LATHAM&WATKINS

Client Alert Commentary

Latham & Watkins Data Privacy & Security Practice 10 juillet 2018 | Number 2342

Promulgation de la loi « *relative à la protection des données personnelles* »

To read this Client Alert in English, please click here.

La loi n° 2018-493 « relative à la protection des données personnelles » a été promulguée le 20 juin 2018 et marque une étape importante dans l'adaptation de la législation française au nouveau corpus européen en matière de protection de ces données.

Eléments clés:

- Outre l'augmentation du montant des sanctions, les pouvoirs de la CNIL sont considérablement renforcés rendant ainsi son action plus efficace.
- Les dérogations au RGPD mises en place par le législateur français s'appliqueront aux seuls résidents français indépendamment du lieu d'établissement du responsable du traitement.
- L'adaptation du droit français au nouveau corpus européen se poursuivra dans les mois à venir.

Le Règlement européen n° 2016/679 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel (le RGPD) entré en application le 25 mai 2018 et la Directive nº 2016/680 relative aux traitements mis en œuvre à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuite en la matière ou d'exécution de sanctions pénales (la Directive) du 27 avril 2016, représentent une avancée considérable en matière de protection des données à caractère personnel. Cette réglementation, axée sur la responsabilisation des acteurs, introduit de nouvelles obligations à la charge des responsables du traitement (tenue d'un registre des activités de traitement, conduite d'analyses d'impact, protection des données dès la conception, information plus complète et transparente des personnes concernées, notification en cas de violation de données, etc.) mais également des sous-traitants (tenue d'un registre des activités de traitement conduites pour le compte du responsable du traitement, conclusion d'un contrat avec le responsable du traitement conforme aux exigences de l'article 28 du RGPD, assistance du responsable du traitement notamment en cas de violation de données, etc.).

Le nouveau régime issu du droit européen, bien que comprenant de nombreuses règles d'application directe, a nécessité une adaptation de la loi n° 78/17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (la Loi Informatique et Libertés) aux nouvelles exigences du RGPD et de la Directive par la loi relative à la protection des données à caractère personnel en date du 20 juin 2018.

Le processus parlementaire

Le projet de la loi « *relatif à la protection des données personnelles* » a fait l'objet de nombreux débats entre l'Assemblée nationale et le Sénat. Bien que la procédure accélérée fut engagée dès le 13 décembre 2017 par le Gouvernement, le projet de loi n'a fait l'objet d'une adoption définitive que le 14 mai 2018. La saisine du Conseil Constitutionnel effectuée par plus de 60 sénateurs le 16 mai dernier a retardé la promulgation du texte qui devait initialement intervenir avant l'entrée en application du RGPD le 25 mai 2018. Le Conseil Constitutionnel a rendu sa décision le 12 juin 2018 et a validé l'essentiel du texte.

Les prochaines étapes à venir

Le décret n° 2005-1309 du 20 octobre 2005 pris en application de la Loi Informatique et Libertés devrait également être modifié.

Une ordonnance devrait être promulguée dans un délai de six mois pour procéder à une réécriture de l'ensemble de la Loi Informatique et Libertés afin notamment d'améliorer son intelligibilité et assurer la cohérence de l'ensemble de la législation applicable à la protection des données à caractère personnel.

Les principales modifications apportées à la Loi Informatique et Libertés

Les modifications apportées auront des implications importantes pour les individus et les entreprises. Plus particulièrement, elles octroient de nouveaux pouvoirs à Commission nationale de l'Informatique et des Libertés (la CNIL) et comportent l'exercice par le législateur français de plusieurs marges de manœuvres laissées à la discrétion des Etats membres par le RGPD.

Les nouveaux pouvoirs de la CNIL

Une mission d'accompagnement

Dotée d'une mission d'accompagnement des acteurs, la CNIL pourra élaborer de nouveaux outils de droit souple sous forme de lignes directrices, de recommandations ou encore de référentiels (basés sur les anciennes autorisations uniques et normes simplifiées actualisées au regard des nouvelles exigences du RGPD) (article 11, Loi Informatique et Libertés).

Des pouvoirs de contrôles étendus

D'une part, le régime d'opposabilité du secret professionnel a été clarifié : le secret ne peut être opposé aux agents de la CNIL sauf lorsque les informations concernées sont couvertes par le secret avocat-client, le secret des sources journalistiques ou le secret médical. A titre de rappel, la Loi Informatique et Libertés était antérieurement muette sur ce sujet.

Les agents de la CNIL peuvent désormais faire usage d'une identité d'emprunt pour renforcer l'efficacité des contrôles en ligne.

D'autre part, l'ancienne rédaction de l'article 44 de la Loi Informatique et Libertés prévoyait que les membres et agents de la CNIL étaient habilités à visiter des locaux « *à usage professionnel* », ce qui conduisait à exclure certaines zones telles que les halls d'immeuble ou les couloirs. Cette précision disparaît désormais afin d'accroître l'efficacité des contrôles sur place, avec pour limite la protection du domicile privé.

Enfin, une nouvelle voie de recours est instituée en faveur de la CNIL (article 43 quinquies, Loi Informatique et Libertés) dans le cadre d'un transfert de données vers un Etat non membre de l'Union

Européenne, la CNIL peut être saisie d'une réclamation dirigée contre un responsable du traitement ou un sous-traitant. Si elle estime fondés les griefs avancés relatifs à la protection des droits et libertés d'une personne, elle peut saisir le Conseil d'État afin que celui-ci ordonne la suspension du transfert. La CNIL peut assortir ses conclusions d'une demande de question préjudicielle à la Cour de justice de l'Union européenne.

Un pouvoir de sanction accru

La loi « *relative à la protection des données personnelles* » augmente considérablement les pouvoirs de sanctions de la CNIL (articles 45 et 46, Loi Informatique et Libertés). Lorsque des manquements aux obligations du responsable du traitement ou du sous-traitant sont portés à sa connaissance, la CNIL réunie en formation restreinte peut prononcer à l'égard du responsable du traitement fautif les sanctions suivantes :

- Un avertissement (facultatif)
- Une mise en demeure de se mettre en conformité ; en cas d'extrême urgence, le délai peut être fixé à 24 heures
- Un rappel à l'ordre
- Une limitation temporaire ou définitive du traitement, son interdiction ou le retrait d'une autorisation accordée
- Une injonction de se mettre en conformité susceptible d'être accompagnée d'une astreinte dont le montant ne peut excéder 100 000 € par jour de retard
- Une injonction de satisfaire aux demandes d'exercice des droits des personnes concernées
- Un retrait d'une certification, ou l'injonction, à l'organisme certificateur concerné, de refuser une certification ou de retirer la certification accordée
- Une suspension des flux de données adressées à un destinataire situé dans un pays tiers ou à une organisation internationale
- Une suspension partielle ou totale de la décision d'approbation des règles d'entreprises contraignantes
- Une amende administrative qui selon les manquements varie entre (i) un montant de 10 millions d'euros ou 2% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu, et (ii) un montant de 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu

La CNIL reconnaît que les contrôles opérés auront essentiellement pour but, dans un premier temps, d'accompagner les organismes dans une courbe d'apprentissage vers la bonne mise en œuvre des textes lorsque des obligations nouvelles sont concernées. Cela étant dit, les principes fondamentaux de la protection des données (loyauté du traitement, pertinence des données, durée de conservation, sécurité des données, etc.) continueront de faire l'objet de vérifications rigoureuses par la CNIL.

L’instauration d’une procédure d’urgence

Le président de la CNIL peut saisir la formation restreinte dans le cadre d’une procédure d’urgence (article 46, Loi Informatique et Libertés) qui sera définie par décret en Conseil d’Etat lorsque :

- Le non-respect d’une disposition du RGPD ou de la Loi Informatique et Libertés porte atteinte à l’identité humaine, aux droits de l’homme, à la vie privée, aux libertés individuelles ou publiques
- Le président de la CNIL considère qu’il est urgent d’intervenir

La formation restreinte pourra alors prendre l’une des mesures suivantes :

- L'interruption provisoire de la mise en œuvre du traitement, y compris d'un transfert de données hors de l'Union européenne, pour une durée maximale de trois mois
- La limitation du traitement de certaines des données à caractère personnel traitées, pour une durée maximale de trois mois
- La suspension provisoire de la certification délivrée au responsable de traitement ou à son sous-traitant
- La suspension provisoire de l'agrément délivré à un organisme de certification ou un organisme chargé du respect d'un code de conduite
- La suspension provisoire de l'autorisation de traiter des données à caractère personnel dans le domaine de la santé lorsque le traitement n’est pas conforme aux référentiels de la CNIL
- L’injonction de mettre en conformité le traitement avec les obligations résultant du RGPD ou de la Loi Informatique et Libertés ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, pouvant être assortie d'une astreinte dont le montant ne peut excéder 100 000 € par jour de retard à compter de la date fixée par la formation restreinte
- Un rappel à l'ordre
- L'information du Premier ministre pour la prise de mesures permettant de faire cesser la violation constatée, si le traitement en cause est au nombre de ceux qui intéressent la sûreté de l'Etat ou la défense ou de ceux relevant de la Directive lorsqu'ils sont mis en œuvre pour le compte de l'Etat

Les marges de manœuvre adoptées en droit français

Le champ d'application territoriale des marges de manœuvre

La France a choisi le critère du **lieu de résidence de la personne concernée** comme critère pour déterminer le champ d'application territoriale des marges manœuvres françaises permises par le RGPD. Ainsi, la loi nationale s'applique dès lors que la personne concernée réside en France et ce, même si le responsable du traitement n'est pas établi en France (sauf traitement relatif à la liberté d'expression et d'information) (article 5-1, Loi Informatique et Libertés). Ce choix plus protecteur pour les individus n'a fait l'objet d'aucune discussion ou débats entre les parlementaires. Cela avait pourtant interpellé la CNIL qui n'avait pas manqué de soulever les difficultés pratiques qui pourraient se présenter. En effet, le législateur aurait pu faire le choix de ne rien indiquer dans la loi et de laisser, en cas de litiges, les juridictions nationales appliquer les règles classiques en matière de conflit de lois.

L'âge de consentement du mineur

Après des débats houleux entre l'Assemblée Nationale et le Sénat, l'âge à partir duquel un mineur peut consentir seul au traitement de ses données concernant l'offre directe de services de la société de l'information est fixée à 15 ans (article 7-1, Loi Informatique et Libertés). Cette position défendue par l'Assemblée Nationale et approuvée par le Conseil Constitutionnel repose sur un souci de cohérence avec d'autres textes législatifs en vigueur (par exemple, dans le domaine de la médecine, un mineur de 15 ans peut exiger de son médecin qu'il ne divulgue pas les informations médicales à son sujet).

Lorsque le mineur est âgé de moins de 15 ans et que le traitement repose sur le consentement, la licéité du traitement est conditionnée au recueil d'un double consentement : celui du mineur et celui du titulaire de l'autorité parentale. Le Conseil Constitutionnel a estimé que le RGPD permettait aux États membres de prévoir (i) soit que le consentement était donné pour le mineur par le titulaire de l'autorité parentale, (ii) soit que le mineur était autorisé par le titulaire de l'autorité parentale à consentir, ce qui suppose alors le double consentement.

La possibilité de former une action de groupe

La loi « *relative à la protection des données personnelles* » élargit la possibilité de former une action de groupe dans le domaine des données à caractère personnel (article 43 ter, Loi Informatique et Libertés). Pour compenser les dommages matériels et moraux d'une violation de la protection de leurs données à caractère personnel et en constatation d'un manquement du responsable du traitement ou de son sous-traitant, la personne concernée pourra ainsi agir en réparation auprès d'une association agréée (dont l'objet statutaire est la protection de la vie privée et des données à caractère personnel). Cette action de groupe peut être exercée devant la juridiction civile ou la juridiction administrative compétente par le demandeur qui en informe la CNIL. Toutefois, cette action de groupe ne sera ouverte que pour les faits générateurs du dommage survenus après le 24 mai 2018.

Le traitement des données relatif aux condamnations pénales, aux infractions et aux mesures de sûreté

La loi « *relative à la protection des données personnelles* » pose le principe selon lequel il est interdit de procéder au traitement des données de nature pénale par des personnes autres que l'autorité publique (article 9, Loi Informatique et Libertés).

Elle modifie la loi existante afin d'introduire trois autres exceptions à l'interdiction du traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions :

- Les entités collaborant au service public de la justice (ces catégories d'entités seront définies par un décret d'application)

- Les victimes ou les défendeurs (qu'il s'agisse de personnes physiques ou morales) afin de leur permettre de préparer, d'engager et de suivre une procédure judiciaire ;

- Les utilisateurs de l'information publique disponible dans les décisions judiciaires

Ces exceptions s'ajoutent aux exceptions existantes pour les tribunaux, les entités publiques et les entités juridiques exploitant un service public, les auxiliaires de justice et les entités juridiques dont le but premier est d'administrer le droit d'auteur. Ainsi, la loi n'accorde aux employeurs aucune base juridique pour le traitement et les vérifications des antécédents judiciaires.

L'exception concernant les victimes ou les défenseurs n'est autre que la consécration de la réserve d'interprétation formulée par le Conseil Constitutionnel dans sa décision n° 2004-499 en date du 29 juillet 2004 qui avait censuré l'article 9 de la Loi Informatique et Libertés dans sa rédaction issue de la loi n° 2004-801 du 6 août 2004.

La suppression des formalités préalables

Le RGPD marque la fin de la plupart des formalités déclaratives préalables. Toutefois, le législateur a choisi de conserver une formalité préalable pour trois types de traitement:

- **Les traitements de données de santé :** la loi « *relative à la protection des données personnelles* » maintient un régime protecteur sur le traitement des données de santé ; si le traitement est conforme à un référentiel ou règlement-type de la CNIL, il pourra être mis en œuvre après une déclaration auprès de la CNIL attestant de sa conformité ; s'il n'est pas conforme, il ne pourra être mis en œuvre qu'après autorisation de la CNIL (article 54, Loi Informatique et Libertés).

  La CNIL doit rendre sa décision suite à la demande d'autorisation dans un délai de deux mois (renouvelable une fois) par décision motivée de son Président ou lorsque l'affaire est soumise à l'Institut National de l'Informatique de la Santé ; en revanche, si la CNIL n'émet pas d'avis dans ce délai, la demande est réputée acceptée.

- **Les traitements mis en œuvre pour le compte de l'Etat qui portent sur des données génétiques ou des données biométriques nécessaires à l'authentification ou au contrôle de l'identité des personnes** : ces traitements seront soumis à un régime d'autorisation par décret après avis de la CNIL (article 27, Loi Informatique et Libertés).

- **Le traitement du Numéro d'Inscription au Répertoire (NIR) :** la loi « *relative à la protection des données personnelles* » maintient un régime protecteur sur le traitement du NIR. Cependant, la loi prévoit un allègement des formalités liées à la mise en œuvre de traitements sur le NIR (article 22, Loi Informatique et Libertés). Elle propose de prévoir un décret-cadre, pris après avis motivé et publié de la CNIL pour autoriser l'utilisation du NIR par catégorie de responsables du traitement et pour des finalités précises.

Les prochaines étapes

La loi « *relative à la protection des données personnelles* » permet ainsi la mise en œuvre concrète en droit français du corpus européen de protection des données à caractère personnel adopté par l'Union européenne.

Le corpus européen sera bientôt complété par l'adoption du Règlement « *vie privée et communications électroniques* » (dit ePrivacy) destiné à remplacer la directive ePrivacy 2002/58/CE. Ce texte actuellement en cours de négociations au Conseil de l'UE vise à garantir la confidentialité qui s'applique au traitement des données de communications électroniques en relation avec la fourniture et l'utilisation de services de communications électroniques et aux informations concernant l'équipement terminal des utilisateurs finaux. Toutes les communications sont ciblées, tant les communications traditionnelles (déjà réglementées par l'ancienne Directive ePrivacy) que les nouvelles communications électroniques, comme les applications de messagerie instantanée. A l'ère de la digitalisation de la société, de très nombreuses entreprises seront concernées.

Pour toute question relative à cette Client Alert, vous pouvez contacter l'un des auteurs ci-dessous ou l'avocat de Latham & Watkins qui vous conseille habituellement :

Myria Saarinen
myria.saarinen@lw.com
+33.1.40.62.20.00
Paris

Julie Ladousse
julie.ladousse@lw.com
+33.1.40.62.20.00
Paris

Elise Auvray
elise.auvray@lw.com
+33.1.40.62.20.00
Paris

Floriane Cruchet
floriane.cruchet@lw.com
+33.1.40.62.20.00
Paris

Vous pourriez également être intéressé par :

The Technology, Media & Telecommunications Review, Eighth Edition - France

GDPR Resource Center

Global Privacy & Security Compliance Law Blog