



ARTICLE



M-5 : ACCOUNTABILITY » & GOUVERNANCE DES DONNÉES : COMMENT SE PRÉPARER ?

IT et données personnelles Droit de la concurrence, consommation et distribution Contrats commerciaux et internationaux | 15/12/17 | Florence Chafiol Stéphanie Lapeyre

TECH & DIGITAL PROTECTION DES DONNÉES PERSONNELLES

L'« *accountability* » (notamment mentionnée aux articles 5 et 22 du RGPD) désigne l'obligation pour tout responsable de traitement de mettre en œuvre des mesures techniques et organisationnelles appropriées pour s'assurer que les traitements de données à caractère personnel sont effectués conformément au RGPD et être en mesure de le démontrer. Le responsable de traitement concerné doit donc non seulement (i) prendre des mesures efficaces et appropriées afin de se **conformer au RGPD** mais également (ii) identifier et documenter les mesures mises en œuvre afin de pouvoir – si l'on traduit littéralement la formule - « **rendre des comptes** » aux autorités et leur permettre ainsi de vérifier l'efficacité des mesures prises et l'effectivité de la protection des données.

On abandonne ainsi désormais la logique de « formalités préalables » et d'autorisations effectuées auprès de la CNIL en amont de la mise en œuvre d'un traitement au profit d'une logique de responsabilisation et de traçabilité afin de permettre un contrôle en aval par les autorités compétentes. Si les grands principes de la loi Informatique et Liberté demeurent (et sont même renforcés), cette logique d'*accountability* doit se traduire par un changement de culture interne qui nécessite de mobiliser toutes les compétences de l'entreprise (DSI, prestataires, services juridiques, directions métier) afin de permettre une gouvernance efficace des données.

1. Comment se montrer responsable ?

Afin de garantir un haut niveau de protection des données personnelles en permanence, les responsables de traitement doivent organiser les procédures internes qui garantissent la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement, dont notamment les procédures suivantes :



| Principe | Description de l'obligation/du processus | Exemples de mesures à mettre en œuvre |
|---|--|---|
| <p>Prendre en compte la protection des données personnelles dès la conception d'un projet et par défaut (Article 25 RGPD)</p> | <p>Le « Privacy by design » impose au responsable de traitement de prendre en compte la protection des données personnelles dès la conception d'un projet et tout au long de son cycle de vie. L'objectif est d'anticiper et de lister les obligations juridiques pesant sur tout nouveau projet impliquant le traitement de données personnelles (lancement d'une application, élaboration d'un logiciel, proposition d'un nouveau service ou produit, etc.) puis de développer les outils et procédures adaptées pour que ces obligations soient respectées de manière effective lors de la mise en œuvre du projet et surtout au long de son exécution.</p> <p>Le « Privacy by default » consiste à prendre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données qui sont nécessaires au regard de la finalité spécifique du traitement sont collectées et utilisées.</p> | <ul style="list-style-type: none"> > Réduire la quantité de données collectées et l'étendue du traitement effectué ; > Pseudonymiser les données personnelles dès que possible ; > Garantir la transparence du traitement ; > Permettre à la personne concernée d'exercer ses droits ; > Mettre en place des dispositifs de sécurité et les améliorer. |
| <p>Assurer la sécurité des données – Anticiper les violations (Articles 32, 33 et 34 du RGPD)</p> | <p>De manière générale les organismes doivent garantir la sécurité des données. Ils doivent également identifier les risques associés aux opérations de traitement mises en œuvre et prendre les mesures nécessaires à leur prévention.</p> <p>Par ailleurs, les responsables de traitement doivent mettre en place les procédures adéquates afin d'être en mesure de repérer toute violation de données à caractère personnel et, dans certains cas, de la notifier à l'autorité de protection des données dans les 72 heures et aux personnes concernées dans les meilleurs délais.</p> <p>> Pour plus de détails voir la newsletter n°8 à venir sur l'obligation de sécurité et l'obligation de notification des violations de données.</p> | <ul style="list-style-type: none"> > Pseudonymiser les données ; > Chiffrer les données, notamment en cas de transferts ; > Réaliser des audits réguliers ; > Restreindre et contrôler l'accès aux données : accès physique limité (détention de badges, vidéosurveillance, alarme, etc.) et accès numérique limité (login, mot de passe) ; > Réaliser des sauvegardes régulières ; > Installer des anti-virus et firewall ; > Mettre en place des procédures de gestion des incidents (personnes à contacter, modalités de la notification, etc.). <p>Un téléservice de notification des violations sera disponible sur le site de la CNIL au plus tard en mai 2018.</p> |
| <p>Désigner un Délégué à la Protection des Données (« DPD ») (Articles 37, 38 et 39 du RGPD)</p> | <p>Le DPD est la pierre angulaire de l'accountability.</p> <p>Grâce à son expertise et à son positionnement au sein de l'entreprise il peut en effet, seul ou assisté d'une équipe, faire le lien entre les différents protagonistes, informer et conseiller les décideurs pour sécuriser les initiatives, contrôler le respect de la réglementation dès la conception de projets, piloter la conformité tout en s'adaptant aux contraintes de développement ou encore documenter les processus de traitement pour être prêt en cas de contrôle. Il sert également de point de contact privilégié auprès de la CNIL et des personnes concernées.</p> <p>> Pour plus de détails voir la newsletter n°4 sur le Délégué à la Protection des données</p> | <ul style="list-style-type: none"> > Déterminer si la désignation d'un DPD est obligatoire et, à défaut, si elle présente un intérêt pour l'organisme – documenter la position adoptée ; > Procéder à la détermination d'un profil adapté et d'un positionnement approprié au sein de l'organisme pour remplir la mission de DPD et s'assurer que le DPD possède les connaissances adéquates et les ressources nécessaires ; > S'assurer que les missions du DPD sont bien conformes aux dispositions du RGPD ; > Veiller à ce que le DPD soit associé en temps utile à toutes questions relatives à la protection des données en mettant par exemple en place des procédures de saisine obligatoire du DPD. <p>Le formulaire de désignation du DPD sera mis en ligne sur le site de la CNIL dans les prochains mois.</p> |



| | | |
|--|---|---|
| <p>Gérer les demandes des personnes (Article 12 du RGPD)</p> | <p>Le responsable de traitement doit s'assurer que les procédures et règles internes adéquates ont été mises en place afin de permettre aux personnes concernées d'exercer leurs droits (droits d'accès, de rectification, d'opposition, d'effacement, droit à la limitation du traitement, droit à la portabilité, retrait du consentement) et de traiter leurs demandes et réclamations dans les délais impartis (un mois – prolongeable de 2 mois dans certains cas).</p> <p>> Pour plus de détails voir la voir la newsletter n°12 à venir sur les droits des personnes.</p> | <ul style="list-style-type: none"> > Définir les moyens mis à la disposition des personnes pour exercer leurs droits (l'exercice des droits doit notamment pouvoir se faire par voie électronique si les données ont été collectées par ce moyen) ; > Désigner les acteurs chargés de répondre aux demandes reçues ; > Préparer des modèles types de réponse afin de gérer efficacement toute demande ; > Mettre en place les outils nécessaires pour répondre aux demandes notamment pour le droit d'accès et le droit à la portabilité. |
| <p>Sensibiliser et former les collaborateurs</p> | <p>Les données personnelles constituant un patrimoine de plus en plus stratégique pour les entreprises, tous les acteurs et toutes les divisions sont susceptibles de devoir, à un moment ou à une autre, manipuler de telles données. Il est donc primordial que chacun soit formé et sensibilisé aux questions relatives à la protection des données personnelles.</p> | <p>Le responsable de traitement doit mettre en place un plan de formation et de communication auprès des personnes susceptibles de traiter des données personnelles dans le cadre de leurs fonctions.</p> |

2. Comment « rendre compte » ?

Le second volet du principe d'*accountability* consiste, pour le responsable de traitement, à rendre des comptes et être en mesure d'expliquer et prouver les mesures de protection des données mises en œuvre. Le responsable de traitement doit alors constituer et regrouper la documentation nécessaire (qui doit être présentée aux autorités de contrôle sur simple demande) afin d'assurer la traçabilité des mesures prises, dont notamment la documentation suivante :

| Principe | Description de l'obligation/du processus | Exemples de mesures à mettre en œuvre |
|---|---|---|
| <p>Tenir un registre des activités de traitement (Article 30 du RGPD)</p> | <p>Aux déclarations des traitements ponctuelles se substitue, avec le RGPD, la prise en compte des problématiques de données personnelles en continu. Les traitements mis en œuvre doivent ainsi désormais être répertoriés dans un registre.</p> <p>Le RGPD précise que ces registres doivent se présenter sous une forme écrite, y compris électronique.</p> <p>Une seule exception est prévue à l'obligation de tenir des registres qui s'adresse aux entreprises ou organismes comptant moins de 250 salariés. Les cas d'application de cette exception sont cependant très limités dans la mesure où celle-ci ne s'applique pas si le traitement est susceptible de comporter un risque pour les droits et libertés des personnes concernées, s'il porte notamment sur des données dites « de catégorie particulière » ou relatives à des infractions ou condamnations pénales, et surtout s'il n'est pas occasionnel. Dans les faits, tout traitement qui présente une certaine pérennité devra être inscrit dans un registre, que l'entité comporte plus ou moins de 250 salariés. Il est donc conseillé de tenir un tel registre dans tous les cas.</p> | <ul style="list-style-type: none"> > Déterminer si la tenue d'un registre est obligatoire et, à défaut, si elle présente un intérêt pour l'organisme – documenter la position adoptée ; > Tenir un registre comportant toutes les informations listées par le RGPD (nom et coordonnées du responsable du traitement et du DPD, finalités du traitement, catégories de personnes concernées, catégories de données traitées et de destinataires, durée de conservation et mesures sécurité mises en place si possible) ; > Mettre à jour ce registre régulièrement. <p>Afin d'accompagner les entreprises, la CNIL propose un modèle de registre sur son site.</p> |



Réaliser des analyses d'impact relatives à la protection des données (Privacy Impact Assessment - PIA)
(Articles 35 et 36 du RGPD)

Lorsqu'un traitement est susceptible d'exposer les personnes à un risque élevé au regard de leurs droits et libertés, notamment ceux qui recourent aux nouvelles technologies, le responsable de traitement doit effectuer une analyse d'impact relative à la protection des données. Cette analyse doit permettre d'évaluer, en particulier, l'origine, la nature, la particularité et la gravité de ce risque afin de déterminer, à partir du résultat de l'évaluation, les mesures appropriées à prendre.

L'analyse d'impact est notamment requise pour :

- > Les opérations qui servent à traiter un volume considérable de données personnelles et qui sont susceptibles d'engendrer un risque élevé, par exemple en raison de leur caractère sensible ;
- > Les traitements réalisés en vue de prendre des décisions relatives à des personnes physiques à la suite d'une évaluation d'aspects personnels ;
- > Les traitements aux fins de surveillance à grande échelle de zones accessibles au public.

Il convient de noter que le G29 a établi une liste de 9 critères devant être pris en compte pour déterminer les opérations de traitement devant faire l'objet d'une analyse d'impact du fait d'un risque inhérent élevé.

Le GDPR n'impose pas de méthodologie particulière pour la conduite de l'analyse d'impact mais prévoit ce que cette dernière doit contenir a minima. Si l'analyse révèle que le risque lié au traitement ne peut être atténué par des moyens raisonnables, le responsable doit consulter l'autorité de contrôle.

> Pour plus de détails voir la voir la newsletter n°7 à venir sur les Analyses d'Impact.

> Déterminer pour chaque traitement mis en œuvre si ce dernier est susceptible d'exposer les personnes à un risque élevé au regard de leurs droits et libertés ;

> Si oui réaliser une analyse comprenant notamment les éléments suivants :

- La description des traitements et des finalités ;
- Une évaluation de la nécessité et de la proportionnalité du traitement ;
- Une appréciation des risques pour les droits et libertés des personnes ; et
- Les mesures envisagées pour faire face à ces risques.

> Consulter l'autorité de contrôle (et garder une trace de cette consultation) afin d'obtenir son autorisation préalable en cas de risque résiduel important (l'autorité devra rendre un avis dans un délai de 8 semaines qui peut être prolongé de 6 semaines).

Encadrer les transferts de données hors UE
(Articles 44 à 50 du RGPD)

Lorsque des données sont transférées en dehors de l'UE, dans des pays ne bénéficiant pas d'une décision d'adéquation, des garanties appropriées doivent être mises en place (notamment, les clauses contractuelles types et les BCR). Ces garanties permettront à l'organisme de démontrer la conformité du transfert au RGPD.

A noter que les BCR peuvent être considérées comme une véritable certification de l'entreprise bénéficiaire et ainsi comme un outil majeur de l'accountability.

> Déterminer et mettre en place les mesures nécessaires à l'encadrement des transferts (existence ou pas d'une décision d'adéquation, signature de clauses contractuelles types, mise en place de BCR, adhésion au Privacy Shield, application de dérogations spécifiques) ;

> Envisager de rédiger des BCRs comme outil global de mise en conformité du groupe.



Informez les personnes (Articles 13 et 14 du RGPD)

En cas de collecte directe de données personnelles un certain nombre d'informations doivent être fournies à la personne concernée.

De manière générale ces informations doivent être communiquées de manière concise, transparente, compréhensible, aisément accessible et en des termes clairs et simples.

Les responsables de traitement devront dès lors être en mesure de démontrer aux autorités l'exhaustivité et la transparence des informations communiquées aux personnes ainsi que les modalités de cette communication et rendre ainsi accessibles les mentions d'information délivrées et les procédures mises en place pour assurer l'exercice des droits des personnes.

> Pour plus de détails voir la voir la newsletter n°11 à venir sur l'information des personnes.

> Rédiger et tenir à disposition des autorités les mentions d'information requises par le RGPD. Ces informations doivent idéalement être fournies par écrit à des fins probatoires (politique de confidentialité en ligne, charte informatique annexée au règlement intérieur, notices d'information sur les formulaires de collecte des données, emails, panneaux d'affichage, etc.) ;

> Fournir aux autorités de contrôle toutes chartes et politiques à destination des salariés imposant à ces derniers de traiter les données personnelles des tiers en conformité avec le RGPD.

Encadrer la sous-traitance et la co-traitance de données (Articles 26 et 28 du RGPD)

Le RGPD impose la conclusion d'un contrat écrit entre le responsable du traitement et le sous-traitant dont les dispositions obligatoires sont listées au sein de l'article 28. Outre des informations sur le traitement lui-même (finalité, objet et durée du traitement, etc.), le contrat doit prévoir l'engagement du sous-traitant à respecter toute une série de devoirs à l'égard du responsable de traitement (n'agir que sur instruction documentée, assurer la confidentialité et la sécurité des données, obtenir une autorisation en cas de sous-traitance, etc.).

Les responsables conjoints du traitement doivent quant à eux également définir dans un contrat leurs obligations respectives aux fins d'assurer le respect des exigences du RGPD.

> Pour plus de détails voir la voir la newsletter n°10 à venir sur la sous-traitance.

> Déterminer si le responsable de traitement se trouve dans un rapport de responsabilité conjointe ou de sous-traitance des données ;

> Inclure dans le contrat avec son co-contractant les obligations relatives à la protection des données et notamment :

- En cas de sous-traitance, l'ensemble des dispositions listées à l'article 28 du RGPD ;
- En cas de responsabilité conjointe, les obligations respectives des parties en ce qui concerne l'information et l'exercice des droits des personnes concernées notamment.

Mettre en place une politique de durée de conservation des données

Afin de démontrer le respect des articles 5 (durée de conservation limitée des données), 13 (information des personnes) et 25 (privacy by design and by default) du RGPD, il est fortement recommandé que le responsable de traitement mette en place une politique de conservation des données personnelles cohérente au sein de son organisme.

> Définir les durées de conservation adéquates pour les différents types de données traitées par l'organisme (données RH, commerciales, bancaires, marketing, etc.), en tenant compte de (i) la durée nécessaire au regard des finalités poursuivies, (ii) des recommandations de la CNIL et (iii) des dispositions légales dont les délais de prescription applicables.

> Préciser également la durée et les conditions d'archivage des données le cas échéant.



Identifier et documenter la base légale du traitement (Articles 7, 9, 13 et 21 du RGPD)

Un traitement de données à caractère personnel, pour être licite, doit respecter l'une des six bases légales fixées par RGPD : l'exécution d'un contrat, le respect d'une obligation légale ou l'exécution d'une mission d'intérêt public, la préservation d'un intérêt vital, l'intérêt légitime poursuivi par le responsable de traitement ou encore le consentement de la personne (les conditions d'obtention dudit consentement étant encadrées). Le responsable de traitement devra être à même de justifier auprès des autorités la base choisie.

En cas de collecte de données sensibles, la condition permettant de déroger au principe général d'interdiction du traitement de telles données devra également être documentée.

> Pour plus de détails voir la voir la newsletter n°3 sur les bases légales de traitement.

> S'assurer que les traitements mis en œuvre reposent sur une base adaptée et conforme au RGPD ;
> Conserver les modèles de recueil de consentement et la preuve du recueil du consentement par tout moyen (écrit, trace technologique, enregistrement oral, etc.) ;
> Lorsque le traitement a pour fondement juridique l'« intérêt légitime », vérifier et documenter l'équilibre entre l'intérêt légitime invoqué par le responsable de traitement et les droits de la personne concernée.

Réaliser régulièrement des audits

De manière générale, des procédures régulières de vérification devraient être mises en œuvre afin de s'assurer de l'effectivité et de l'efficacité des mesures prises dans le cadre du RGPD et d'identifier d'éventuels manquements afin de pouvoir prendre les mesures correctives adaptées.

> Prévoir de réaliser une fois par an des audits sur certaines applications.
> Auditer les sous-traitants.

Appliquer des codes de conduite et certifications (Articles 40, 41, 42 et 43)

Le RGPD précise que l'application d'un code de conduite ou d'un mécanisme de certification approuvé peut servir à attester du respect des obligations incombant au responsable de traitement.

Concrètement, le code de conduite est un outil de preuve de la conformité (l'adhésion à un code de conduite est d'ailleurs prise en compte dans les analyses d'impact en ce qu'elle permet de minimiser les risques liés aux traitements réalisés) et constitue une « circonstance atténuante » devant être prises en compte par les autorités de contrôle en cas de décision de sanction.

La certification doit également permettre d'attester de la conformité au RGPD des traitements poursuivis. L'adhésion à un mécanisme de certification peut également être prise en compte par l'autorité de contrôle en cas de décision de sanction.

> Pour plus de détails voir la voir la newsletter n°9 à venir sur les certifications et codes de conduite.

Il n'existe pas encore de certification RGPD. Cependant, la CNIL propose plusieurs labels, dont le label « Gouvernance Informatique et Libertés », le label « Formation » ou encore le label « coffre-fort numérique ». La CNIL a publié en septembre une mise à jour des labels formation et gouvernance pour prendre en compte les exigences du RGPD et pour permettre aux organismes labellisés d'adapter dès que possible leurs procédures et produits labellisés.