TD 1 : Gestion des données personnelles

Entrée en vigueur de la nouvelle loi « Informatique et Libertés » et de son nouveau décret d'application

03 juin 2019

Le décret n° 2019-536, publié le 30 mai 2019, constitue la dernière étape de la mise en conformité du droit national avec le Règlement général sur la protection des données (RGPD) et la Directive « police-justice », applicable aux fichiers de la sphère pénale. Le cadre juridique national relatif à la protection des données est dorénavant stabilisé. La CNIL a rendu un avis sur ce texte le 9 mai 2019.

RGPD Chapitre 1

Article 5 - Principes relatifs au traitement des données à caractère personnel

1. **Les données à caractère personnel doivent être :**

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);

d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);

2. **Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité).**

Article 6 - Licéité du traitement

1. **Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :**

a) la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques;

b) le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci;

c) le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis;

d) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;

e) le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;

f) le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.
Le point f) du premier alinéa ne s'applique pas au traitement effectué par les autorités publiques dans l'exécution de leurs missions.

2. **Les États membres peuvent maintenir ou introduire des dispositions plus spécifiques pour adapter l'application des règles du présent règlement pour ce qui est du traitement dans le but de respecter le paragraphe 1, points c) et e), en déterminant plus précisément les exigences spécifiques applicables au traitement ainsi que d'autres mesures visant à garantir un traitement licite et loyal, y compris dans d'autres situations particulières de traitement comme le prévoit le chapitre IX.**

Article 9 - Traitement portant sur des catégories particulières de données à caractère personnel

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.

Le paragraphe 1 ne s'applique pas si l'une des conditions suivantes est remplie :

a) la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée;

b) le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale, dans la mesure où ce traitement est autorisé par le droit de l'Union, par le droit d'un État membre ou par une convention collective conclue en vertu du droit d'un État membre qui prévoit des garanties appropriées pour les droits fondamentaux et les intérêts de la personne concernée;

c) le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement;

d) le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale, à condition que ledit traitement se rapporte exclusivement aux membres ou aux anciens membres dudit organisme ou aux personnes entretenant avec celui-ci des contacts réguliers en liaison avec ses finalités et que les données à caractère personnel ne soient pas communiquées en dehors de cet organisme sans le consentement des personnes concernées;

e) le traitement porte sur des données à caractère personnel qui sont **manifestement rendues publiques** par la personne concernée;

f) le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle;

g) le traitement est nécessaire pour des motifs d'intérêt public important, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée;

h) le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale sur la base du droit de l'Union, du droit d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé et soumis aux conditions et garanties visées au paragraphe 3;

i) le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux, sur la base du droit de l'Union ou du droit de l'État membre qui prévoit des mesures appropriées et spécifiques pour la sauvegarde des droits et libertés de la personne concernée, notamment le secret professionnel;

j) le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, conformément à l'article 89, paragraphe 1, sur la base du droit de l'Union ou du droit d'un État membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée.

Chapitre II : Droits de la personne concernée

Article 51

I.-Le **droit à l'effacement** s'exerce dans les conditions prévues à l'article 17 du règlement (UE) 2016/679 du 27 avril 2016.

II.-En particulier, sur demande de la personne concernée, **le responsable du traitement est tenu d'effacer dans les meilleurs délais les données à caractère personnel qui ont été collectées dans le cadre de l'offre de services de la société de l'information lorsque la personne concernée était mineure au moment de la collecte.** Lorsqu'il a transmis les données en cause à un tiers lui-même responsable de traitement, il prend des mesures raisonnables, y compris d'ordre technique, compte tenu des technologies disponibles et des coûts de mise en œuvre, pour informer le tiers qui traite ces données que la personne concernée a demandé l'effacement de tout lien vers celles-ci, ou de toute copie ou de toute reproduction de celles-ci.

Article 53

Le **droit à la limitation du traitement** s'exerce dans les conditions prévues à l'article 18 du règlement (UE) 2016/679 du 27 avril 2016.

Article 55

Le **droit à la portabilité des données** s'exerce dans les conditions prévues à l'article 20 du règlement (UE) 2016/679 du 27 avril 2016.

Article 15 - Droit d'accès de la personne concernée

1. **La personne concernée a le droit d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel ainsi que les informations suivantes:**

a) **les finalités du traitement**;

b) **les catégories** de données à caractère personnel concernées;

c) **les destinataires** ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, en particulier les destinataires qui sont établis dans des pays tiers ou les organisations internationales;

d) lorsque cela est possible, **la durée de conservation** des données à caractère personnel envisagée ou, lorsque ce n'est pas possible, les critères utilisés pour déterminer cette durée;

e) l'existence du droit de demander au responsable du traitement **la rectification ou l'effacement de données à caractère personnel**, ou une limitation du traitement des données à caractère personnel relatives à la personne concernée, ou du droit de s'opposer à ce traitement;

f) le **droit d'introduire une réclamation** auprès d'une autorité de contrôle;

g) lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée, toute **information disponible quant à leur source**;

h) **l'existence d'une prise de décision automatisée**, y compris un profilage, visée à l'article 22, paragraphes 1 et 4, et, au moins en pareils cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

2. **Lorsque les données à caractère personnel sont transférées vers un pays tiers ou à une organisation internationale**, la personne concernée a le droit d'être informée des garanties appropriées, en vertu de l'article 46, en ce qui concerne ce transfert.
3. **Le responsable du traitement fournit une copie des données à caractère personnel faisant l'objet d'un traitement**. Le responsable du traitement peut exiger le paiement de frais raisonnables basés sur les coûts administratifs pour toute copie supplémentaire demandée par la personne concernée. Lorsque la personne concernée présente sa demande par voie électronique, les informations sont fournies sous une forme électronique d'usage courant, à moins que la personne concernée ne demande qu'il en soit autrement.

Article 16 - Droit de rectification

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. Compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire.

Article 17 - Droit à l'effacement («droit à l'oubli»)

1. La personne concernée a le **droit d'obtenir du responsable du traitement l'effacement,** dans les meilleurs délais, de données à caractère personnel la concernant et le responsable du traitement a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais, lorsque l'un des motifs suivants s'applique:

a) **les données à caractère personnel ne sont plus nécessaires** au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière;

b) **la personne concernée retire le consentement** sur lequel est fondé le traitement, conformément à l'article 6, paragraphe 1, point a), ou à l'article 9, paragraphe 2, point a), et il n'existe pas d'autre fondement juridique au traitement;

c) **la personne concernée s'oppose au traitement** en vertu de l'article 21, paragraphe 1, et il n'existe pas de motif légitime impérieux pour le traitement, ou la personne concernée s'oppose au traitement en vertu de l'article 21, paragraphe 2;

d) les données à caractère personnel ont fait l'objet **d'un traitement illicite**;

e) **les données à caractère personnel doivent être effacées pour respecter une obligation légale** qui est prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis;

f) les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information visée à l'article 8, paragraphe 1.

2. Lorsqu'il a rendu publiques les données à caractère personnel et qu'il est tenu de les effacer en vertu du paragraphe 1, le responsable du traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables, y compris d'ordre technique, pour informer les responsables du traitement qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement par ces responsables du traitement de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci.

3. **Les paragraphes 1 et 2 ne s'appliquent pas dans la mesure où ce traitement est nécessaire:**

a) à l'exercice du droit à la liberté d'expression et d'information;

b) pour respecter une obligation légale qui requiert le traitement prévue par le droit de l'Union ou par le droit de l'État membre auquel le responsable du traitement est soumis, ou pour exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement;

c) pour des motifs d'intérêt public dans le domaine de la santé publique, conformément à l'article 9, paragraphe 2, points h) et i), ainsi qu'à l'article 9, paragraphe 3;

d) à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, dans la mesure où le droit visé au paragraphe 1 est susceptible de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement; ou

e) à la constatation, à l'exercice ou à la défense de droits en justice.

Article 21 - Droit d'opposition

1. La personne concernée a le **droit de s'opposer** à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant fondé sur l'article 6, paragraphe 1, point e) ou f), y compris un profilage fondé sur ces dispositions. Le responsable du traitement ne traite plus les données à caractère personnel, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice.
2. Lorsque les données à caractère personnel sont traitées **à des fins de prospection**, la personne concernée a le droit de s'opposer à tout moment au traitement des données à caractère personnel la concernant à de telles fins de prospection, y compris au profilage dans la mesure où il est lié à une telle prospection.
3. Lorsque la personne concernée **s'oppose au traitement à des fins de prospection**, les données à caractère personnel ne sont plus traitées à ces fins.
4. Au plus tard au moment de la première communication avec la personne concernée, le droit visé aux paragraphes 1 et 2 est **explicitement porté à l'attention** de la personne concernée et est **présenté clairement** et séparément de toute autre information.
5. Dans le cadre de l'utilisation de services de la société de l'information, et nonobstant la directive 2002/58/CE, la personne concernée peut exercer **son droit d'opposition** à l'aide de procédés automatisés utilisant des spécifications techniques.
6. Lorsque des données à caractère personnel sont traitées à des fins de recherche scientifique ou historique ou à des fins statistiques en application de l'article 89, paragraphe 1, la personne concernée a le droit de s'opposer, pour des raisons tenant à sa situation particulière, au traitement de données à caractère personnel la concernant, à moins que le traitement ne soit nécessaire à l'exécution d'une mission d'intérêt public.

Section 2 - Sécurité des données à caractère personnel

Article 32 - Sécurité du traitement

Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins:

a) la **pseudonymisation et le chiffrement des données** à caractère personnel;

b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

c) 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;

d) une procédure visant à **tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles** pour assurer la sécurité du traitement.

Article 7 - Conditions applicables au consentement

1. Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.
2. Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante.
3. La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement.
4. Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat.
5. «**consentement**» de la personne concernée, toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement

Le cas R.Dashian

Mme Dashian voyage beaucoup. Lors d'un séjour dans le Morbihan, elle a réservé en ligne une chambre dans un hôtel de la chaine Goodhotel. La réservation et le paiement de la chambre ont nécessité la création d'un compte client en ligne. La chaine Goodhotel appartient à un groupe international Entertainement limited group qui possède une compagnie d'aviation et des parcs d'attractions.

Le formulaire de réservation faisait mention de droits relatifs au RGPD et la case était pré-cochée et Mme Dashian a du faire état de son allergie pour le Tofu (donc des problèmes de santé) et renseigner ses empreintes digitales, mentions prévues dans le formulaire web.

Le formulaire évoquait aussi vaguement un traitement de données pour gérer la bonne exécution de la réservation de la chambre.

Très vite après son séjour Morbihannais, M Dashian constate qu'elle est abonnée à la newsletter de Entertainement limited group. Elle est destinataire d'offres de billets d'avion à prix réduits.

Mme Dashian demande alors par lettre recommandée un droit d'accès à ses données auprès du DPO de Goodhotel qui lui envoie des données qui semblent incomplètes car les données bancaires qu'elle a renseignées n'y figure pas.

Pas de mention non plus des traitements de données réalisées par Goodhotel ou Entertainement limited group …

Mme Dashian demande donc à exercer son droit d'opposition. Elle envoie une demande au DPO, qui ne répondra jamais.

Une semaine plus tard, Mme Dashian reçoit une offre commerciale pour le parc d'attraction Funland Paris, propriété du group Entertainement limited. Mme Dashian est abasourdie d'autant que dans la presse, une fuite de données concernant Goodhotel est rendue publique par l'ANSSI et la CNIL. Un serveur mal sécurisé aurait laissé fuiter les données.

D'autant que Mme Dashian a vu qu'elle pouvait choisir un mot de passe assez court (5 caractères) : elle a utilisé le mot de passe suivant : kanye .

Elle se souvient alors qu'elle vient de verser 100 000 $ par virement à la suite d'un message reçu de son assurance santé. Elle a peur d'avoir été l'objet d'un phishing.

En googlisant Goodhotel, Mme Dashian lit sur des forums que Goodhotel continuerait à envoyer des messages commerciaux à des clients ayant résidés dans leur hôtel 10 ans auparavant ! Certains sont semblent-ils décédés depuis.

Mme Dashian vous contacte pour la conseiller sur une action judiciaire possible. A partir des éléments du RGPD et des affaires proches (depuis 2020) documentées sur le site de la CNIL (dans la section Communiqués du site), rédigez une proposition d'action auprès de la CNIL et identifiez des articles du RGPD qui pourraient être invoqués et qui ont été retenus dans les précédentes affaires.