Données personnelles
Conseils pratiques pour l'application du RGPD

Conseils pratiques à l'attention des entreprises en prévision de la mise en application du Règlement sur la protection des données applicable à compter du 25 mai 2018

Le présent article ne prétend pas à une forme d'exhaustivité quant aux apports du Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données (ci-après « *RGPD* »).

Il se focalisera essentiellement sur les avancées pratiques les plus importantes pour les sociétés qui souhaiteraient savoir en quoi le RGPD, applicable dès le 25 mai 2018, consiste en un changement de paradigme par rapport à ce qui constitue jusqu'ici le droit applicable en matière de traitement des données à caractère personnel.

Nous verrons donc successivement à quelles entreprises françaises, européennes ou internationales s'appliquera le RGPD, pour quelles raisons on parle désormais de l'avènement d'une responsabilisation (« *accountability* ») des acteurs tant par rapport aux données à caractère personnel qu'ils traitent que celles qu'ils permettent de traiter.

Nous traiterons également des questions du partage de responsabilité entre le responsable du traitement et le sous-traitant et de la sécurité des données qui connaissent un développement par rapport à ce qui était prévu notamment dans la loi du 6 janvier 1978. Nous évoquerons l'obligation pour certains acteurs de désigner un délégué à la protection des données (ci-après DPD), de la question des transferts des données à caractère personnel hors de l'Union européenne, celle du renforcement du droit des personnes dont les entreprises se devront de tenir compte et enfin les sanctions considérables qui sont désormais susceptibles de peser sur les épaules tant des responsables du traitement que de leurs sous-traitants.

La prise en compte du fait que le RGPD s'applique au-delà des strictes sociétés basées dans l'Union européenne

Le RGPD a, en effet, vocation à s'appliquer très largement par le biais d'un champ d'application territorial très étendu. Aux termes de l'article 3 du RGPD, la législation européenne s'applique au traitement des données à caractère personnel effectué par un responsable du traitement ou un sous-traitant établi sur le territoire de l'Union européenne. Peu importe, dans ce cas, que le traitement ait lieu ou non sur le territoire de l'Union.

De plus, le RGPD reste applicable bien que le responsable du traitement ou le sous-traitant ne soit pas établi sur le territoire, si ces derniers :

- effectuent un traitement relatif à une offre de biens ou de services à des personnes se trouvant dans l'Union ;
- suivent le comportement de ces personnes sur le territoire de l'Union (cf. cookies et autres outils de traçage).

Les facteurs permettant de définir si le responsable du traitement ou le sous-traitant offre des biens ou services à des personnes se trouvant au sein de l'Union ne sont pas clairement établis par le RGPD. Il conviendra de se reporter aux faisceaux d'indices permettant de prouver que l'offre de biens ou services est à destination d'un public situé sur le territoire de l'Union, tels que par exemple l'utilisation d'une langue courante dans un ou plusieurs Etats membres, l'utilisation de l'euro comme devise permettant d'acheter des biens ou souscrire à des abonnements, etc.

Ainsi la législation européenne est susceptible de protéger des personnes physiques qui résident hors de l'Union, mais qui s'y trouvaient lors du traitement et donc d'être contraignante

à l'égard des personnes morales et physiques dont le domicile ou le siège social se situe en dehors de l'Union européenne eu égard aux traitements qu'ils effectuent.

La question de savoir où se situe la cible du traitement peut donc donner lieu à application du RGPD à l'égard d'un responsable du traitement situé hors de l'Union européenne.

Le principe de responsabilisation (accountability) du responsable du traitement et du sous-traitant des données à caractère personnel

Afin de responsabiliser le responsable du traitement et le sous-traitant par rapport aux données qu'ils traitent, parfois, en quantité importante, le législateur européen a instauré le principe d'accountability ou de responsabilisation.

Le RGPD a donc choisi de supprimer le système déclaratif actuel par un système en vertu duquel le responsable du traitement sera dispensé de déclarer auprès de l'autorité de contrôle nationalement compétente (Cnil en France) le traitement envisagé, avant sa mise en œuvre. Nonobstant ce qui précède, un régime restreint d'autorisation et de consultation perdurera lorsque le traitement constituera un risque élevé d'atteinte à la vie privée.
A compter du 25 mai 2018, tant le responsable du traitement que le sous-traitant (lequel n'a, en l'état de la législation actuelle, aucune obligation déclarative auprès de l'autorité compétente) devront tenir un registre, similaire à celui tenu par le Correspondant Informatique et libertés prévu par la législation en vigueur dans lequel sera répertorié notamment le nom et l'adresse du responsable du traitement, la finalité du traitement, le service chargé de sa mise en œuvre, les catégories de données traitées, les catégories de personnes concernées par le traitement, les destinataires habilités à recevoir communication des données, la durée de conservation des données traitées, etc.

En conséquence, la suppression des formalités administratives inhérente à l'accountability aura pour corollaire une plus grande responsabilisation des acteurs. Les responsables du traitement et les sous-traitants seront tenus de mettre en place des mesures de sécurité appropriées aux données qu'ils collectent et aux traitements qu'ils effectuent et, surtout, d'être en mesure de démontrer qu'ils ont mis en place lesdites mesures de sécurité en adéquation avec les exigences du RGPD ainsi que leur efficacité.

A titre d'exemple, l'article 35 du RGPD prévoit une obligation dans certains cas de figure de mener une analyse d'impact afin d'évaluer le risque et façonner un cadre aussi protecteur que possible. Ces analyses d'impact s'imposeront surtout pour les traitements faisant courir un risque d'atteinte à la vie privée des utilisateurs[1]. L'objectif de ces analyses d'impact sera d'évaluer, en particulier, l'origine, la nature, la portée, le contexte, la particularité et la gravité du risque lié audit traitement de données à caractère personnel.

Le principe de responsabilisation adopté par le RGPD implique que les responsables prennent donc toutes les « *mesures techniques et organisationnelles appropriées* » afin de respecter les dispositions européennes (article 24 § 1).
Il pourrait, en effet, leur être reproché de ne pas avoir mis en place les mesures adéquates.

C'est ce même principe qui implique que le responsable du traitement comme le sous-traitant soient tenus, dès la conception des produits et services, de mettre en œuvre un socle protecteur des données à caractère personnel (notion dite de « *privacy by design* »).

De la même façon, ils devront s'assurer que sans l'intervention préalable des personnes physiques concernées, les données à caractère personnel ne peuvent être rendues accessibles à un nombre indéterminé de personnes physiques et, que soient collectées et traitées uniquement des données à caractère personnel pertinentes au regard de la finalité du traitement considéré (notion dite de « *privacy by default* » -article 25 § 2).
De manière générale, il conviendra pour l'entreprise de faire un arbitrage afin de déterminer si le traitement qu'elle décide d'effectuer devra être soumis à une analyse d'impact. Il sera donc opportun pour lesdites entreprises de procéder à un audit préalable afin de vérifier si elles sont susceptibles, en raison de leur activité ou du traitement de données à caractère personnel qu'elles envisagent, de faire courir un risque d'atteinte à la vie privée des utilisateurs.

La responsabilité entre le responsable du traitement le sous-traitant encadrée contractuellement

Il convient de distinguer ce que le RGPD, reprenant les stipulations prévues dans la législation européenne en vigueur, entend d'un responsable du traitement, d'une part, et d'un sous-traitant, d'autre part.
L'article 4 du RGPD est consacré aux définitions qui visent à faciliter une meilleure compréhension des dispositions y figurant. Est notamment considéré comme le responsable du traitement : « *la personne physique ou morale qui détermine les finalités et les moyens de toute opération appliquée à des données à caractère personnel. Il s'agit de la personne pour le compte de laquelle est réalisée le traitement* ».

Le sous-traitant est quant à lui défini comme étant : « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement* ».
Ce dernier est donc un exécutant extérieur qui intervient dans le cadre de la mise en œuvre du traitement effectué par le responsable précité. Le sous-traitant agit donc sous l'autorité du responsable du traitement et sur instruction de ce dernier.

En l'état actuel du droit, il incombe au responsable du traitement qui passe par un sous-traitant de s'assurer que ce dernier apporte des garanties suffisantes quant à la mise en œuvre

et au respect des mesures de sécurité à effectuer. Il convient dès lors de prévoir dans le contrat de prestations de services liant le responsable du traitement à son sous-traitant une clause stipulant que le sous-traitant met en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel. Mais in fine, le responsable du traitement verra sa responsabilité engagée dans l'hypothèse où le traitement de données à caractère personnel ne respecte pas la réglementation applicable.
A compter du 25 mai 2018 et de l'application du RGPD, les contrats devront prévoir le partage de responsabilité entre le responsable du traitement et le sous-traitant, ce dernier pouvant donc voir sa responsabilité engagée plus largement. Des clauses contractuelles types pour la rédaction des clauses de responsabilité en matière de données à caractère personnel dans les contrats de prestations de services doivent être élaborées par la Commission européenne et pourront servir de modèle/standard lors de l'élaboration et négociation de contrats.

Un développement accru de l'obligation de sécurité des données

Le sous-traitant sera, tout comme le responsable du traitement, soumis à une obligation de sécurité des données, prévue à l'article 32 du RGPD, considérablement renforcée par rapport à ce que prévoit actuellement la loi 78-17 du 6 janvier 1978 modifiée en 2004. Les mesures adoptées par les deux acteurs se devront d'être adaptées à la nature des données et aux risques encourus. Cette obligation aura un rôle clé dans les contrats liant les deux acteurs, et toute violation pourra entraîner des sanctions administratives, voire pénales.

L'article précité énonce les mesures pouvant être déployées pour assurer cette sécurité :

1. la pseudonymisation et le chiffrement des données à caractère personnel ;
2. des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
3. des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
4. une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ».

Ces dispositions doivent inciter les entreprises à être plus attentives à leur politique de sécurité, et à la modifier si besoin afin de toujours offrir une sécurité optimale.

L'article 33 du RGPD met, par ailleurs, à la charge du responsable du traitement une obligation de notification à l'autorité de contrôle nationalement compétente, en l'espèce la Cnil pour la France, de toute violation de données à caractère personnel. Et ce dans : « *Les meilleurs délais et, si possible, 72 heures au plus tard après avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques* ».

Le responsable devra, par ailleurs, notifier les failles de sécurité ayant eu des conséquences directement à la personne concernée par cette violation, si celles-ci font courir un risque d'atteinte à sa vie privée. Il est utile de préciser que l'obligation de notification des failles de sécurité est une responsabilité qui pèse sur le responsable du traitement.

Le sous-traitant qui subira une violation des données à caractère personnel qu'il traite pour le compte du responsable du traitement sera tenu à l'égard de ce dernier d'un devoir d'information qui l'obligera à lui indiquer dans les meilleurs délais après en avoir pris connaissance la faille qu'il a subie afin que le responsable du traitement puisse prendre les mesures précitées dans le délai indiqué en direction de l'autorité de contrôle et/ou des individus concernés.

Dans l'hypothèse où la notification à l'autorité de contrôle par le responsable du traitement n'a pas lieu dans les 72 heures, elle devra être accompagnée des motifs du retard.

S'agissant du contenu de la notification des failles de sécurité à l'autorité compétente, ladite notification devra contenir :

- une description de la nature de la violation de données à caractère personnel y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés ;
- la communication du nom et des coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- une description des conséquences probables de la violation de données à caractère personnel ;
- une description des mesures prises ou que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

L'obligation de désigner un Data Protection Officer (ci-après DPO) ou Délégué à la protection des données (DPD)

L'article 37 du RGPD européen impose au responsable et au sous-traitant de désigner un Délégué à la protection des données personnelles dans les 3 cas suivants :

1. le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle ;

2. les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées ; ou
3. les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9(4) et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10 ».

En dehors de ces cas, la désignation d'un Délégué à la protection des données est toujours possible.

En premier lieu, le délégué aura pour mission d'informer et de conseiller le responsable du traitement ou le sous-traitant.

En second lieu, il devra contrôler le respect du RGPD européen et de la loi nationale. Enfin, il coopérera avec l'autorité de contrôle et sera ainsi le point de contact de celle-ci. Si le sous-traitant ne respecte pas ces nouvelles obligations, sa responsabilité pourra être engagée, et il pourra ainsi se faire sanctionner par l'autorité de contrôle.
Le Délégué à la protection des données est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir les missions visées à l'article 39 du RGPD. Il peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service.

Le responsable du traitement ou le sous-traitant devront publier les coordonnées du Délégué à la protection des données et les communiquer à l'autorité de contrôle.

Il est vivement conseillé à l'entreprise qui se verra dans l'obligation de désigner un DPD à compter du 25 mai 2018 de réfléchir à la nomination d'un tel profil dès aujourd'hui afin que la mise en place de mesures visées dans le RGPD, au-delà même de sa simple nomination, soit envisagée bien en amont.

Les transferts de données à caractère personnel hors Union européenne

Le RGPD, par son chapitre V, organise le cadre juridique des transferts de données à caractère personnel vers un pays tiers ou des organisations internationales. Il prévoit différents cas autorisant ces transferts, mais pour autant il ne semble pas mettre à la charge du responsable des obligations spécifiques. Ces transferts peuvent être fondés, sur une décision d'adéquation, des garanties appropriées, peuvent prendre la forme de règles d'entreprise contraignantes, ou résulter de situations particulières.

En conséquence, le RGPD ne modifie pas en l'état les règles déjà applicables en matière de transfert de données à caractère personnel en dehors du territoire de l'Union européenne d'un point de vue juridique, même si dans l'hypothèse où des groupes de sociétés avaient mis en place des règles d'entreprise contraignantes, celles-ci devront être revues et complétées à l'aune des dispositions du RGPD.

La différence majeure tient essentiellement dans le fait qu'en l'état actuel, les pays étant considérés comme assurant un niveau de protection adéquat (i.e. les pays situés hors du territoire de l'Union européenne mais pour lesquels les transferts de données à caractère personnel étaient autorisés) ne seront plus fixés par les Etats membres mais par la Commission européenne.

Un renforcement du droit des personnes dont les données sont traitées et collectées

Le RGPD a choisi de renforcer des droits dont les personnes pouvaient déjà se prévaloir, mais aussi d'en créer de nouveaux. Il prévoit un renforcement du droit d'accès de la personne concernée ainsi que du droit de rectification et d'opposition.

L'article 16 du RGPD, concernant le droit de rectification dispose, que « *la personne concernée a le droit d'obtenir du responsable du traitement, dans les meilleurs délais, la rectification des données à caractère personnel la concernant qui sont inexactes* ». Il ne s'agit plus d'un délai de deux mois mais « *dans les meilleurs délais* ».

Concernant le droit d'opposition, l'article 21 du RGPD le subordonne non plus à des motifs légitimes mais à « *des raisons tenant à la situation particulière* » de la personne concernée. Le RGPD rend, par ailleurs, bénéficiaires les personnes concernées de nouveaux droits tels que le droit à la portabilité (article 20), d'intenter des actions collectives (article 80), à la réparation d'un dommage (article 82), à l'oubli (article 17), et à la limitation du traitement (article 18).

Sanctions dues au non-respect des obligations

L'article 58 dispose que chaque autorité nationale de contrôle possède le pouvoir :

- de prononcer un avertissement ;
- de mettre en demeure l'entreprise ;
- de limiter temporairement ou définitivement un traitement ;
- de suspendre les flux de données ;
- d'ordonner et de satisfaire aux demandes d'exercice des droits des personnes ;
- d'ordonner la rectification, la limitation ou l'effacement des données.

Le RGPD contient, par ailleurs, des conditions générales sur le prononcé d'amendes administratives par les autorités nationales de contrôle (article 83 § 2). Parce que ces amendes se doivent d'être effectives, proportionnées et dissuasives, en fonction du type d'infraction, elles pourront s'élever jusqu'à 10 millions € ou, dans le cas d'une entreprise, jusqu'à 2% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu (article 83 § 4)

– exemples : absence de protection des données dès la conception, non respect de la désignation d'un DPD -, voire selon un autre type d'infraction jusqu'à 20 millions € ou, dans le cas d'une entreprise, jusqu'à 4% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu (article 83 § 5) – exemples : infraction relative aux transferts des données ou au non-respect des règles du consentement au traitement -.

Le responsable du traitement pourra d'ailleurs être sanctionné par de telles mesures si son sous-traitant viole le RGPD. Il devra donc porter une attention toute particulière au choix du sous-traitant qu'il sollicite ainsi qu'au contrat qu'il signe avec lui.

Il est, par ailleurs, utile de préciser que la violation d'une disposition légale occasionnant des amendes administratives telle que celles figurant dans le RGPD ne peut faire l'objet d'une couverture par une assurance responsabilité professionnelle à hauteur de tout ou partie des sanctions prévues dans le RGPD. Le fait de ne pas respecter la loi fait par essence partie des hypothèses d'exclusion.

Par ailleurs, l'application du RGPD européen sera sans influence sur les sanctions pénales prévues aux articles 226-16 à 226-24 du code pénal puisqu'il est prévu que les législations nationales puissent déterminer le régime des sanctions pénales susceptibles d'être prononcées en cas de violation.

Pour toutes les raisons exposées précédemment, à compter du 25 mai 2018, nulle entreprise ne pourra prétendre ignorer la loi.

Cela étant, et même si l'alourdissement des sanctions prévues par le RGPD fait peser un risque accru pour les entreprises au regard de la protection des données à caractère personnel, le respect de ce cadre juridique européen harmonisé permettra aux entreprises qui mettront en place une politique adaptée de créer un climat de confiance à l'égard de leurs clients/utilisateurs personnes physiques et d'assurer (autant que possible) la sécurité de leurs données circulant sur le réseau Internet et les autres circuits de communication.

En outre, l'esprit des autorités de contrôle compétentes (tout du moins la Cnil) étant à ce jour, non pas de sanctionner dès la constatation d'un manquement, mais d'accompagner les entreprises contrôlées afin qu'elles respectent les réglementations en vigueur, on peut raisonnablement s'attendre, à compter de mai 2018, à une certaine tolérance à l'égard des entreprises qui prouveront avoir pris conscience en interne des implications du RGPD et tenté de mettre en œuvre tout ou partie des obligations y figurant, ce qui devrait leur permettre d'éviter une condamnation sans sommation et sans un accompagnement préalable de ladite autorité visant à corriger le dispositif ainsi mis en place.

Il est donc temps qu'elles s'y préparent avec l'aide de leurs propres services juridiques pour celles qui en ont les moyens ou de prestataires extérieurs parmi lesquels les cabinets d'avocats intervenant en la matière.

Dans ce domaine comme ailleurs, une entreprise avertie en vaudra deux… voire plus…si l'on s'en tient à la seule analyse de l'ampleur du risque qui pèse désormais sur elle.

Thierry PELIKS
Avocat au Barreau de Paris

Sadry PORLON
Avocat au Barreau de Paris
Docteur en Droit

Notes

(1) *a) L'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques qui est fondée sur un traitement automatisé y compris le profilage ; b) Le traitement à grande échelle de catégories particulières de données visées à l'article 9 §2 ; c) La surveillance systématique à grande échelle d'une zone accessible au public ;*

(2) *Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits ».*