#GDPR

EN ROUTE VERS LA CONFORMITÉ

Livre blanc

Business & Decision

SOMMAIRE

— *Par Mick Levy*

PRÉFACE

« Si la Data est le nouveau pétrole, la Confiance est la nouvelle monnaie. GDPR crée le cadre pour instaurer cette confiance »

GDPR : UN RÈGLEMENT FONDATEUR POUR L'EXPLOITATION DES DONNÉES

Le règlement 679/2016 appelé GDPR (General Data Protection Regulation) s'applique à toutes les entreprises qui détiennent ou traitent des données personnelles de citoyens européens. GDPR est traduit en Français par Règlement Général sur la Protection des Données (RGPD). Le périmètre des données personnelles concernées est large.

Le règlement définit en 99 articles un ensemble de règles pour respecter et sécuriser les données personnelles. Approuvé par 29 pays européens signataires, il s'étend sur un champ d'application mondial. Toutes les organisations et entreprises qui détiennent ou traitent des données personnelles de citoyens européens doivent donc s'y conformer.

Le règlement entre en application le 25 mai 2018. Les organisations non conformes à cette date s'exposent à des amendes pouvant atteindre 4 % de leur chiffre d'affaires mondial (ou 20 millions d'euros, le maximum des 2 formules étant retenu). On laissait entendre jusqu'alors que la CNIL ne disposait pas de moyen assez dissuasif pour faire respecter les lois, c'est maintenant chose faite !

« Si la Data est le nouveau pétrole, la Confiance est la nouvelle monnaie. GDPR crée le cadre pour instaurer cette confiance ». Tout est dit dans cette phrase. Au gré de l'émergence de dispositifs digitaux de plus en plus gourmands en informations (tracking, applications mobiles, objets connectés, assistants personnels, etc.), les citoyens sont très concernés par les questions liées aux libertés et aux données personnelles. GDPR vient répondre à ces inquiétudes et redonne aux individus le pouvoir sur leurs données personnelles. Sans régulation, le pétrole du XXIème siècle aurait pu se tarir ou pourrir au gré d'utilisations non éthiques et de transferts hasardeux.

Le scandale de la NSA et la multiplication des affaires de pertes ou de vols de données qui ont défrayé la chronique (Yahoo, Dropbox, Sony ou la Mutuelle Générale de la Police par exemple) ont largement contribué à cette prise de conscience. En réaction, l'Europe se dote d'un outil complet et unique au monde. Par cet outil, la première puissance économique mondiale vient aussi réaffirmer sa souveraineté et imposer ses règles qui sonnent comme un avertissement lancé notamment aux GAFA (Google, Amazon, Facebook, Apple) : « Si vous souhaitez exploiter les données de nos citoyens, conformez-vous à nos règles ! ». →

GDPR en 4 chiffres

99
articles composent le règlement

29
pays signataires pour un champ d'application mondial

2
ans pour se conformer : entrée en application en mai 2018

4%
du CA global ou 20 M€ d'amende possible

GDPR : OBLIGATIONS MAIS AUSSI (ET SURTOUT) OPPORTUNITÉS

GDPR remet clairement les pendules à l'heure en édifiant un principe fort de responsabilité des organisations (au sens juridique du terme) quant aux risques soulevés par l'exploitation des données personnelles. Cette responsabilité repose sur de nombreuses exigences dont celles liées à la maîtrise des usages que font les organisations des données personnelles et celles liées à la mise en sécurité de ces informations. De plus, avec le principe d'*accountability*, les organisations doivent être capables de faire la preuve des mesures prises et de la traçabilité des informations.

La mise en conformité à GDPR demande un travail important pour les entreprises et organisations publiques. Ces travaux vont avoir une grande vertu : celle de forcer les organisations à se pencher sur les usages et la gouvernance des données. Une fois la mise en conformité réalisée, tout sera alors en place pour mieux exploiter les données dans des projets à très forte valeur ajoutée. La qualité des informations sera améliorée, le flux des données maîtrisé et la connaissance sur cette formidable matière première largement étendue. S'ouvre ainsi une ère de développement de nouveaux usages, de nouveaux modèles business et de nouveaux services à fort retour sur investissement fondés sur les données.

Vous l'aurez compris, GDPR est un sujet majeur pour les citoyens et les organisations. Sa complexité implique de l'apprécier sous de multiples angles : juridique, IT, usages, changement… C'est pourquoi nous sommes heureux que des auteurs aux sensibilités différentes aient contribué à ce livre blanc.

Bonne lecture !

Mick Levy
@mick_levy
Directeur de l'Innovation Business, Business & Decision

Data Maniac !
15 ans d'expérience dans la valorisation du capital des données de l'entreprise au sein de Business & Decision. Acteur engagé, Mick conseille de nombreuses organisations sur leur stratégie Data et sur l'adoption des nouveaux usages digitaux.

GDPR EN UN COUP D'ŒIL!

C'est le réglement européen relatif à la protection des données Personnelles

Il entre en application En **MAI 2018**

Pour **NOUS CITOYENS** C'est une très bonne Nouvelle

Car le réglement protège les données des citoyens européens **PARTOUT DANS LE MONDE**

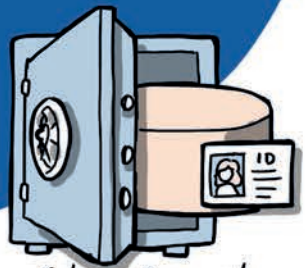
Mais pour **NOS ORGANISATIONS** C'est plus compliqué.

Pour ne pas en faire TROP ni TROP PEU

SE FAIRE ACCOMPAGNER PAR DES EXPERTS

IL N'EXISTE QU'UNE SEULE SOLUTION POUR SE PRÉMUNIR DU RISQUE: ETRE EN CONFORMITÉ!

Or les infractions peuvent coûter **TRES CHER**



Car le réglement encadre **TOUS** les Traitements de Données Personnelles

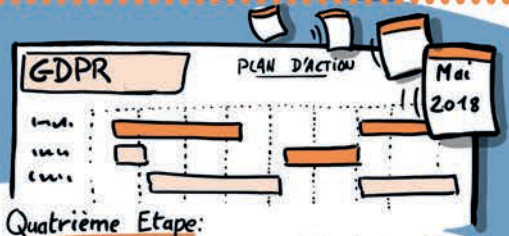
INITIER UN PROJET TRANSVERSE

Première étape: DESIGNER UN CDO

Deuxième Etape: CARTOGRAPHIER LES DONNÉES PERSONNELLES ET LEURS TRAITEMENTS

Troisième Etape:

INVENTORIER LES NON CONFORMITÉS ET EVALUER LES RISQUES



Quatrième Etape: PLANIFIER LES ACTIONS DE MISE EN CONFORMITÉ

4 PANS DE TRAVAUX

Juridique

Conduite du Changement

Gouvernance de la donnée

Sécurité

@Marc_Dugue Pour @BD_Group, le 26/05/2017

De nouveaux droits en matière de données personnelles

— *Par Clarence Tchoussi-Masso*

GDPR renforce et précise les droits des personnes physiques dont les données personnelles sont exploitées, ainsi que les obligations des entités qui assurent le traitement de ces données.

LES NOUVELLES EXIGENCES EN MATIÈRE DE CONSENTEMENT

Lorsque le traitement des données est fondé sur le consentement de la personne concernée, la demande de consentement doit être formulée en des termes clairs et simples, en particulier lorsqu'elle est adressée à un mineur. Le consentement quant à lui doit résulter d'un acte positif. Le silence, l'inactivité ou une case cochée par défaut ne peuvent donc pas être considérés comme un accord. De plus, le consentement peut être retiré à tout moment.

LE RENFORCEMENT DES DROITS DES PERSONNES DONT LES DONNÉES SONT COLLECTÉES

Le Règlement précise les droits existants, et en crée de nouveaux. Ainsi la personne dont les données sont traitées dispose des droits suivants :

Information (Art 13 et 14) : lorsque les données sont collectées auprès d'une personne ou d'un tiers, plusieurs informations doivent lui être communiquées. Il s'agit notamment des finalités du traitement ou encore des droits dont elle dispose.

Droit d'accès (Art 15) : elle a le droit d'obtenir la confirmation que les données sont traitées ou non, et si oui, l'accès à ces données ainsi que certaines informations telles que celles susmentionnées.

Droit de rectification (Art 16) : elle a le droit d'obtenir, dans les meilleurs délais, que les données inexactes soient rectifiées, et que les données incomplètes soient complétées.

Droit à l'effacement (Art 17) : elle a le droit d'obtenir, dans les meilleurs délais, l'effacement de ses données, lorsqu'elle a retiré son consentement au traitement, lorsqu'elle s'y oppose, lorsque les données ne sont plus nécessaires au regard des finalités du traitement, lorsqu'elles ont fait l'objet d'un traitement illicite, ou lorsqu'elles doivent être effacées en vertu d'une obligation légale, sauf dans certains cas. Si le responsable du traitement a rendu publiques les données, il devra informer les autres responsables du traitement qui les traitent de les effacer ainsi que toutes reproductions de celles-ci. →

Droit à la limitation du traitement (Art 18) : elle a le droit d'obtenir la limitation du traitement lorsqu'elle s'y est opposée, lorsqu'elle conteste l'exactitude des données, lorsque leur traitement est illicite, ou lorsqu'elle en a besoin pour la constatation, l'exercice ou la défense de ses droits en justice.

Droit à la portabilité (Art 20) : lorsque le traitement est fondé sur le consentement ou sur un contrat, et effectué à l'aide de procédés automatisés, la personne concernée a le droit de recevoir les données dans un format structuré, couramment utilisé, lisible par machine et interopérable, et de les transmettre à un autre responsable du traitement sans que le responsable du traitement initial y fasse obstacle.

Droit d'opposition (Art 21) : la personne concernée a le droit de s'opposer à tout moment au traitement des données, lorsque celui-ci est nécessaire à l'exécution d'une mission d'intérêt public ou aux fins des intérêts légitimes du responsable du traitement. Elle peut également s'opposer au traitement fait à des fins marchandes.

Prise de décision automatisée (Art 22) : la personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant, sauf lorsque cette décision est nécessaire à la conclusion ou à l'exécution d'un contrat, est autorisée légalement, ou est fondée sur son consentement.

À l'ère où il est possible de communiquer ses données personnelles en un clic, GDPR octroie une multitude de droits permettant d'avoir un certain contrôle sur l'usage qui est fait des données. Ce contrôle ne peut cependant pas s'établir sans la mise en place d'obligations pour les responsables du traitement des données et les sous-traitants ●

Clarence Tchoussi-Masso
@BD_Group
Juriste, Business & Decision

Titulaire d'un Master 2 en droit des affaires et fiscalité obtenu à l'université Paris I Panthéon Sorbonne, Clarence travaille sur les problématiques de protection des données personnelles et de contrat.

Quelles obligations pour les responsables du traitement des données ?

— *Par Clarence Tchoussi-Masso*

Outre l'approfondissement des droits des personnes dont les données à caractère personnel sont traitées, GDPR pose un large éventail d'obligations, à charge des entités traitant les données de les respecter.

LES OBLIGATIONS DES RESPONSABLES DU TRAITEMENT ET DES SOUS-TRAITANTS

Les obligations de GDPR sont pour certaines à la charge du responsable du traitement seul, et pour d'autres, partagées entre ce dernier et le sous-traitant.

Il s'agit tout d'abord d'obligations générales :

Le responsable du traitement doit être en mesure de démontrer que les traitements qu'il opère ou fait opérer le sont dans le respect du Règlement (c'est le principe d'*Accountability*). Pour ce faire, il peut notamment faire appliquer un code de conduite ou des mécanismes de certification (Art 24).

Le responsable du traitement est également tenu de mettre en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement, des mesures permettant le respect du Règlement (privacy by design), ainsi que d'adopter des mesures permettant de garantir, par défaut, que le traitement soit limité à ce qui est nécessaire (privacy by default) (Art 25).

Lorsqu'il est établi en dehors de l'UE, le responsable du traitement ou le sous-traitant doit désigner un représentant établi au sein de l'UE (Art 27).

Le sous-traitant doit présenter des garanties suffisantes quant à la conformité au Règlement. Il ne peut recruter un autre sous-traitant sans l'autorisation du responsable de traitement, et il veille au respect de la confidentialité des données. En outre, sauf exception, le sous-traitant ainsi que toute personne sous son autorité, ou sous l'autorité du responsable du traitement, ne peut traiter les données sans autorisation de ce dernier (Art 28).

Le responsable du traitement et le sous-traitant doivent tenir un registre détaillé des opérations de traitement, registre qui peut être mis à disposition de l'autorité de contrôle à tout moment, et coopérer avec celle-ci (Art 29 et 30).

Le Règlement fixe ensuite des obligations spécifiques :

Le responsable du traitement est tenu de mettre en œuvre des mesures techniques et organisationnelles permettant de garantir la sécurité du traitement, telles que la pseudonymisation et le chiffrement des données (Art 32).

Le responsable du traitement doit notifier à l'autorité de contrôle compétente de toute violation susceptible d'engendrer des risques pour les droits et libertés des personnes, et ce, dans les →

« Le responsable du traitement est tenu de mettre en œuvre des mesures techniques et organisationnelles permettant de garantir la sécurité du traitement »

meilleurs délais. Il doit également notifier les personnes concernées, à moins qu'il n'ait mis en œuvre des mesures. Le sous-traitant quant à lui doit notifier toute violation des données au responsable du traitement, dans les meilleurs délais (Art 33 et 34).

Lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés, le responsable du traitement effectue une analyse de l'impact des opérations de traitement envisagées sur la protection des données. Cette analyse est requise en particulier en cas de traitement automatisé (y compris profilage) ou de traitement de données visées aux articles 9 et 10 (Art 35).

Le responsable du traitement et le sous-traitant doivent nommer un délégué à la protection des données (Data Protection Officer/DPO), dont le rôle est de mettre en œuvre la conformité au Règlement. Le rôle et les missions du DPO seront détaillés dans le prochain chapitre.

Des codes de conduite et des mécanismes de certification peuvent être mis en place afin de contribuer à la bonne application du Règlement (Art 40 à 43).

Le responsable du traitement ou le sous-traitant ne peut transférer des données vers des pays tiers ou à des organisations internationales qu'en présence d'une décision de la Commission (décision d'adéquation), ou s'il a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives. En dehors de ces cas, sauf exceptions prévues par le Règlement (à l'article 49), le transfert n'est possible que si ce transfert ne revêt pas de caractère répétitif, ne touche qu'un nombre limité de personnes concernées, est nécessaire aux fins des intérêts légitimes, et si le responsable du traitement a évalué toutes les circonstances entourant le transfert et a offert, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données (Art 45 à 50).

SANCTION DU NON-RESPECT DES OBLIGATIONS POSÉES PAR LE RÈGLEMENT

L'une des nouveautés majeures du Règlement est la mise en place d'une sanction financière, sous forme d'une amende. Cette amende peut s'élever à 20 M€ ou, dans le cas d'une entreprise, à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu (Art 83) ●

Comprendre le rôle stratégique du DPO

— *Par Cécile Théard-Jallu*

La nomination d'un délégué à la protection des données personnelles (DPO pour « Data Protection Officer »), dont le régime est explicité par les articles 37 à 39 du Règlement, est au cœur de la réforme. Son importance s'illustre par l'adoption, dès le 13 décembre 2016 par le G29 en séance plénière, de lignes directrices dédiées. Elles font partie des trois premiers guides adoptés par le G29 et constituent le document le plus fouillé et volumineux des trois.

UN DPO, POUR QUI ?

Sans préjudice d'autres cas qui seraient prévus par les Etats Membres, les responsables de traitement et les sous-traitants devront obligatoirement désigner un DPO lorsque :

- le traitement est effectué par une autorité ou un organisme public (à l'exception des juridictions dans leur rôle juridictionnel) ; le règlement ne définissant pas « autorité ou un organisme public », la notion est déterminée en vertu du droit national de chaque État membre ;
- leurs activités de base les conduit (du fait de la nature, portée et/ou finalité de ces activités) à effectuer un suivi régulier et systématique des personnes à grande échelle ;
- leurs activités de base les amène à traiter à grande échelle des données sensibles ou qui ont trait à des condamnations et infractions pénales ; pour mémoire, sont considérées comme des données sensibles, notamment, les données génétiques, biométriques, ou afférentes à la santé, à la religion, aux opinions politiques ou à l'appartenance syndicale.

Si le responsable de traitement remplit les critères de désignation obligatoire, son sous-traitant n'est pas nécessairement tenu lui-même de nommer un DPO, et inversement.

QUE SIGNIFIE « SUIVI RÉGULIER ET SYSTÉMATIQUE DES PERSONNES À GRANDE ÉCHELLE » ET « ACTIVITÉ DE BASE » ?

Le G29 recommande notamment de prendre en considération les facteurs suivants pour déterminer si le traitement est effectué « à grande échelle » :

- le nombre de personnes concernées ;
- le volume de données et/ou le spectre des catégories de données ;
- la durée ou la permanence de l'activité de traitement ;
- l'étendue géographique de l'activité de traitement.

Le G29 estime, à titre d'exemples, que sont concernés par la nomination d'un DPO les traitements de données (trafic, contenu, localisation) par téléphone, par un fournisseur de services internet ou encore ceux réalisés à titre habituel par une banque ou une société d'assurance. En revanche, ne constitue pas un traitement à grande échelle, le traitement des données d'un patient par un médecin particulier ou relatif aux condamnations et infractions pénales par un avocat.

L' « activité de base » d'une entreprise est considérée par le G29 comme l'activité clé lui permettant de →

réaliser ses objectifs ou qui est inextricablement liée au traitement (à titre d'exemple, un hôpital qui traite les données de ses patients, est donc tenu de nommer un DPO ; en revanche, la gestion de la paie ou le service informatique d'une entreprise sont considérés comme des activités marginales).

À la lecture de GDPR, il existait des doutes quant à la portée des hypothèses de désignation reposant sur des notions à interprétation variable comme celui d'« activité de base » d'un responsable ou de traitement « à grande échelle » des données. La réponse du G29 tend vers une large interprétation de ces notions et étend autant que possible les hypothèses de désignation à retenir.

EST-IL POSSIBLE DE DÉSIGNER UN DPO EN DEHORS DES CAS OBLIGATOIRES ?

Oui, il est possible de le faire volontairement même lorsque les critères susvisés ne sont pas remplis. Le G29 encourage d'ailleurs cette désignation volontaire. Celle-ci emporte la soumission du DPO aux dispositions réglementaires le concernant, au même titre que les DPO ayant été désignés de façon obligatoire.

Les organismes non soumis à l'obligation de désignation d'un DPO et ne souhaitant pas en nommer un, peuvent employer du personnel ou des consultants extérieurs chargés de la protection des données à caractère personnel. Dans cette hypothèse, il est important de veiller à ce qu'il n'y ait aucune confusion quant à leurs titre et tâches. En tout état de cause, le responsable de traitement conservera les obligations lui incombant.

QUELLES SONT LES MISSIONS DU DPO ?

Le DPO apparaît comme un réel « chef d'orchestre » principalement chargé d'informer et de conseiller le responsable de traitement ou le sous-traitant, mais aussi les employés.

Concrètement, il lui appartient de s'informer sur les nouvelles obligations, d'assister les décideurs sur les conséquences des traitements, d'en réaliser l'inventaire, de concevoir des actions de sensibilisation et de piloter en continu la conformité. Il doit être impliqué correctement et en temps utile dans toutes les problématiques liées à la protection des données à caractère personnel. A ce titre, les ressources et le temps nécessaires à l'accomplissement de ses missions et à l'entretien de ses connaissances spécialisées doivent impérativement lui être donnés.

Bien qu'il soit autorisé à exercer d'autres fonctions, le DPO doit être indépendant et ne pas être placé en situation de conflit d'intérêts. Il est soumis à une obligation de confidentialité.

Le G29 recommande que le responsable de traitement demande l'avis du DPO, entre autres, sur la nécessité d'effectuer une analyse d'impact sur la protection des données (PIA), la méthodologie à suivre →

« Le DPO apparaît comme un chef d'orchestre principalement chargé d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que les employés »

et les garanties à appliquer pour atténuer les risques d'atteinte aux droits de la personne concernée.

Attention, le DPO n'est pas responsable de la conformité au GDPR à la place du responsable de traitement ou du sous-traitant et si l'avis du DPO n'est pas suivi par le responsable de traitement ou le sous-traitant, le G29 insiste sur l'importance pour ce dernier de documenter le processus ayant conduit à une telle décision.

En somme, le DPO représente un élément de coordination à la fois en interne et en externe, agissant comme le point de contact de l'autorité de contrôle et des personnes concernées, avec qui il doit coopérer. Il occupe ainsi un poste stratégique qui va au-delà de celui du CIL.

COMMENT CHOISIR UN DPO ?

Le choix du DPO doit suivre un certain nombre de critères de compétences et d'éthique. Ainsi, son niveau d'expertise tant technique que réglementaire doit permettre de répondre à la nature, à la complexité du traitement et au niveau de protection exigé pour les données, notamment en cas de données sensibles ou de transfert hors UE. Evidemment, une connaissance approfondie du RGPD et de la réglementation et des pratiques de data privacy nationales et européennes est requise.

Le fonctionnement de l'entreprise (notamment au niveau IT) est également intrinsèque à la fonction.

L'intégrité et l'éthique professionnelle du DPO sont elles-mêmes primordiales et conditionnent la promotion, à assurer par le DPO, d'une culture de protection des données personnelles au sein de la structure. Le DPO peut être un membre du personnel ou un prestataire externe.

UN GROUPE D'ENTREPRISES PEUT-IL NOMMER UN DPO COMMUN ?

Oui, à la condition que le DPO soit facilement accessible par chacun des établissements. Il appartient au responsable de traitement de s'assurer qu'un DPO unique sera en capacité d'exécuter efficacement chaque tâche lui incombant.

La protection des données étant un sujet transverse, elle n'implique pas seulement le DPO mais tous les métiers de l'entreprise, y compris la direction, les services RH et les équipes IT. L'organisation des processus implique la sensibilisation et la remontée d'informations. Ainsi, l'humain représente le maillon fort permettant de garantir le respect de GDPR dans la structure, tant au niveau technique qu'organisationnel ●

Cécile Théard-Jallu
@CecileJallu
Avocate Associée,
De Gaulle Fleurance & Associés

Cécile Théard-Jallu intervient principalement sur des opérations contractuelles complexes, notamment en R&D, transfert de technologies, licensing, IT, commercial et projets de mutation technologique. Elle accompagne les entreprises dans leur transformation digitale, y compris dans le traitement des données, en France et à l'international.

Le droit à la portabilité des données : ce que prévoit GDPR

Par Clarence Tchoussi-Masso

La nomination d'un DPO n'est pas le seul élément essentiel du nouveau règlement. Dans la quête de son objectif de renforcement du contrôle que les individus ont sur leurs données, GDPR a également mis en place le droit à la portabilité des données. De quoi s'agit-il exactement ?

Le droit à la portabilité des données correspond au droit qu'ont les personnes à « recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine » et de « transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle ».

Inscrit à l'article 20 du GDPR, le droit à la portabilité doit faciliter le passage d'un prestataire de service à un autre et ainsi renforcer la concurrence entre les prestataires.

Le G29 a élaboré des lignes directrices sur le droit à la portabilité des données, qui définissent les conditions et modalités d'exercice de ce droit.

DANS QUELS CAS LES INDIVIDUS PEUVENT-ILS EXERCER LEUR DROIT À LA PORTABILITÉ DES DONNÉES ?

L'exercice du droit à la portabilité des données n'est possible que dans certains cas.

La personne concernée peut opérer la portabilité de ses données lorsque les 2 conditions cumulatives suivantes sont remplies :

- le traitement est fondé sur le consentement de la personne concernée ou sur un contrat auquel elle est partie. Le G29 prend à titre d'exemple de données susceptibles de faire l'objet d'une portabilité, les titres de livres que la personne concernée a achetés sur une librairie en ligne, ou des chansons qu'elle a écoutées via un service de streaming, du fait de l'existence d'un contrat entre elle et le prestataire ;
- le traitement est effectué à l'aide de procédés automatisés. Il n'y a donc pas de droit à la portabilité lorsque le traitement est manuel.

LES DONNÉES CONCERNÉES

Le droit à la portabilité ne peut s'exercer que sur les données relatives à la personne concernée qu'elle a elle-même fournies.

Données relatives à la personne concernée

Les données doivent concerner la personne qui en demande la portabilité. Cette exigence soulève la question du transfert de données lorsque celles-ci comprennent des données relatives à des tiers. C'est par exemple le cas lorsque l'utilisateur d'un service de messagerie demande la portabilité de ses conversations avec ses contacts. Dans un tel cas, bien que la demande porte sur des →

données concernant également des tiers, le responsable du traitement doit y répondre.

Si ces données sont par la suite transmises à un autre responsable du traitement, celui-ci ne pourra les traiter d'une manière susceptible de porter atteinte aux droits et libertés de ces personnes tierces. Cela pourrait être le cas si celles-ci ne sont pas informées et ne peuvent pas exercer leurs droits (droit de rectification, etc.).

Le traitement qui sera effectué par le nouveau responsable du traitement devra avoir un fondement autre que le consentement de la personne concernée ou l'existence d'un contrat auquel elle est partie prenante. L'article 6 du GDPR énonce les fondements possibles d'un traitement (consentement, existence d'un contrat, intérêts légitimes, etc.). Le traitement devra donc être fondé sur l'un des autres cas possibles, tel que les intérêts légitimes poursuivis par le responsable du traitement. En reprenant l'exemple du service de messagerie, il n'y aura donc pas atteinte aux droits et libertés des tiers si les données sont utilisées par le nouveau responsable du traitement pour la même finalité. En revanche, il y aura atteinte si les données sont par exemple utilisées à des fins de marketing.

Afin de limiter les risques d'atteinte aux droits et libertés des tiers, les responsables du traitement pourraient alors mettre en place des outils permettant aux personnes concernées de sélectionner uniquement les données pertinentes et d'exclure les données de tiers, ou encore des outils permettant de recueillir le consentement des tiers.

Données qu'elle a elle-même fournies

Le droit à la portabilité vise donc les informations que la personne concernée a volontairement et directement communiquées au responsable du traitement, telles que son nom, son adresse de messagerie, son adresse postale, son âge, etc. Il vise également les données indirectement fournies par elle, c'est-à-dire découlant de son activité, telles que la liste des musiques qu'elle a écoutées ou encore la liste des vêtements qu'elle a pu consulter sur un site d'achat. Sont exclues les données que le responsable du traitement a déduit ou dérivé des données fournies par l'utilisateur, en ce qu'elles sont générées par le responsable du traitement lui-même.

QU'EST-CE QUE L'EXERCICE DE CE DROIT IMPLIQUE POUR LES RESPONSABLES DU TRAITEMENT ?

L'exercice de ce droit pose diverses obligations à la charge des responsables du traitement.

1. Une obligation d'information

Dès le moment où les données sont collectées, le responsable du traitement doit informer la personne concernée de l'existence de ce droit. Il doit le distinguer des autres droits, notamment en précisant les données susceptibles de faire l'objet d'une portabilité. Le G29 recommande en outre de signaler aux personnes concernées l'existence de ce droit, en cas de fermeture de leurs comptes, afin de faciliter le stockage et le transfert des données par la personne concernée avant qu'elle ne mette fin au contrat la liant au responsable du traitement.

2. La pertinence des données reçues

Le nouveau responsable du traitement doit s'assurer que les données →

reçues ne vont pas au-delà de ce qui est nécessaire au regard de la finalité du traitement.

3. Les modalités de réponse à la demande de portabilité des données

Selon l'article 12 du GDPR, le responsable du traitement doit répondre à la demande de portabilité dans les meilleurs délais, et en tout état de cause dans un délai d'un mois, délai qui peut être prolongé au besoin à deux mois. S'il ne donne pas suite à la demande, il doit informer la personne concernée des motifs de son inaction dans un délai d'un mois à compter de la réception de la demande.

S'agissant du coût de l'exercice du droit à la portabilité, le responsable du traitement ne peut exiger des frais, sauf lorsque les demandes d'une personne sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif.

4. Les modalités de transmission des données

Selon le G29, les responsables du traitement devraient mettre à disposition des personnes concernées divers outils leur permettant d'exercer leur droit à la portabilité. Ils pourraient par exemple leur permettre de télécharger leurs données, mais également de les transmettre eux-mêmes à d'autres responsables du traitement, par le biais d'une API (Application Programming Interface). Les personnes concernées pourraient également disposer d'espaces de stockages des données, auxquels ils autoriseraient l'accès aux responsables du traitement afin que ceux-ci puissent procéder au traitement et transmettre les données aisément.

S'agissant du format dans lequel les données doivent être transmises, selon l'article 20 du Règlement, les données doivent être fournies « dans un format structuré, couramment utilisé et lisible par machine». Cette formule signifie que les données doivent être transmises sous un format interopérable (définition à l'article 2 de la Décision n° 922/2009/CE du Parlement européen et du Conseil du 16 septembre 2009).

L'existence de ce droit implique donc pour les responsables du traitement de permettre l'interopérabilité. En revanche, il ne leur impose pas d'adopter ou de maintenir des systèmes de traitement qui sont techniquement compatibles.

Les données doivent être fournies dans un format ayant un haut niveau d'abstraction. En outre les métadonnées doivent être les plus précises possibles. La transmission de données relatives à des e-mails par exemple, doit être faite dans un format préservant toutes les métadonnées et permettant une réutilisation effective des données. Ainsi, lorsque le responsable du traitement choisit le format de transmission, il doit prendre en compte l'impact que ce format pourrait avoir sur le droit de la personne concernée de réutiliser les données, ou le fait que ce format puisse entraver l'exercice de ce droit.

5. L'exercice du droit à la portabilité sans préjudice des autres droits de la personne concernée

Par ailleurs, l'exercice du droit à la portabilité des données ne doit pas faire obstacle à l'exercice, par la personne concernée, de ses autres droits. En effet il n'implique pas pour le responsable du traitement la suppression automatique des données une fois qu'il les a transmises à la personne concernée.

Celle-ci pourra donc continuer de bénéficier des services du responsable du traitement, et pourra exercer n'importe quel autre droit, aussi longtemps qu'il procèdera au traitement de ses données. Pour autant, le responsable du traitement n'a pas à conserver les données plus longtemps que nécessaire ou plus longtemps que prévu, dans l'optique de permettre à la personne concernée d'en exercer la portabilité.

6. La sécurité des données

Le responsable du traitement doit prendre les mesures propres à assurer la sécurité des données lors du transfert, telles que le cryptage, et doit s'assurer de transmettre les données à la bonne personne. L'adoption de telles mesures ne doit toutefois pas empêcher la personne concernée de faire usage de son droit, notamment du fait que des coûts additionnels aient été imposés.

Le responsable du traitement pourrait également aiguiller la personne concernée vers des méthodes sécurisées de stockage des données.

Il convient de préciser que le responsable du traitement n'est pas responsable de l'usage qui est fait des données par la personne concernée ou par le nouveau responsable du traitement.

La question de la sécurité des données devient un enjeu d'autant plus crucial pour les données issues des objets connectés ●

Les objets connectés et GDPR, comment sécuriser le tout-connecté ?

— *Par Jean-Michel Franco*

GDPR a donc un impact considérable sur les entreprises dans toute l'Europe. Cependant, la protection des données est un défi qui concerne aussi les données collectées par les objets connectés. Les entreprises vont devoir mieux maîtriser leur processus de collecte, d'intégration, de certification, de publication, de supervision et, bien entendu, de protection de toutes leurs données relatives aux personnes, qu'il s'agisse de leurs employés, clients et autres tiers.

DE NOUVELLES PRATIQUES POUR LA GESTION ET LE PARTAGE DE DONNÉES

Face à la multiplication des fuites majeures de données, les entreprises se sont jusqu'ici focalisées sur la sécurité des data. Elles sont en revanche généralement bien moins organisées vis-à-vis des pratiques imposées par la nouvelle réglementation en termes de gestion et de partage des données personnelles. Or, ceci représente un risque sérieux pour deux grandes raisons.

Tout d'abord, le terme « confidentialité des données » est très vaste dans le cadre de GDPR. Les responsabilités des organisations y sont très étendues comme nous avons pu le voir précédemment.

Deuxième élément : l'émergence, voire l'avènement de l'Internet des objets (IoT) donne un poids supplémentaire à ces problématiques. En effet, l'IoT concrétise le concept de client connecté en permanence. Ce modèle est précieux pour les entreprises cherchant à générer et à capturer d'importants volumes de données sur les préférences et les comportements de leurs clients afin de se démarquer de la concurrence.

Cependant, bien que l'essentiel de ces données soient davantage liées aux produits qu'aux individus, le risque sur le plan de la confidentialité subsiste. En effet, à partir du moment où un objet connecté est explicitement associé à celui qui l'utilise, il devient alors porteur de données personnelles. Ainsi les informations fournies par un véhicule connecté, deviennent des données personnelles dès lors que l'on peut l'associer à l'identité de celui qui l'utilise.

DES DONNÉES CONSIDÉRÉES PAR DÉFAUT COMME PERSONNELLES

Les fabricants de dispositifs connectés prennent désormais conscience qu'une fois que leurs produits se →

« Le contrôleur de données dispose d'un mois pour répondre aux demandes d'accès de la part des usagers »

trouvent entre les mains des clients, toutes les données transmises peuvent être potentiellement considérées par défaut comme personnelles. D'où la nécessité pour eux de tenir compte dès le départ des principes de confidentialité. Et ce, dans leurs propres environnements et avec l'ensemble des fournisseurs impliqués dans la collecte, le stockage et le traitement des données.

Le fabricant de produits d'électronique grand public Vizio s'est vu infliger en février 2017 une amende de 2,2 millions de dollars après que l'autorité américaine de protection des consommateurs ait découvert qu'il utilisait des logiciels de reconnaissance de contenu afin d'effectuer un suivi de ses utilisateurs sans leur consentement. Près de 11 millions de téléviseurs connectés à Internet auraient ainsi pu espionner les habitudes de visionnage des consommateurs et relier ces données à des informations sociodémographiques, pour être ensuite partagées avec des sociétés de marketing tierces. L'entreprise a affirmé pour sa défense que ses télévisions « n'associaient jamais des données de visionnage à des informations personnelles comme des noms ou des coordonnées ».

Si l'amende infligée paraît significative, il est important de souligner que si l'entreprise avait vendu ces téléviseurs-là en Europe après la mise en application de GDPR, l'entreprise s'exposerait cette fois à une amende supérieure à 292 millions de dollars !

OÙ SONT MES DONNÉES ?

Autre problématique de poids pour les entreprises : savoir où résident leurs données privées et sensibles, et qui en a la responsabilité. Bon nombre d'entre elles sont incapables de répondre clairement à ces questions, car leurs données sont dispersées dans différents départements (commercial, marketing, financier, service client, etc.). L'incapacité à disposer d'une vue unifiée sur les clients et employés d'une entreprise représente un véritable problème dans le cadre de la conformité à GDPR.

Selon ce nouveau règlement, le contrôleur de données dispose →

d'un mois pour répondre aux demandes d'accès de la part des usagers, même si cette période peut être étendue pour les requêtes particulièrement complexes. Cette politique est donc bien plus stricte que celles des réglementations actuelles. Jusqu'à lors, ce délai était de 60 jours en France. Mais les droits des individus ne seront pas limités à l'accès aux données : GDPR garantit également un droit de rectification, de suppression (droit à l'oubli), de restriction/d'objection au traitement de données, ou de non évaluation dans le cadre de traitements automatisés. Tous ces droits ont un impact considérable sur les pratiques en matière de gestion de données.

ORGANISER LA RIPOSTE

Comment les organisations peuvent-elles faire face aux problématiques énoncées précédemment dans le cadre de la gestion de leurs données ? La première étape serait d'en effectuer un inventaire afin de savoir quels types de données sont en leur possession et où elles résident.

Vient ensuite la question de la qualité, une problématique particulièrement urgente pour les organisations en phase de déploiement de leurs capacités de gestion de l'IoT. En effet, dans ce domaine, la volonté de limiter les coûts pousse souvent les organisations à faire avec des réseaux de qualité médiocre, ce qui peut affecter la qualité et la sécurité des données.

Dans le contexte de GDPR, la faible maîtrise de la qualité et l'harmonisation des données devient une problématique critique, en particulier si cela empêche les organisations de dégager une vision unique de leurs clients, contrairement à ce qu'exige la réglementation.

L'une des principales problématiques en la matière vient de l'existence de silos de données difficiles à intégrer. Prenons le cas où une entreprise disposerait d'informations sur un client à la fois issues de dispositifs IoT, d'applications de gestion telles des ERP ou des applications de gestion de la relation client et d'applications de marketing. En cas de demande, l'entreprise serait alors tenue de lui fournir l'ensemble de ses données privées le concernant (silos inclus), comme l'exige GDPR. Les entreprises devront donc rapprocher l'ensemble de leurs informations, y compris celles provenant des objets connectés.

APPRÉHENDER LES PROBLÉMATIQUES DE L'IOT EN MATIÈRE DE DONNÉES

L'IoT devrait apporter une multitude d'avantages aux organisations du monde entier générant de vastes volumes de données, et s'en servant dans le cadre de leurs processus décisionnels. Grâce à ce système, les entreprises peuvent relier le monde physique et numérique, et ont l'opportunité de définir les expériences clients de demain. Cependant, comme souligné, ces données représentent également des défis, notamment en matière de confidentialité, et donc de conformité avec GDPR ●

Jean-Michel Franco
@jmichel_franco
Directeur du Marketing Produit, Talend

Tout au long de son parcours professionnel, Jean-Michel Franco a eu pour mission de développer l'adoption des innovations technologiques.

5 challenges et conseils pour la conformité

— *Par Mick Levy*

Les entreprises doivent agir vite pour pouvoir s'assurer de leur conformité avec GDPR dès mai 2018. Il leur est donc essentiel de prendre les mesures nécessaires sans plus tarder pour résoudre les différentes problématiques dont nous avons parlé précédemment.

1 CARTOGRAPHIER LES DONNÉES PERSONNELLES DANS LE SI

L'une des premières questions est : « Où y a-t-il des données personnelles dans l'entreprise ? ». Cette question a priori triviale, représente en réalité un véritable casse-tête tant les SI des entreprises sont silotés et les informations éparpillées. Il est nécessaire de débusquer toutes les données personnelles qu'elles soient structurées (comme dans une base de données SQL) ou non (telles que dans des mails ou fichiers bureautiques). De plus, les données sont à rechercher non seulement dans les composantes visibles du système d'information (les SI de gestion, le décisionnel, le big data) mais également là où les utilisateurs naviguent (les postes de travail des collaborateurs).

Les principaux domaines de données personnelles sont généralement ceux des clients/prospects, ceux des ressources humaines mais aussi ceux de tiers (prestataires, partenaires, etc.).

Nous vous conseillons d'outiller cette cartographie : les éditeurs de logiciel ont développé des solutions pour simplifier et pour fiabiliser cette étape préliminaire cruciale.

2 CONDUIRE UN PROJET TRANSVERSE AUX IMPLICATIONS IMPORTANTES

La réglementation, de par ses multiples exigences, nécessite une approche transverse à l'entreprise. Et c'est bien connu, les projets transverses c'est complexe ! L'impulsion pour la mise en conformité est généralement donnée par la Direction Juridique (ou Conformité quand il y en a) et un sponsoring fort et impliqué de la Direction Générale est souhaitable.

Nous vous conseillons de nommer rapidement un DPO. Exigé par le règlement pour toutes les entreprises de plus de 250 salariés, il sera en charge d'animer les chantiers à mener en impliquant la Direction Juridique et la Direction du Système d'Information ainsi que toutes les autres directions impliquées dans le traitement de données personnelles (Marketing, Commerce, Ressources Humaines, etc.). →

3 CHOISIR LES SOLUTIONS POUR LA MISE EN CONFORMITÉ

Si le « pourquoi » et le « quoi » de la règlementation sont bien définis, le « comment » est encore assez flou sur certains aspects du règlement. De plus, il n'y a pas de solution unique et les chemins possibles pour répondre aux exigences sont nombreux.

Le G29 a publié le 13 Décembre 2016 trois dossiers d'opinion « guidelines » pour GDPR (Portabilité des données, Data Protection Officer, Autorités de surveillance). D'autres dossiers sont à venir.

Pour choisir sans se tromper, nous vous conseillons de réaliser un assessment. Cela vous permettra de faire un point complet sur votre situation, d'évaluer les risques et de prioriser les chantiers et solutions.

4 RÉUNIR LES COMPÉTENCES POUR INTÉGRER LES SOLUTIONS DE MISE EN CONFORMITÉ

Mener le projet de mise en conformité à GDPR nécessite de déployer de nombreuses compétences dans l'entreprise. Les directions juridiques (qui donnent l'impulsion pour ce projet) ne sont généralement pas familières de la conduite de projets transverses dans l'entreprise et bien souvent mal informées des problématiques relatives à la protection des données personnelles.

Les compétences à avoir pour déployer les solutions pour GDPR concernent principalement 2 domaines :

- Sécurité : Identity and Access Management (IAM), Cryptage, anti-hacking, etc.
- Data Management : Anonymisation, Minimisation, Traçabilité, Gouvernance, etc.

Le point central de GDPR est donc la Data, matière sur laquelle bon nombre d'entreprises n'ont pas encore défini de stratégie ou de gouvernance et sur laquelle beaucoup de DSI manquent de compétences et d'expertise.

Sur ce point, nous vous conseillons de mobiliser une équipe à la DSI pour travailler sur ces enjeux. Business & Decision organise des séminaires d'évangélisation au sein de missions « GDPR Starter » pour mettre le pied à l'étrier et mobiliser les bonnes personnes de l'entreprise.

5 CHANGER LES COMPORTEMENTS DANS L'ENTREPRISE

Ce dernier challenge est certainement le plus complexe car il touche aux comportements de tous les collaborateurs en contact avec des données personnelles. 69 % des fuites de données sont dues à des collaborateurs dûment habilités à accéder à ces données, généralement suite à une négligence (source Ponemon Institute - True Cost of Compliance Study 2013). Ce chiffre montre à lui seul le chemin à parcourir en termes de changement.

De plus, dans les équipes projet, les méthodes de pilotage et la conception doivent évoluer pour tenir compte des principes de « privacy by design » et « privacy by default ».

Nous vous conseillons de traiter la conduite du changement au sein d'un chantier dédié. Ce chantier est à lancer au plus tôt en démarrant par des actions d'évangélisation et de communication ●

GDPR SUR LA ROUTE DE LA CONFORMITÉ

À partir de tous les éléments présentés dans ce livre blanc, la question centrale est d'organiser le projet de mise en conformité et d'adopter le bon rythme pour la mener à terme.

40%

des entreprises ne seront pas totalement conformes en 2020 (soit 2 ans après la date limite).

2023

date à laquelle toutes les entreprises seront conformes (soit 5 ans après la date limite)

Source : Gartner, *EU Privacy Will Impact Delivery of Your DataSecurity Product Marketing Messages*, 10 mars 2017

Ces chiffres de Gartner montrent qu'il sera difficile pour bon nombre d'organisations d'être en conformité totale à GDPR le 25 mai 2018. Et la CNIL en a probablement conscience.

Dans ce contexte, les travaux doivent être priorisés pour :

1. se mettre en mode projet et initier les travaux ;

2. établir une feuille de route de mise en conformité réaliste et volontaire ;

3. conduire rapidement les actions prioritaires (celles qui sont les plus simples à mener et qui vont permettre de réduire le risque sur les points de non-conformité les plus significatifs).

Une sanction de la CNIL n'est pas à redouter en mai 2018 pour une organisation qui serait sur le chemin de la conformité même si tout n'était pas encore accompli. En revanche, il est probable qu'une organisation qui n'aurait encore lancé aucun chantier et qui serait non conforme sur plusieurs points réglementaires puisse être sévèrement sanctionnée.

Les chantiers qui s'ouvrent à nous pour GDPR sont significatifs et dans certains cas de grande ampleur. →

Pour vous assister dans ces travaux, Business & Decision a mis au point une roadmap.

GDPR Starter

Organiser le projet,
Impliquer les collaborateurs

GDPR Assessment

Cartographier les données,
Évaluer les risques,
Établir la roadmap.

GDPR Compliance

Faire évoluer le
système d'information,
Mettre en œuvre la sécurité
et la gouvernance des données,
Conduire le changement
dans l'entreprise.

Les premières opérations d'évaluations (Assessment) sont déterminantes pour la mise en conformité. Elles permettent de mobiliser et d'organiser le projet, d'obtenir une cartographie des données et des traitements ainsi qu'une évaluation du risque associé. Surtout, elles permettent de bénéficier de préconisations et de mettre sur pied une feuille de route réaliste, adaptée au contexte particulier de chaque organisation. Pour ce faire, Business & Decision a développé une méthodologie et des outils dédiés à ces assessments pour GDPR.

Aprés cette phase d'évaluation et de planification, vient le temps des travaux de réalisation et d'intégration dans votre système d'information. Business & Decision peut vous assister sur la totalité de ces travaux de mise en conformité au travers d'expertises dédiées à la Data et la Gouvernance, à la Sécurité des Données et à la Conduite du Changement. Ces compétences au cœur du métier du Groupe, sont complétées par celles de nos partenaires technologiques pour la fourniture des solutions et celles de nos partenaires avocats pour les travaux juridiques ●

Contactez-nous pour être en conformité
contact@businessdecision.com

CONTACTEZ-NOUS POUR ÊTRE EN CONFORMITÉ

contact@businessdecision.com

Business & Decision