont à peu près prêtes. Elles ont déjà mis en place des outils susceptibles de suivre le cheminement de la donnée jusqu'au poste de travail. ».*

Toutefois, l'expert émet des réserves quant au chemin qu'il reste à parcourir pour que les *« collaborateurs de l'entreprise adoptent un comportement idoine pour être en conformité »* car selon lui *« on passe avec le GDPR d'une infrastructure de la sécurité à une sécurité périmétrique et il n'est pas certain qu'au 25 mai 2018 les entreprises seront en mesure de dire si elles sont conformes au processus de sécurité exigé par le réglement ».*

Juridique ensuite, car les exigences du nouveau réglement a une influence directe sur les futurs contrats conclus avec les prestataires. Sont concernées également, toutes les procédures en vigueur au sein d'une entreprise.

Le cas des sous-traitants

Jusqu'ici les sous-traitants avaient une responsabilité contractuelle vis-à-vis du responsable du traitement sous réserve d'un contrat écrit entre les deux parties.

A partir du 25 mai 2018, même en l'absence d'un contrat signé, les sous traitants seront désormais partiellement responsables des traitements de données qu'ils mettent en œuvre pour le compte d'une entreprise tierce. Ils pourront donc être audités voire sanctionnés en cas de non-respect du GDPR.

Quelles sont leurs nouvelles obligations ?

- Tenir un registre des traitements
- En cas de violation de sécurité, mettre en œuvre les procédures et mesures de sécurité
- Contester les instructions du responsable de traitement si elles sont contraires à la loi
- Assister le responsable de traitement en cas de demande d'accès, d'effacement, de portabilité, etc.

« Aujourd'hui, beaucoup d'entreprises stockent de la donnée sans la classifier et sans savoir à quoi elle correspond. Il est important, avant d'engager des reformes et une mise en conformité, que les entreprises soient sûres que leurs systèmes d'information, leurs hébergeurs et leurs données soient absolument classifiés. »

Thierry Brun, GDPR Ambassador Software Segment Leader – IBM Europe

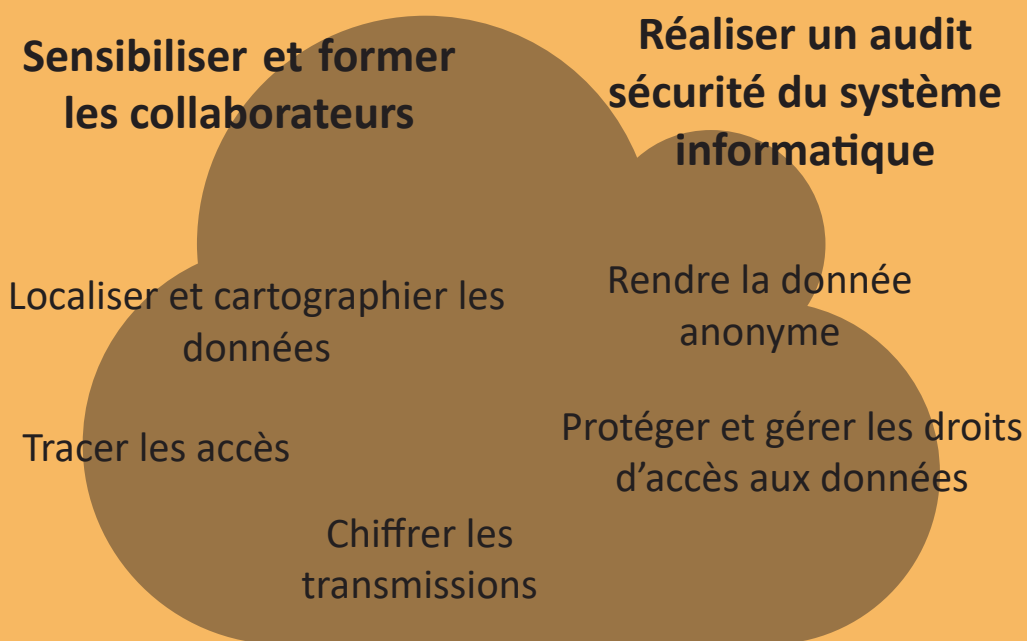
Comment sécuriser les données ?

Sécuriser un système informatique nécessite de prendre en compte tous les aspects de sa gestion. Cette sécurité passe par le respect de bonnes pratiques et le maintien de l'outil informatique à l'état de l'art quant aux attaques dont il peut faire l'objet.

La définition du risque selon la CNIL

Un risque est un scénario qui combine une situation crainte (atteinte de la sécurité des traitements et ses conséquences) avec toutes les possibilités qu'elle survienne (menaces sur les supports des traitements). On estime son niveau en termes de gravité (ampleur et nombre des impacts) et de vraisemblance (possibilité/probabilité qu'il se réalise). Pour la CNIL, gérer les risques est un moyen efficace de protéger les «libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, à l'égard du traitement des données à caractère personnel» (article premier de la Directive 95/46/CE).

Comment procéder ?



ENTREPRISES : COMMENT SE METTRE EN ORDRE DE MARCHE ?

Lors du colloque « GDPR, une bombe à retardement ? » qui s'est tenu le 2 mars, l'ensemble des acteurs présents se sont accordés sur un point : la différence de maturité et le niveau d'information des entreprises. Comme le souligne **Arnaud Zilliox, fondateur de NOVENCIA Group** *« des acteurs comme la MGEN, certaines banques, assurances ou des Telecom ont pris le chantier à bras le corps mais aucun acteur aujourd'hui sur le marché ne peut dire qu'il est prêt ».*

Concrètement, c'est le taux d'exposition d'une entreprise ou d'une organisation aux données personnelles qui va déterminer son degré de mise en conformité. C'est à dire, plus une entreprise est exposée aux données personnelles, plus son niveau de risque est élevé. La première étape dans une démarche de mise en conformité *« c'est de faire une analyse de risque à tous les niveaux »* préconise **Thierry brun, GDPR Ambassador, Software Segment Leader – IBM Europe**

Alors, à moins de quelques mois de la mise en conformité, comment se préparer ?

Garder la tête froide, se mettre en ordre de marche et envisager le nouveau réglement comme une opportunité. Celle de remettre la confiance au cœur de la relation qu'entretient l'entreprise et l'utilisateur, son client ! Un autre point sur lequel s'accordent les experts.

« À quelques mois de la transposition du réglement en droit national, la première étape doit obligatoirement être une phase d'audit, afin de délimiter et décrire le contexte du(des) traitement(s) considéré(s) et ses enjeux notamment en terme de risque(s). Il revient à chaque entreprise de trancher sur la notion de donnée sensible. Mesurer les risques, c'est la possibilité de déterminer les mesures nécessaires et suffisantes, sur la base d'éléments objectifs, de les hiérarchiser et ainsi optimiser les coûts. »

Arnaud Zilliox, Fondateur de NOVENCIA Group

Afin de maintenir la conformité dans le temps, la mise en œuvre du GDPR s'accompagne inévitablement d'un programme de conduite du changement, de sensibilisation et de formation de l'ensemble des responsables Métiers et IT, en interaction avec des domaines clients, sur ce texte et ses enjeux. Sans cela, il est impossible de garantir dans le temps une conformité de l'entreprise.

De plus, au-delà du seul aspect réglementaire, la mise en conformité GDPR doit aussi être vue comme une double opportunité : garder la confiance de ses clients mais également donner plus de valeur aux données de l'entreprise, en assurant une bonne gouvernance de celles-ci.

C'est pourquoi chez NOVENCIA, nous préconisons une démarche qui intègre les aspects IT et juridiques.

Dans une démarche de mise en conformité, **2 étapes sont primordiales :**

- La première phase consiste à réaliser un audit afin de déterminer la situation de l'entreprise au regard de la réglementation
- La deuxième phase va consister à traiter chaque processus afin de le mettre en conformité

Phase 1 : Audit

Plusieurs approches sont possibles. NOVENCIA a choisi d'adopter une approche « Data Driven » afin de réaliser une étude de risque GDPR.

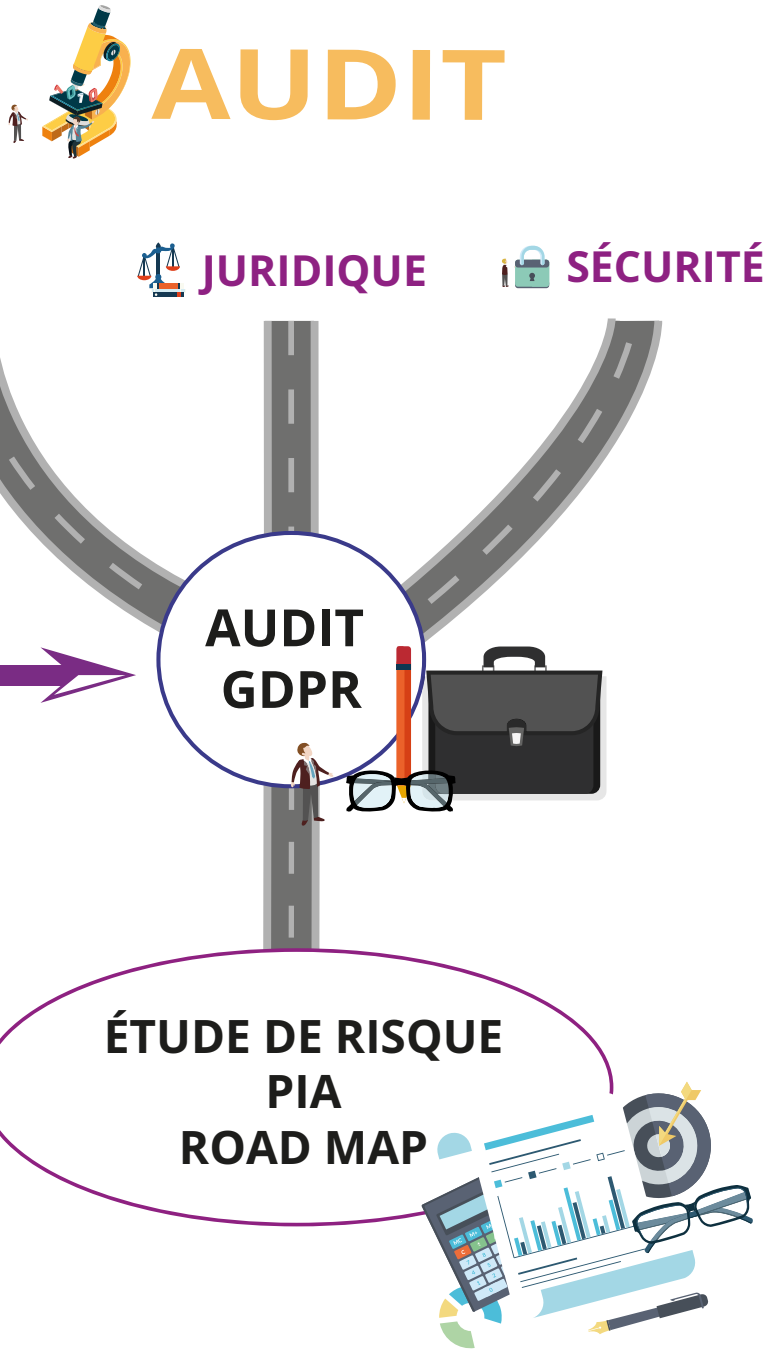
Concrètement, 2 étapes sont nécessaires.

La première étape consiste à recenser l'ensemble des données personnelles stockées au sein de l'entreprise. L'objectif étant de les identifier et surtout de les localiser au sein du système d'information. Suivant le contexte, cette étape peut se réaliser par domaine ou en une seule fois. Nous conseillons toutefois l'utilisation d'outil de Data Management ou Data Quality afin d'être certains de récupérer l'exhaustivité des données personnelles.

Lors de la deuxième étape, nous réalisons une étude de risque(s) à la fois technique et juridique sur ces données ainsi que sur le système d'information en général. A l'issue de cette étude, nous sommes en mesure de proposer au client une roadmap priorisée des actions à entreprendre pour la mise en conformité.

Phase 2 : Remédiation

Pour la mise en œuvre des actions de remédiation, nous préconisons, dans une approche agile, de remonter des données aux processus afin d'assurer leur mise en conformité.
En fonction du cas d'usage à traiter (application spécifique, progiciel, datalake, e-commerce), une approche had hoc devra être envisagée afin d'assurer la mise en conformité de la donnée personnelle, de son acquisition à sa destruction.


AUDIT
IT
JURIDIQUE
SÉCURITÉ
RÉGLEMENT GDPR
AUDIT GDPR
ÉTUDE DE RISQUE
PIA
ROAD MAP

LE DATA PROTECTION OFFICER

La personne qui endossera cette responsabilité devra connaître quelles sont les données collectées et stockées, la finalité de leur stockage, et pouvoir communiquer ces informations aux intéressés sur simple requête.

Qui peut être DPO ?

S'il n'est pas accompagné par son service juridique et/ou un avocat, *« le délégué doit posséder des connaissances spécialisées de la législation et des pratiques en matière de protection des données. Une connaissance du secteur d'activité et de l'organisme pour lequel il est désigné est également recommandée. Il doit enfin disposer de qualités personnelles, et d'un positionnement lui donnant la capacité d'exercer ses missions en toute indépendance »*. (source, CNIL)

Dans quel cas la désignation d'un DPO est-elle obligatoire ?

- **Autorités ou Organismes publics** : ministères, collectivités territoriales, personnes morales (de droit public ou privé)

- **Traitement régulier et systématique des personnes à grande échelle** (profiling): compagnies d'assurance ou banques pour leurs fichiers clients, opérateurs téléphoniques ou fournisseurs d'accès internet...

- **Traitement « à grande échelle » des données sensibles** : données biométriques, génétiques, origine raciale ou ethnique, convictions religieuses ou philosophiques ou l'appartenance syndicale…

Dans les autres cas : en dehors des cas de désignation obligatoire, la désignation d'un délégué à la protection des données est encouragée notamment pour les entreprises qui comptent plus de 250 salariés.

L'INFLATION DES SANCTIONS

Pour qu'elles soient dissuasives et contraindre les GAFA à se plier à la politique européenne de protection des données personnelles, l'article 79 du réglement édicte que, les amendes prononcées en cas d'infraction doivent être « effectives, proportionnées et dissuasives »

Avant le 25 mai 2018

150 000 euros maximum pour un premier manquement constaté (article 47 de la loi Informatiques et Libertés).

Si l'entreprise réitère

300 000 euros ou 5% du chiffre d'affaires hors taxes du dernier exercice clos, dans la limite de 300 000 euros (article 47 de la loi Informatiques et Libertés).

À partir du 25 mai 2018

10 000 000 euros ou 2% maximum du chiffre d'affaires annuel mondial total de l'exercice précédent pour un premier manquement constaté (article 79 du réglement).

Dans quel cas : absence de sécurité des données, absence de privacy by design et by default, absence de registre des traitements, absence de notifications de violation(s) de données, non respect des règles de nomination d'un DPO.

20 000 000 euros ou 4% maximum du chiffre d'affaires annuel mondial total de l'exercice précèdent (article 79 du réglement).

Dans quel cas : absence de respect des principes fondateurs du GDPR, non respect du consentement éclairé, absence de respect des dispositions concernant le transfert de données hors de l'espace économique européen.

LES NOUVEAUX DROITS DES CITOYENS

Le nouveau réglement permettra au citoyen de disposer d'informations complémentaires sur le traitement de ses données mais également de les obtenir sous une forme claire, accessible et compréhensible.

Le droit à l'oubli est conforté et un nouveau droit, le droit à la portabilité, est prévu, rendant ainsi plus effective la maîtrise de ses données par la personne. Les mineurs font également l'objet d'une protection particulière.

Je peux emporter mes données

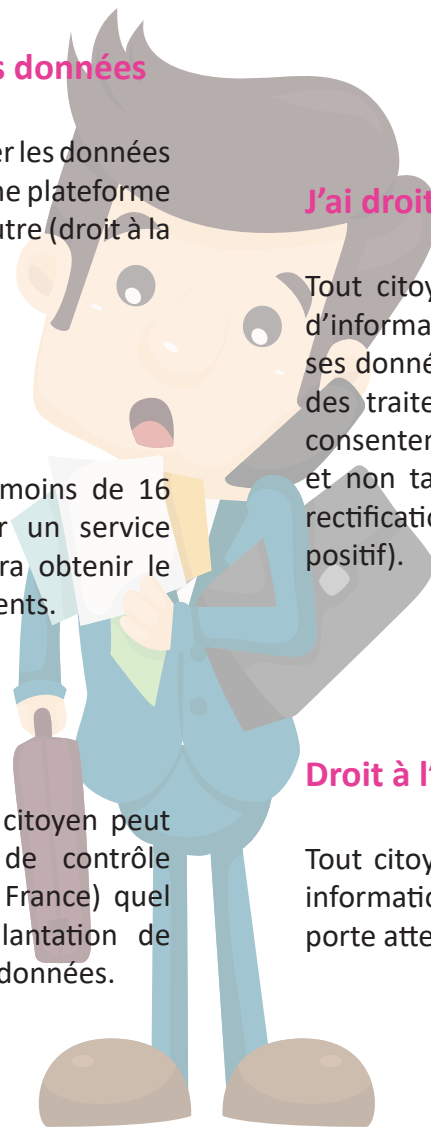
Tout citoyen peut récupérer les données qu'il a communiquées à une plateforme et les transmettre à une autre (droit à la portabilité).

Droit des mineurs

Avant qu'un mineur de moins de 16 ans puisse s'inscrire sur un service en ligne, ce dernier devra obtenir le consentement de ses parents.

Un guichet unique

En cas de problème, un citoyen peut s'adresser à l'autorité de contrôle de son pays (la CNIL en France) quel que soit le pays d'implantation de l'entreprise qui traite ses données.



J'ai droit à plus de transparence

Tout citoyen devra bénéficier de plus d'informations sur ce qui est fait sur ses données, notamment sur la finalité des traitements. Il devra donner son consentement explicite, non équivoque et non tacite. (Droit d'accès, droit de rectification, consentement éclairé et positif).

Droit à l'oubli

Tout citoyen peut demander qu'une information soit supprimée si elle porte atteinte à sa vie privée.

508 Millions

C'est le nombre de personnes habitant au sein de l'UE qui verront leurs droits renforcés en 2018. *(Source CNIL)*

« Les entreprises doivent être transparentes sur ce qu'elles font avec les données car la confiance sera au cœur de l'expérience client. Le GDPR peut être perçu comme un label de confiance qui amènera l'utilisateur à communiquer de vraies informations. Ce qui permettra, à terme, aux services connectés de créer des services personnalisés et créer le cercle vertueux de l'innovation. »

Mathieu Domain, Directeur associé chez Ekino (Groupe Havas)

FUITE, VIOLATIONS : LES OBLIGATIONS D'UNE ENTREPRISE

Le responsable de traitement aura **72 heures** pour notifier à l'autorité de contrôle compétente une violation de données à caractère personnel et **tout retard devra être justifié.**

Dans le cas d'un sous-traitant, il doit notifier au responsable de traitement toute violation dont il a connaissance, et ce dans les meilleurs délais.

Lorsque la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour une personne, le responsable de traitement devra l'informer dans les meilleurs délais.

Une violation, c'est quoi ?

La destruction, la perte, l'altération, la divulgation ou l'accès non-autorisé à des données.

« Contrairement aux idées reçues, les collaborateurs constituent la cause majeure de fuite de données. Elle peut être intentionnelle comme le vol de documents d'entreprise ou résulter de négligence. Mais il est essentiel de comprendre que la lutte contre les fuites passe par la mise en place de bonnes pratiques internes et par le choix de solutions de protection pertinentes et de bons outils de chiffrement, de transfert sécurisé… »

Thierry Guenoun, Directeur Europe Moyen Orient et Afrique pour Appdome

NOVENCIA

Tél. : 01.44.63.53.13.
Email : contact@NOVENCIA.com

KEEP IN TOUCH!

www.NOVENCIA.com
https://www.NOVENCIA.com/blog/

NOVENCIA-Groupe

NOVENCIA-Groupe

@NOVENCIA

À propos de NOVENCIA Group

NOVENCIA Group est un cabinet de Conseil IT et Métiers fondé en 2001 par Arnaud Zilliox. Grâce à un niveau d'expertise élevé conjugué à une offre de services très spécialisée, NOVENCIA Group se positionne très vite comme un chasseur d'innovations.
Résultat : aujourd'hui le cabinet de conseil répond à 80% des cas d'usage de ses clients.

Problématiques IT et Métiers, Data & Analytics, IoT, Blockchain, Transformation des organisations, depuis 15 ans NOVENCIA Group accompagne ses clients (Finance, Banque, Assurance, Média & Numérique) vers un nouveau monde : celui du partage des connaissances et de l'agilité.