PROTECTION DES DONNÉES PERSONNELLES

39 Les défis de la conformité au GDPR



Merav Griguer,
avocat associée du cabinet Bird & Bird

Julie Schwartz,
avocat, cabinet Bird & Bird

Adrien Aulas,
élève-avocat, cabinet Bird & Bird

The coming into force of the new General Data Protection Regulation (GDPR) as of May, 25th 2018 brings up much uncertainty for concerned companies and public bodies in France, as the legislator has not addressed yet major discrepancies between domestic law and the new European principles. Moreover, the latter themselves still appear to lack sufficient clarity to be thoroughly grasped and enforced. The announced reform of the French Loi Informatique et Libertés should therefore be aimed at creating a consistent, GDPR-compliant legal framework, by implementing and specifying the new applicable rules.

À l'aube de la mise en œuvre des programmes de conformité au nouveau règlement européen sur la protection des données à caractère personnel (GDPR), lequel sera d'application immédiate au 25 mai 2018, et alors même que les organismes publics et privés s'apprêtent à engager des moyens humains et financiers importants en ce sens, de nombreuses problématiques et interrogations se posent encore.

L'actuelle loi n° 78-17 du 6 janvier 1978, dite loi « Informatique et Libertés », bien que récemment réformée, en octobre dernier, par la loi pour une République numérique, présente en effet un certain nombre d'incohérences avec la nouvelle réglementation européenne, qu'il conviendra de gommer. D'autre part, le nouveau règlement européen comprend, quant à lui, un grand nombre d'imprécisions, sources d'insécurité juridique.

À moins d'un an de la date d'application du GDPR, à partir de laquelle la Commission Nationale de l'Informatique et des Libertés (CNIL) a d'ores et déjà annoncé qu'elle opèrerait ses contrôles à l'aune des nouvelles règles, il apparaît donc urgent, pour une préparation sereine et efficace des entités concernées, de démarrer le processus législatif d'adoption de la nouvelle loi Informatique et Libertés, toilettée et augmentée des apports du texte européen.

Cette loi nouvelle devra non seulement veiller à assurer la cohérence entre le droit national et la réglementation européenne en matière de protection des données à caractère personnel, mais également préciser autant que possible les modalités de mise en œuvre des nouveaux principes érigés par le GDPR, sous peine de rendre ineffectif le nouveau cadre juridique applicable en France.

Le présent dossier explore les domaines où les efforts d'adaptation apparaissent les plus urgents : nouveau droit à la portabilité *(dossier 40)*, notification des violations de données à caractère personnel *(dossier 41)*, introduction du délégué à la protection des données ou data protection officer (DPO) *(dossier 42)* et responsabilité nouvelle du sous-traitant *(dossier 43)*.

LES DÉFIS DE LA CONFORMITÉ AU GDPR

40

Le nouveau droit à la portabilité

Entre imprécision et risque de confusion

Merav Griguer,
avocat associée du cabinet Bird & Bird

Adrien Aulas,
élève-avocat, cabinet Bird & Bird

L'article 20 du GDPR introduit au bénéfice des personnes dont les données à caractère personnel sont traitées un nouveau droit à la portabilité, défini comme le droit « *de 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* »[1].

Ce droit, dont le champ d'application est limité par plusieurs conditions restrictives, soulève de nombreuses interrogations quant aux modalités exactes de sa mise en pratique, auxquelles les lignes directrices récemment publiées par le Groupe de travail de l'Article 29 (G29) n'ont que partiellement répondu[2].

D'autre part, la loi pour une République numérique, en insérant d'ores et déjà dans le Code de la consommation français une sous-section dédiée à la « récupération et [la] portabilité des données »[3], est venue créer un risque d'incohérence et de confusion entre le droit français à la portabilité et le droit européen à la portabilité. L'articulation de ces dispositions nationales avec le GDPR, dont notamment les contours exacts de leur applicabilité, devrait donc être précisée dans le souci d'une plus grande sécurité juridique.

1. Un droit limité aux données fournies par la personne concernée

Le droit à la portabilité, tel que défini par le GDPR, ne couvre expressément que les données à caractère personnel fournies au responsable du traitement par la personne qui exerce ce droit, dans le cadre d'un traitement automatisé auquel cette personne a consenti, ou nécessaire à l'exécution d'un contrat ou de mesures précontractuelles auxquels cette personne est partie.

Est ainsi clairement exclue la portabilité de données traitées manuellement (par exemple au moyen d'un logiciel de tableur), ainsi que des données traitées, par exemple, sur le fondement d'une obligation légale ou réglementaire incombant au responsable du traitement.

Concernant la délimitation des données « *fournies* » par une personne donnée, le G29 précise que celle-ci devait faire l'objet d'une interprétation large, incluant non seulement les données volontairement transmises - par exemple, lors de la création d'un compte ou par voie d'un formulaire en ligne-, mais également les données brutes issues de l'observation de l'activité de cette personne, telles que des historiques de navigation ou de géolocalisation.

Ne demeurent donc hors du champ du droit à la portabilité, selon le G29, que les données « *inférées ou dérivées* » au terme d'une analyse menée par le responsable du traitement, par exemple, un profil de consommateur généré par l'algorithme d'une régie publicitaire.

1. *PE et Cons. UE, règl. (UE) 2016/679, 27 avr. 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, art. 20.1 : JOUE n° L 119, 4 mai 2016, p. 1.*
2. *G29, Lignes directrices relatives au droit à la portabilité des données, 5 avr. 2017.*
3. *L. n° 2016-1321, 7 oct. 2016 pour une République numérique, art. 48 : JO 8 oct. 2016, texte n° 1.*

Les entreprises et organismes publics responsables de traitements devront, par conséquent, être en mesure de retracer en permanence avec certitude l'origine de chaque donnée, ainsi que le fondement de son traitement, afin de faire la distinction entre celles relevant du droit à la portabilité et celles n'en relevant pas. Les systèmes internes de référencement des données devront ainsi, dans certains cas, évoluer afin de permettre une telle distinction. Les contrats avec les hébergeurs et les autres sous-traitants devront par ailleurs prévoir les conditions de leur participation à la sélection et à la transmission des données pertinentes[4].

Cette distinction, dans la mesure où elle devra être opérée par les responsables de traitement eux-mêmes face à chaque demande, et compte tenu des sanctions encourues en cas de non-respect du droit à la portabilité (jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial annuel de l'entreprise), devrait reposer sur un critère clair et certain. L'autorité de contrôle ou le législateur français œuvreraient ainsi utilement en précisant davantage, au niveau national, les limites exactes des catégories de données concernées.

2. Des incertitudes quant aux obligations des responsables de traitement

Le nouveau règlement exige, d'autre part, que le droit à la portabilité « *ne porte pas atteinte aux droits et libertés de tiers* »[5]. Cette formulation, très large, ne précise pas cependant la nature des droits et libertés ainsi protégés, ni la répartition des responsabilités, en cas d'atteinte, entre la personne exerçant son droit à la portabilité, le responsable de traitement qui s'y conforme, et éventuellement le tiers à qui les données sont portées.

Des difficultés pourraient ainsi naître dans l'hypothèse où une personne demanderait la portabilité à une société tierce de certains de ses courriers électroniques susceptibles d'attenter à la vie privée d'autrui, ou de révéler des informations couvertes par un secret professionnel ou industriel. La personne lésée pourrait, dans ce cas, se retourner contre le responsable du traitement qui a donné suite à la demande, pour ne pas avoir efficacement filtré ou protégé les informations litigieuses.

Si le G29 indique expressément que l'entité qui communique les données, dans la mesure où elle se borne à agir sur instruction de la personne qui exerce son droit à la portabilité, ne saurait être tenue pour responsable des usages qui en sont faits par leur destinataire, de telles situations demeurent *a priori* largement problématiques.

En effet, l'application d'une qualification de complicité pénale ne saurait être exclue, dans le cas, par exemple, de la violation d'un secret professionnel, sur le seul fondement des lignes directrices précitées. Ainsi, comme l'a récemment souligné le Conseil d'État, les avis du G29 n'ont pas, au regard du droit français, de valeur normative[6] . Il convient donc d'appliquer les recommandations et avis du G29 avec prudence.

La réforme annoncée de la loi Informatique et Libertés devrait envisager de clarifier, sous forme d'un texte ayant pleine valeur légale ou réglementaire, les conditions de la responsabilité des différents acteurs en jeu dans le cadre d'une demande de portabilité, dont notamment leur articulation avec l'ensemble des autres règles de responsabilité, civile ou pénale, pouvant être invoquées à leur encontre.

3. Une dualité de régimes source de confusion

Les responsables de traitement concernés sont enfin confrontés à l'ambiguïté des nouvelles dispositions des articles L. 224-42-1 et suivants du Code de la consommation. En créant un droit à la portabilité spécifique aux consommateurs, le législateur français a en effet introduit une dualité de fondements juridiques pour un même objet, sans préciser clairement les modalités de leur chevauchement.

Ce droit à la portabilité national, dont l'entrée en vigueur a d'ailleurs été repoussée au 25 mai 2018 par souci d'alignement avec le GDPR[7], est conçu comme couvrant aussi bien des données à caractère personnel que des données « *autres* » (en d'autres termes, dépourvues de caractère personnel), listées à l'article L. 224-42-3 du Code de la consommation. Le champ d'application de ce texte excède donc celui de l'article 20 du GDPR.

Il est en revanche réservé aux consommateurs au sens de l'article liminaire du code précité, à savoir « *toute personne physique qui agit à des fins qui n'entrent pas dans le cadre de son activité commerciale, industrielle, artisanale, libérale ou agricole* », pour des données fournies dans le cadre de services de communication au public en ligne uniquement[8], là où le droit à la portabilité du nouveau règlement peut être exercé par toute personne physique.

Concernant la « *récupération* » des données à caractère personnel de ces consommateurs, les nouvelles dispositions de droit national se bornent à renvoyer au régime du droit à la portabilité prévu par le GDPR. Sur ce terrain, leur impact paraît donc limité.

La difficulté tient aux données « *autres* », pour lesquelles l'article L. 224-42-3 semble introduire un régime de récupération spécial, imposant notamment au fournisseur d'un service de

4. *GDPR, art. 28.3.e).*
5. *GDPR, art. 20.4.*
6. *CE, 9e et 10e ch. réunies, 8 févr. 2017, n° 393714 : JurisData n° 2017-002339.*
7. *L. n° 2016-1321, 7 oct. 2016, préc., art. 48.II.*
8. La communication au public en ligne est définie par l'article 1er de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique comme « *toute transmission, sur demande individuelle, de données numériques n'ayant pas un caractère de correspondance privée, par un procédé de communication électronique permettant un échange réciproque d'informations entre l'émetteur et le récepteur* ». Constitue ainsi un service de communication au public en ligne, notamment, tout site Internet, hormis dans la mesure où il n'offre qu'un service de correspondance privée ; les services de messagerie électronique, par exemple, ne sont donc manifestement pas couverts par le régime du droit à la portabilité national.

communication au public en ligne de prévoir une fonctionnalité gratuite permettant au consommateur de récupérer « *par une requête unique* » l'ensemble des données en question.

Ces données couvrent « *tous les fichiers mis en ligne par le consommateur* » et « *toutes les données résultant de l'utilisation du compte d'utilisateur du consommateur et consultables en ligne par celui-ci, à l'exception de celles ayant fait l'objet d'un enrichissement significatif par le fournisseur en cause* », ainsi que plus largement les données « *associées au compte utilisateur* » qui « *facilitent le changement de fournisseur de service ou permettent d'accéder à d'autres services* ». Pour ces dernières, le texte invite par ailleurs à « *prend*[re] *en compte l'importance économique des services concernés, l'intensité de la concurrence entre les fournisseurs, l'utilité pour le consommateur, la fréquence et les enjeux financiers de l'usage de ces services* ».

Cette définition paraît problématique à deux égards. D'une part, le dernier critère suggère une forme de mise en balance trop peu déterminée, source d'insécurité juridique pour les fournisseurs de services qui seront amenés à devoir la mettre en œuvre. D'autre part, il est probable qu'un grand nombre de ces données « *autres* » s'avéreraient, à l'analyse, présenter en réalité un caractère personnel, compte tenu de l'interprétation usuellement très large de cette notion par les autorités de contrôle. Il sera ainsi vraisemblablement en pratique très difficile, pour les entreprises concernées, de distinguer le régime à appliquer à différents paquets de données.

Ici encore, l'intervention du législateur français, dans le cadre de la réforme de la loi Informatique et Libertés, paraît donc souhaitable, afin de clarifier l'articulation du texte national et du texte européen, dans le sens d'une meilleure lisibilité.

LES DÉFIS DE LA CONFORMITÉ AU GDPR

41

Notification des violations des données à caractère personnel

Vers un cumul de régimes pour les fournisseurs de services de communications électroniques accessibles au public

Merav Griguer,
avocat associée du cabinet Bird & Bird

Julie Schwartz,
avocat, cabinet Bird & Bird

La gestion des violations de données à caractère personnel est un enjeu important tant pour les individus que pour les responsables de traitement, d'autant plus que les attaques informatiques profitant de failles de sécurité sont récurrentes. Ainsi, le GDPR précise qu'une violation de données à caractère personnel peut causer aux personnes physiques concernées des dommages variés aussi bien physiques, matériels que moraux : perte de contrôle des données, limitation des droits des personnes, discrimination, vol, usurpation d'identité, perte financière, renversement non autorisé d'une procédure de pseudonymisation, atteinte à la réputation, perte de confidentialité de données protégées par le secret professionnel, ou encore, tout autre dommage d'ordre économique ou social. Pour les organismes publics comme privés, la violation des données à caractère personnel dont ils sont responsables constitue un enjeu d'ordre réputationnel et financier (risque de sanction pécuniaire, action en dommages et intérêts, etc.).

1. Le nouveau régime de violation des données à caractère personnel

L'article 33 du GDPR[1] pose l'obligation pour tout responsable de traitement, entreprises privées comme organismes publics, de notifier à l'autorité de contrôle les violations des données à caractère personnel susceptibles d'engendrer un risque pour les droits et libertés des personnes physiques. Est entendu par violation de données à caractère personnel « *toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données* »[2].

1. *GDPR, art. 3* : « *En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation en question à l'autorité de contrôle compétente conformément à l'article 55, dans les meilleurs délais et, si possible, 72 heures au plus tard après en 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. Lorsque la notification à l'autorité de contrôle n'a pas lieu dans les 72 heures, elle est accompagnée des motifs du retard* ».

2. *GDPR, art. 4.*

L'article 34 du GDPR prévoit l'obligation, pour tout responsable de traitement, de communiquer dans les meilleurs délais aux personnes concernées la violation de données à caractère personnel les concernant susceptible d'engendrer un risque élevé pour leurs droits et libertés, sauf si le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées telles que le chiffrement, ou s'il a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées n'est plus susceptible de se matérialiser, ou encore, si cette communication exige des efforts disproportionnés (auquel cas la communication doit être publique)[3].

Le GDPR prévoit, en cas de non-respect des dispositions relatives aux violations de données à caractère personnel, une amende plafonnée à 10 millions d'euros ou 2 % du chiffre d'affaires annuel mondial.

Les organismes publics comme privés se préparent donc dès à présent à intégrer des outils et procédures internes adaptés pour être en mesure de gérer au mieux les violations de données à caractère personnel et devront documenter toutes les violations de données à caractère personnel subies, leurs effets et les mesures prises pour y remédier, afin de permettre à l'autorité compétente d'exercer ses contrôles.

2. Obligation de notification des sous-traitants

Les sous-traitants, traitant des données à caractère personnel pour le compte de responsables de traitement, sont, quant à eux, soumis à l'obligation de notifier au responsable de traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

Il est donc recommandé d'intégrer l'obligation d'information du sous-traitant dans le contrat conclu avec le responsable de traitement afin de définir dans quel délai le sous-traitant doit informer le responsable de traitement, sous quelle forme, à quelle personne le sous-traitant doit notifier, etc. Il peut également être envisagé de désigner un interlocuteur dédié chez le responsable de traitement pour réceptionner ces informations, ou bien encore de mettre en place une ligne téléphonique afin qu'il soit joignable à tout moment.

3. Le risque de cumul de deux régimes de notification des violations des données à caractère personnel pour les fournisseurs de services de communications électroniques accessibles au public

L'article 34 bis de la loi Informatique et Libertés, introduit par ordonnance[4], prévoit à ce jour que seuls les fournisseurs de services de communications électroniques accessibles au public doivent notifier les violations de données à caractère personnel à la CNIL.

L'introduction dans le GDPR de l'obligation pour tout responsable de traitement de données à caractère personnel de notification des violations de données à caractère personnel interroge quant au maintien ou non du régime particulier pour les fournisseurs de services de communications électroniques accessibles au public.

L'obligation spécifique, prévue par l'article 34 bis de la loi Informatique et Libertés, est en effet plus étendue et plus contraignante que celle prévue par le GDPR : les fournisseurs de services de communications électroniques accessibles au public sont tenus de notifier à la CNIL, l'intégralité des violations de données à caractère personnel qu'ils subissent, indépendamment de tout critère de risque pour les personnes concernées. De plus, le règlement européen (UE) 611/2013[5] précise les modalités et délais de notification prévus à leur égard, qui sont plus exigeants : la notification à la CNIL est fixée à 24 heures maximum pour la constatation de la violation, et au plus tard 72 heures pour les détails complémentaires, sauf retard à justifier. Le contenu obligatoire de la notification est, en outre, particulièrement détaillé et l'information à fournir aux personnes concernées doit inclure un résumé de l'incident ayant causé la violation, ainsi que des recommandations circonstanciées pour atténuer les préjudices.

La nouvelle loi Informatique et Libertés devra tenir compte de ce risque de juxtaposition avec l'actuel régime particulier applicable aux fournisseurs de services de communications électroniques accessibles au public. Le législateur français dispose déjà d'un signal à suivre au niveau européen : la récente proposition de règlement « Vie privée et communications électroniques » (dit règlement e-privacy), publiée le 10 janvier dernier, a en effet opté pour une disparition pure et simple du régime spécial des fournisseurs de services de communications électroniques, au profit d'une application uniforme du GDPR. Cette solution aurait ainsi l'avantage de la lisibilité. Le G29 a d'ailleurs salué cette volonté d'uniformisation dans son avis sur

3. *GDPR, art. 34.3 : « La communication à la personne concernée visée au paragraphe 1 n'est pas nécessaire si l'une ou l'autre des conditions suivantes est remplie :*
a) le responsable du traitement a mis en œuvre les mesures de protection techniques et organisationnelles appropriées et ces mesures ont été appliquées aux données à caractère personnel affectées par ladite violation, en particulier les mesures qui rendent les données à caractère personnel incompréhensibles pour toute personne qui n'est pas autorisée à y avoir accès, telles que le chiffrement ;
b) le responsable du traitement a pris des mesures ultérieures qui garantissent que le risque élevé pour les droits et libertés des personnes concernées visé au paragraphe 1 n'est plus susceptible de se matérialiser ;
c) elle exigerait des efforts disproportionnés. Dans ce cas, il est plutôt procédé à une communication publique ou à une mesure similaire permettant aux personnes concernées d'être informées de manière tout aussi efficace ».

4. *Ord. n° 2011-1012, 24 août 2011 relative aux communications électroniques : JO 26 août 2011, p. 14473.*

5. *Comm. UE, règl. (UE) n° 611/2013, 24 juin 2011 concernant les mesures relatives à la notification des violations de données à caractère personnel : JOUE n° L 173, 26 juin 2013, p. 2.*

le règlement e-privacy[6] soulignant qu'un tel choix permettrait d'éviter toute superposition de réglementation.

En toutes hypothèses, les fournisseurs de services de communications électroniques accessibles au public ainsi que tout responsable de traitement devront mettre en place des outils et procédures pour répondre aux obligations du GDPR.

Sur le plan technique, des procédures de détection des failles de sécurité devront être réalisées et des audits des traitements et des pratiques devront être régulièrement menés. En cas de traitement présentant manifestement un degré de criticité élevé, des analyses d'impact préalables (*Privacy Impact Assessments*) devront être réalisées afin de déterminer les mesures de sécurité spécifiquement adaptées à ces traitements.

Sur le plan opérationnel, il est recommandé dès à présent d'établir en interne une procédure pour décrire les différentes étapes à suivre en cas de violation de données à caractère personnel. Cette procédure devra prendre la forme de lignes directrices indiquant notamment les personnes à informer en interne, les éléments à porter à leur connaissance et leur formalisme, les délais à respecter, les actions devant être priorisées, etc. Cette procédure devra également indiquer les actions à entreprendre après la notification à l'autorité de contrôle compétente afin d'assurer un suivi de la notification et des mesures mises en œuvre en interne. La procédure devra être particulièrement adaptée au secteur d'activité de l'entreprise ou organisme concerné ainsi qu'aux données traitées, notamment s'il s'agit de données sensibles ou de traitements à risques. La rédaction et la mise en œuvre de cette procédure participe de plus à la constitution de la documentation rendue obligatoire par le GDPR ainsi qu'à l'anticipation du principe d'*accountability*.

Les employés devront par ailleurs être formés à cette procédure et sensibilisés aux risques et enjeux des violations de données à caractère personnel. Il pourra par exemple être édicté des bonnes pratiques ou un code de conduite au sein de l'entreprise ou de l'organisme concerné pour minimiser le risque de violation de données à caractère personnel. Des délégations de pouvoir pourront être prévues pour optimiser la gestion de crise en cas de violation de données à caractère personnel.

Le data protection officer[7] (DPO) aura de surcroît un rôle central en cas de violation de données à caractère personnel, non seulement en amont dans la réalisation de procédures et la formation et sensibilisation des employés, mais également en aval en tant que point de contact avec l'autorité compétente. Le DPO aura également un rôle de coordinateur entre les différents services et directions. En effet, en cas de violation de données à caractère personnel, il sera essentiel que les équipes notamment juridique, informatique, conformité, ressources humaines et marketing collaborent, tout particulièrement pour la mise en œuvre des mesures de protection des données, la rédaction de la notification et l'information des personnes concernées.

Enfin, les sous-traitants devront être choisis en fonction des garanties de sécurité et de confidentialité des données qu'ils offrent. Le contrat entre responsable de traitement et sous-traitant devra contenir une clause contenant les obligations des deux parties en termes de sécurité et de confidentialité des données ainsi que la répartition des responsabilités.

Au regard des risques encourus et de la multiplication des attaques informatiques liées à des failles de sécurité, il est essentiel de se préparer dès aujourd'hui et d'anticiper en interne les dispositions du GDPR relatives aux violations de données à caractère personnel.

6. *G29, opinion 01/2017, 4 avr. 2017 sur la proposition de règlement e-privacy.*

7. V. *ce numéro, dossier 42.*

NOTIFICATION DES VIOLATIONS DE DONNÉES À CARACTÈRE PERSONNEL
TABLEAU COMPARATIF DU RÉGIME ACTUEL ET DU RÉGIME À ANTICIPER

		Article 34 bis de la loi I&L et Règlement (UE) 611/2013	Articles 33 et 34 du GDPR
	Responsables de traitement concernés	**Fournisseurs de services de communications électroniques accessibles au public** (enregistrés auprès de l'ARCEP)	**Tous les responsables de traitements de données à caractère personnel**
Notification à l'autorité de contrôle	**Conditions**	**En toute hypothèse**	**Uniquement si** la violation paraît susceptible d'engendrer un risque pour les droits et libertés des personnes concernées
	Délai	Sans délai (24h maximum pour la constatation, puis 72h pour les détails et éléments supplémentaires)	Dès que l'information est disponible, sans délai (si possible sous 72h) Les informations peuvent être communiquées au fur et à mesure de leur constatation par le responsable de traitement
	Contenu	Utilisation obligatoire du formulaire mis à disposition sur le site de la CNIL, reprenant les informations obligatoires prévues par le règlement (UE) 611/2013 : **Partie 1 (sous 24h) :** identification du fournisseur et informations initiales sur la violation (à compléter dans des notifications ultérieures le cas échéant) • Nom du fournisseur • Identité et coordonnées du DPO ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues • Mention indiquant s'il s'agit d'une première ou d'une deuxième notification • Date et heure de l'incident (si elles sont connues ; une estimation peut être fournie si nécessaire) et du constat de l'incident • Circonstances de la violation (par exemple : perte, vol, reproduction) • Nature et teneur des données concernées • Mesures techniques et organisationnelles appliquées (ou à appliquer) aux données concernées • Recours à d'autres fournisseurs ayant joué un rôle (le cas échéant) **Partie 2 (sous 72h supplémentaires) :** informations supplémentaires sur la violation de données à caractère personnel, notification supplémentaire éventuelle aux abonnés ou aux particuliers et questions transnationales éventuelles • Résumé de l'incident à l'origine de la violation (y compris le lieu physique de la violation et le moyen de stockage concerné) • Nombre d'abonnés ou de particuliers concernés • Conséquences et préjudices potentiels pour les abonnés ou particuliers • Mesures techniques et organisationnelles prises par le fournisseur pour atténuer les préjudices potentiels • Contenu de la notification • Moyens de communication utilisés • Nombre d'abonnés ou de particuliers informés • Extension de la violation à des abonnés ou des particuliers dans d'autres États membres • Notification à d'autres autorités nationales compétentes	• Nature et détails de la violation (nombre et type de données et personnes concernées) • Nom et coordonnées du DPO ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues • Conséquences probables de la violation • Mesures prises ou proposées pour remédier à la violation

		Article 34 bis de la loi I&L et Règlement (UE) 611/2013	Articles 33 et 34 du GDPR
Notification aux personnes concernées	**Conditions**	En cas de **risque d'atteinte** aux données à caractère personnel ou à la vie privée des intéressés, sauf mesures appropriées	Si la violation est susceptible d'engendrer un **risque élevé** pour leurs droits et libertés, sauf mesures appropriées ou efforts disproportionnés
	Délai	Sans délai, à compter soit de la constatation du risque (élevé, sous le nouveau régime), soit de l'injonction de la CNIL (ou de toute autre autorité de contrôle compétente, sous le nouveau régime)	
	Contenu	• Nom du fournisseur • Identité et coordonnées du DPO ou d'un autre point de contact • Résumé de l'incident à l'origine de la violation • Date estimée de l'incident • Nature et teneur des données concernées • Conséquences vraisemblables de la violation • Mesures prises par les fournisseurs pour remédier à la violation • Circonstances de la violation (dont notamment lieu de la violation et durée séparant la violation de sa constatation) • Mesures recommandées aux personnes concernées pour atténuer les préjudices potentiels	• Description en des termes clairs et simples de la nature de la violation • Nom et coordonnées du DPO, du responsable de traitement ou d'un autre point de contact • Conséquences probables de la violation • Mesures prises ou envisagées pour remédier à la violation
Documentation des violations en interne	**Contenu**	Tenue obligatoire d'un inventaire des violations de données à caractère personnel, notamment de leurs modalités, de leurs effets et des mesures prises pour y remédier L'inventaire est tenu à disposition de la CNIL	Documentation obligatoire de toute violation de données à caractère personnel, indiquant les faits concernant la violation, ses effets et les mesures prises pour y remédier La documentation est tenue à disposition des autorités de contrôle compétentes

LES DÉFIS DE LA CONFORMITÉ AU GDPR

42 Issues Related to the Designation of the DPO



Merav Griguer,
avocat associée du cabinet Bird & Bird
Julie Schwartz,
avocat, cabinet Bird & Bird
Adrien Aulas,
élève-avocat, cabinet Bird & Bird

L'obligation de désignation d'un DPO prévue par le GDPR devra être introduite dans la nouvelle loi Informatique et Libertés. Compte tenu du périmètre des missions du DPO et du niveau d'expertise exigé, tout l'enjeu de la création de ce nouveau dispositif consistera à veiller à permettre l'effectivité de cette fonction aussi ambitieuse que fondamentale.

Article 37 of the GDPR, which will be applicable as of May, 25th 2018, introduces the new function of a data protection officer (DPO). This DPO will be made mandatory in many companies and public bodies that qualify as data controller or processor. Said companies and public bodies, along with those that will choose to recruit one as part of their compliance scheme, will have to choose their DPO cautiously, as the GDPR provides for high requirements relating to expected levels of expertise.

As compliance will be required right from the coming into application of the new regulation, with fines up to € 10 million or 2% of the annual worldwide turnover in the case of a company, concerned entities are starting as of now to look for the right candidates, and preparing to accommodate the chosen ones.

Despite some clarification brought by recent WP29 guidelines[1], it is still uncertain, though, how DPOs are to be introduced in the largest of said entities, where one DPO shall be in charge, with a same expected degree of expertise, of many diverse and complex processing operations.

1. A widely applicable new obligation

Pursuant to Article 37 of the GDPR, appointment of a DPO will be mandatory under the following conditions:

- for processing carried out by a public authority or body, except for courts acting in their judicial capacity;
- for data controllers or data processors whose core activities consist of processing operations which, by virtue of their nature, scope and/or purposes, require regular and systematic monitoring of data subjects on a large scale; or,
- for data controllers or data processors whose core activities consist of processing on a large scale of sensitive data (e.g. personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, or data relating to criminal convictions and offences).

These requirements shall apply to data controllers as well as to data processors, the latter now being fully liable under the GDPR provisions. Also, the notion of "large scale" is anticipated to concern many private companies. The WP29 stated that its interpretation should rely on the number of data subjects, the volume of processed data, the duration of the processing and its geographical scope.

In any case, companies that do not meet the above criteria are still highly encouraged to appoint a DPO, as it is a strong signal of internal compliance. Refusal to do so will have to be justified, and the reasons for it documented, so that the data protection authority may exercise its control.

2. An equally wide scope of prerogatives

The DPO will take a leading part within the entity's compliance processes, as he/she should be involved in every personal data-

1. *WP29's Guidelines on Data Protection Officers ('DPOs'), as last revised and adopted on 5 April 2017.*

related activity. In particular, the GDPR provisions and WP29's guidelines describe its prerogatives as comprising:

- advising and informing the data controller or data processor, and their employees carrying out processing, of their obligations;
- ensuring compliance with the GDPR provisions and all other relevant data protection rules;
- advising for drafting of privacy impact assessments (PIAs);
- cooperating with the data protection authorities.

As such, the DPO should participate in every meeting relating to current and new data processing activities, and should be referred to for every matter concerning data protection within the entity, including notably:

- the register of processing activities[2];
- the appropriate security measures[3];
- the data breach notifications[4];
- the PIAs[5];
- the prior consultation of the data protection authority[6];
- the "privacy by design" and "privacy by default" procedures[7];
- as well as every matter arising from the exercise of data subjects' rights as listed under Chapter III of the GDPR.

The DPO shall also be in charge of the information of employees dealing with personal data, possibly in various geographical areas and fields of expertise, which could range, for instance, from HR whistleblowing schemes to customer analytics, or the implementation of a new IT protocol.

WP29 therefore makes it clear that the DPO should have full access to any relevant resources for the fulfillment of his/her tasks, including in particular financial and material resources (budget, premises, sufficient dedicated time in cases where the DPO also holds another position within the company, support team, etc.).

The DPO's contact details should be broadly communicated in order for employees and data subjects to reach him/her easily. They should also be submitted to the competent data protection authority upon appointment. In cases where the concerned entity operates internationally, this could mean that said entity's DPO will be likely to receive requests from many different countries, in many different languages.

3. How to build the data protection governance around the DPO?

The WP29 provides some precise criteria as to what shall make the "perfect" DPO. These criteria refer in particular to technical and legal expertise in the field of data protection with regard to the level of complexity of the operations put under his/her supervision, in-depth knowledge of the company and of its processing activities, personal integrity and ethics.

The DPO may be either appointed within the company, or externalized. However, the DPO should not, in any case, hold a position that would allow him/her to participate in the determination of purposes and means of the company's processing - that is acting as a data controller. Besides, the GDPR allows for the designation of a single DPO within a business group consisting of multiples entities, as long as he/she is easily accessible from each of its facilities (in both technical and linguistic terms).

In contrast, the new regulation stays silent, unfortunately, as to the ability of a given entity to appoint several DPOs, depending on the various countries or regions it operates in, and/or its different fields of business.

This option could be appreciated by large, multinational companies, where they would find it difficult to identify a single candidate whose expertise sufficiently covers, for instance, all its marketing-, HR- or IT-related processing activities. Such processing activities are indeed governed, from a data protection perspective, by different logics, different knowledge and sometimes different national standards, making it all the more complicated to find a "global specialist".

Given the importance of the DPO in the new data protection governance scheme brought up by the GDPR, and the increasing relevance of compliance as a comparative advantage on globalized, cutting-edge markets, clarification on that point by national legislators or data protection authorities would therefore obviously be warmly welcomed.

2. *GDPR, art. 30.*
3. *GDPR, art. 32.*
4. *GDPR, art. 33 & 34.*
5. *GDPR, art. 35.*
6. *GDPR, art. 36.*
7. *GDPR, art. 25.*

LES DÉFIS DE LA CONFORMITÉ AU GDPR

43

Les incertitudes liées à la création du nouveau régime de responsabilité directe pour les sous-traitants

Merav Griguer,
avocat associée du cabinet Bird & Bird

Adrien Aulas,
élève-avocat, cabinet Bird & Bird

L'une des nouveautés majeures portées par le GDPR consiste dans l'introduction d'obligations à la charge du sous-traitant en charge de la mise en œuvre de tout ou partie du traitement de données à caractère personnel, et partant d'une responsabilité directe et personnelle de celui-ci.

Employant des termes équivalents à ceux de l'actuelle loi Informatique et Libertés, le nouveau règlement (GDPR) définit le sous-traitant comme « *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* »[1], ce dernier s'entendant à son tour comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement* »[2].

Compte tenu par ailleurs de l'interprétation traditionnellement large de la notion de traitement de données à caractère personnel[3], sont ainsi autant de sous-traitants au sens de la réglementation l'hébergeur d'un site Internet, le gestionnaire externe d'un parc téléphonique d'entreprise, ou encore la filiale implémentant sur instruction de sa maison-mère une solution informatique visant à centraliser les données relatives aux employés du groupe.

Il découle donc du nouveau texte européen que ces sous-traitants seront eux-mêmes sujets, dès le 25 mai 2018, aux contrôles menés par l'autorité compétente, ainsi qu'aux sanctions qui pourraient en résulter dans le cas d'un manquement aux dispositions applicables du GDPR. Ils seront également susceptibles de faire l'objet d'un recours juridictionnel par les personnes concernées, en cas de violation de l'une de ces dispositions ayant entraîné un préjudice à l'endroit de celles-ci[4].

Ces dispositions ont trait pour l'essentiel à l'obligation de sécurité du traitement[5], à l'obligation de tenir un registre des traitements[6], ou encore à la désignation d'un délégué à la protection des données[7]. Le sous-traitant est par ailleurs tenu d'assister le responsable de traitement pour le compte duquel il opère dans le cadre de l'exécution des obligations de ce dernier[8].

L'application de ce nouveau cadre juridique, si elle correspond à une volonté de renforcer la protection des données à caractère personnel des citoyens européens en étendant le champ de

1. *GDPR, art. 4.8.*
2. *GDPR, art. 4.7.*
3. *GDPR, art. 4.2 :* constitue un traitement « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction* ».
4. *GDPR, art. 79.*
5. *GDPR, art. 32.*
6. *GDPR, art. 30.*
7. *GDPR, art. 37.* - Sur le DPO, V. *ce numéro, dossier 42.*
8. *GDPR, art. 28.3.f.*

la norme aux entreprises simplement « exécutantes », n'est cependant pas sans soulever plusieurs incertitudes.

1. La répartition et l'aménagement des responsabilités entre responsable de traitement et sous-traitant

Les organismes publics comme privés, acteurs concernés, s'interrogent sur l'articulation de ces deux responsabilités dorénavant juxtaposées : celle du sous-traitant et celle du responsable de traitement.

En l'absence de précision du texte européen, plusieurs solutions sont en effet envisageables au regard des différents régimes de responsabilité envisagés par le droit français, à l'égard aussi bien des sanctions administratives prévues par le règlement européen, que des condamnations à des dommages-intérêts qui pourraient découler de l'action civile des personnes concernées.

La responsabilité peut, en premier lieu, être conjointe, le sous-traitant et le responsable de traitement n'étant responsables que du montant de sa sanction ou condamnation personnelle (déterminée, en règle générale, à proportion de la gravité des manquements respectifs à la règle applicable).

La responsabilité peut, en second lieu, être solidaire, le responsable de traitement comme le sous-traitant pouvant être enjoints à payer l'intégralité du montant des sanctions ou condamnations de chacun, à charge pour celui qui s'en acquitte de se retourner contre l'autre.

Dans les deux cas, la responsabilité peut également, sauf à ce qu'elle soit jugée d'ordre public, être aménagée contractuellement : responsable de traitement et sous-traitant pourraient ainsi souhaiter s'entendre pour stipuler des garanties ou des limitations de responsabilité, afin de sécuriser en amont les conséquences pour chacun d'un manquement commis par l'autre.

Chacun de ces régimes (responsabilité conjointe ou solidaire, responsabilité aménageable ou d'ordre public) n'est pas sans entraîner des conséquences aussi différentes qu'essentielles quant au niveau de risque assumé par chacune des parties en présence. Il appartiendra donc au législateur, dans un souci de sécurité juridique, de préciser les règles applicables sur ce point.

L'aménagement de la responsabilité pourra du reste, en toute hypothèse, s'appuyer sur les mécanismes traditionnels de l'assurance : le responsable de traitement est ainsi en droit de subordonner la conclusion du contrat de prestation de service à l'obligation pour son sous-traitant de souscrire une « cyber-assurance », propre à couvrir les risques encourus, notamment, en cas de faille de sécurité engendrant une violation de données à caractère personnel.

2. Une opportunité de renégociation des contrats de sous-traitance

À ces problématiques viennent s'ajouter celles créées par l'obligation nouvelle de formaliser dans un acte juridique contraignant les droits et obligations réciproques du responsable de traitement et du sous-traitant en matière de protection des données à caractère personnel.

L'article 28.3 du GDPR prévoit en effet un certain nombre de clauses obligatoires, à inclure dans les contrats en cours comme dans les contrats nouveaux, afin d'assurer que les sous-traitants recrutés assurent un niveau de protection suffisant des données confiées.

Le sous-traitant est ainsi tenu de s'engager contractuellement à prendre toutes les mesures nécessaires afin d'assurer la sécurité du traitement[9], à assurer le respect de la confidentialité des données par les personnes qu'il autorise à y avoir accès[10], ou encore à mettre à la disposition du responsable de traitement toutes les informations nécessaires pour démontrer le respect de ses obligations, y compris en permettant des audits ou inspections diligentés par ce dernier[11].

Bien que le texte du règlement européen ne précise pas les sanctions à prévoir par le contrat en cas d'inexécution de l'une de ces obligations, il résulte de ces clauses obligatoires la superposition d'un deuxième (voire troisième) niveau de responsabilité pour le sous-traitant, qui sera tenu de justifier de tout manquement à ses obligations aussi bien vis-à-vis du responsable de traitement que de l'autorité de contrôle (et, le cas échéant, des personnes concernées).

La négociation et la rédaction des clauses relatives à la protection des données à caractère personnel devront donc faire l'objet d'un temps et d'une attention rehaussés, d'autant plus que certaines clauses, dont notamment celle autorisant le responsable de traitement à procéder à des audits et des « inspections », pourront sembler difficilement acceptables pour certains sous-traitants.

Les rapports de force sont en effet variables, dès lors qu'un prestataire de services informatiques en *cloud* opérant à l'échelle mondiale se verra appliquer la même qualification de sous-traitant qu'une entreprise de dimension locale, et partant, sera soumis à ce même type d'obligations, en pratique peu réalistes.

L'un des enjeux de l'intégration du GDPR par la nouvelle loi Informatique et Libertés devrait donc à l'évidence consister dans l'aménagement d'une plus grande scalabilité de ces obligations, là où le texte européen omet de le prévoir[12].

9. *GDPR, art. 28.3.c.*
10. *GDPR, art. 28.3.b.*
11. *GDPR, art. 28.3.h.*
12. Il convient de relever que le GDPR prévoit, dans un même souci pragmatique, un certain nombre d'exemptions au bénéfice des petites et moyennes entreprises, par exemple, en matière de tenue du registre des traitements *(art. 30.5)*.