La Newsletter dédiée à la mise en conformité au RGPD

par @Derriennic Associés

DERRIENNIC ASSOCIÉS

Conformité RGPD

#NewsDerriennicRGPD 12

Madame, Monsieur,

Avec le retour des beaux jours, quelles meilleure activité que de s'intéresser à l'actualité récente en matière de données à caractère personnel ?

Nous vous proposons, en ce mois de mars, une lettre RGPD composée des actualités suivantes :

- « *No-deal Brexit* » : no transfer ? ;
- Le renforcement de la coopération entre la CNIL et la DGCCRF pour faire face aux nouveaux enjeux numériques ;
- La reconnaissance du Japon comme assurant un niveau de protection adéquat par la Commission européenne ;
- Le droit d'accès : Nouvelle bête noire des responsables du traitement ?

« No-deal Brexit » : no transfer ?

Le CEPD a publié, le 12 février dernier, deux documents sur les conséquences d'un « no-deal Brexit ». L'un de ces documents évoque les transferts de données et l'autre, les sociétés ayant désigné l'autorité britannique comme autorité chef de file s'agissant de leurs BCR.

Suite au référendum sur le Brexit de juin 2016 et à la procédure enclenchée au niveau européen, la sortie du Royaume-Uni de l'Union européenne doit avoir lieu le 29 mars 2019 à minuit. Cela fera du Royaume-Uni un « pays tiers » au sens du RGPD, ce qui aura plusieurs conséquences.

S'agissant, tout d'abord, de la question du transfert des données vers le Royaume-Uni, le CEPD indique qu'en l'absence d'accord, il conviendra bel et bien de considérer le Royaume-Uni comme un pays tiers à partir du 30 mars prochain.

Dans une telle hypothèse, les outils suivants pourront permettre aux organismes d'encadrer les transferts de données personnelles vers le Royaume-Uni de façon appropriée :

- Les clauses contractuelles types ;
- Les clauses contractuelles spécifiques dites « ad-hoc » ;
- Les BCR ;
- Les codes de conduites et mécanismes de certification.

Il est à noter que le gouvernement britannique a communiqué sa volonté d'incorporer le RGPD au sein d'une loi nationale, ce qui laisse à penser que la Commission européenne serait susceptible de rendre, à l'avenir, une décision d'adéquation au sujet du Royaume-Uni.

Par ailleurs, le Brexit aura également un impact sur l'approbation, par l'autorité de contrôle britannique, des BCR, mécanisme prévue par l'article 47 du RGPD.

En effet, s'agissant des sociétés ayant désigné l'autorité britannique (l'ICO) comme autorité chef de file pour l'approbation de leur BCR, le CEPD rappelle que l'ICO n'aura plus de rôle à jouer pour ce qui est de ladite approbation.

Ainsi :

1° Les groupes ayant leur siège au Royaume-Uni souhaitant soumettre des BCR devront identifier l'autorité chef de file la plus appropriée au sein de l'Union européenne.

2° Les groupes ayant déjà soumis leur BCR à l'ICO devront également identifier une nouvelle autorité chef de file, qui prendra la main sur la procédure de validation et débutera une nouvelle procédure lors de la confirmation du « *no-deal Brexit* ». Si les BCR ont été soumises au CEPD, c'est ce dernier qui désignera la nouvelle autorité chef de file.

3° Les détenteurs de BCR validés par l'ICO devront, eux aussi, désigner une nouvelle autorité chef de file.

Documents :

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12-infonote-bcrs-brexit_en_0.pdf

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12-infonote-nodeal-brexit_en_0.pdf

https://www.gov.uk/government/publications/data-protection-if-theres-no-brexit-deal/data-protection-if-theres-no-brexit-deal

La CNIL et la DGCCRF renforcent leur coopération pour l'adapter aux nouveaux enjeux numériques

La DGCCRF et la CNIL ont annoncé aujourd'hui la signature d'un nouveau protocole de coopération. Afin de renforcer leur collaboration et l'adapter aux nouveaux enjeux numériques, les deux autorités ont renouvelé et mis à jour la convention qui les liait depuis 2011.

La DGCCRF et la CNIL ont décidé de se concentrer sur les axes suivants :

- mieux sensibiliser les consommateurs aux risques encourus lors de la communication de leurs données personnelles et diffuser les bonnes pratiques mises en œuvre par les professionnels ;
- faciliter l'échange d'informations relatives au non-respect du droit de la consommation et de la protection des données personnelles des consommateurs ;
- réaliser des contrôles communs ;
- porter conjointement des propositions d'actions au niveau européen ;
- mutualiser les expertises, notamment en ce qui concerne les outils d'enquête ;
- et partager leurs analyses sur les évolutions du cadre législatif et réglementaire en matière de protection des consommateurs et de leurs données personnelles.

Le Japon reconnu comme assurant un niveau de protection adéquat par la Commission

La Commission Européenne a annoncé que le Japon fait dorénavant parti des pays reconnus comme assurant un niveau de protection adéquat.

Désormais, une entreprise souhaitant transférer des données personnelles au Japon dans le cadre d'un traitement n'aura plus à adopter un mécanisme contractuel de type Règles d'Entreprise Contraignantes (BCR) ou Clauses Contractuelles Types.

Afin d'intégrer le cercle restreint des pays bénéficiant d'une telle « décision d'adéquation », le Japon a accordé aux citoyens européens des garanties additionnelles relativement à :

- la protection des données sensibles,
- aux conditions selon lesquelles leurs données peuvent être transférées ultérieurement depuis le Japon vers un autre pays tiers,
- ainsi qu'à l'exercice des droits individuels des citoyens européens en matière d'accès et de rectification.

La « décision d'adéquation » est entrée en vigueur le 23 janvier 2019

Le droit d'accès : Nouvelle bête noire des responsables du traitement ?

La loi « Informatique et libertés » a été votée en 1978 dans l'optique de protéger les individus contre les dérives potentielles de l'administration dans l'utilisation de l'informatique. Dans cet esprit, le législateur a soumis les détenteurs de fichiers à un certain nombre d'obligations et a donné aux personnes concernées de nouveaux droits, parmi lesquels : le droit d'accès. Près de quarante ans plus tard, on le retrouve dans le règlement (UE) n°2016/679 qui constitue le nouveau socle juridique en matière de protection des données (ci-après « RGPD »). Ce droit d'accès, en application de l'article 15, permet à la personne concernée d'obtenir d'un responsable du traitement la confirmation que des données personnelles la concernant sont ou non traitées par ce dernier. Il permet aussi d'avoir accès auxdites données, ainsi que d'en obtenir la copie.

Depuis le 25 mai 2018, date d'entrée en vigueur du RGPD, le droit d'accès connaît un regain d'intérêt. C'est ce qu'il ressort du dernier bilan publié par la Cnil, qui souligne une augmentation sensible des demandes. Les personnes exerçant leur droit d'accès n'ayant pas à justifier d'un motif légitime, il est difficile de déterminer précisément les raisons qui les poussent à solliciter la communication de leurs données personnelles, notamment lorsqu'il s'agit de salariés ou d'anciens salariés. Ces derniers pensent-ils pouvoir obtenir des informations auprès de leur employeur (ou ancien employeur) qu'ils n'auraient pas pu obtenir par un autre moyen ?

Si la personne concernée peut aisément, par l'exercice de ce droit, obtenir une multitude de données la concernant, il faut aussi souligner que ce droit n'est pas absolu et que le responsable du traitement peut, sous certaines conditions, ne pas y faire droit ou ne pas communiquer toutes les données dont il dispose.

Un droit au service de la personne concernée

A quoi sert-il ?

Le droit d'accès permet à la personne concernée d'interroger un organisme pour savoir s'il traite des données personnelles la concernant. C'est également le droit, en cas de réponse positive de ce dernier, d'obtenir un accès à ces données ainsi qu'à plusieurs informations dont : les finalités du traitement, les catégories de données traitées, les destinataires de ces données, leur durée de conservation. Enfin, la personne concernée est en droit de demander une copie des données traitées par le responsable du traitement. On l'aura compris, le droit d'accès permet à celui qui l'exerce de conserver une maîtrise de ses données, en identifiant les organismes qui traitent ses données et en contrôlant la licéité des traitements réalisés ainsi que l'exactitude desdites données. C'est d'ailleurs ce que le RGPD souligne dans son considérant (63) : « Une personne concernée devrait avoir le droit d'accéder aux données à caractère personnel qui ont été collectées à son sujet et d'exercer ce droit facilement et à des intervalles raisonnables, afin de prendre connaissance du traitement et d'en vérifier la licéité ».

Compte tenu de la diversité et de la nature des données que ce droit permet d'obtenir, il n'est pas étonnant qu'il soit de plus en plus utilisé par les personnes concernées, notamment dans le monde du travail. Il permet, en effet, à un salarié (ou un ancien salarié) d'obtenir de son employeur un

nombre considérable d'informations, comme toutes celles relatives à son recrutement, son historique de carrière, sa rémunération, l'évaluation de ses compétences professionnelles (entretiens annuels d'évaluation, notation), son dossier disciplinaire et tout élément ayant servi à prendre une décision à son égard (comme par exemple, une promotion, une augmentation, un changement d'affectation). Il pourrait également obtenir ses valeurs de classement annuel, mais aussi les informations relatives au « potentiel de carrière ». En revanche, la Cnil précise que l'employé n'a pas le droit d'accéder aux données concernant la situation personnelle d'un tiers, ni aux valeurs de classement annuel ou de potentiel de carrière prévisionnelle qui n'ont pas été utilisées pour prendre une décision le concernant.

La demande de droit d'accès

L'exercice du droit d'accès est simple. Il suffit pour la personne concernée d'identifier l'organisme et de lui adresser une demande. « Vous pouvez exercer votre demande de droit d'accès par divers moyens, souligne la Cnil : par voie électronique (formulaire, adresse mail, bouton de téléchargement, etc.) ou par courrier par exemple. Si votre demande est formulée par voie électronique, le responsable du traitement vous répondra par voie électronique, à moins que vous ne précisiez que vous souhaitez obtenir une réponse par un autre moyen (ex. papier) ».

Il n'est pas utile de joindre à la demande une copie de la pièce d'identité, dès lors que la personne est parfaitement identifiable par le destinataire. Si tel n'est pas le cas et que l'organisme a des doutes raisonnables sur l'identité du demandeur, ce dernier peut être invité à joindre tout document permettant de prouver son identité, notamment pour éviter les usurpations d'identité.

Le droit d'accès est gratuit. Le responsable du traitement serait toutefois légitime à facturer les « frais raisonnables liés au traitement [du] dossier » en cas par exemple, indique la Cnil, « de demande de copie supplémentaire ».

Le considérant (63) du RGPD précise que « lorsque le responsable du traitement traite une grande quantité de données relatives à la personne concernée, il devrait pouvoir demander à celle-ci de préciser, avant de lui fournir les informations, sur quelles données ou quelles opérations de traitement sa demande porte ».

Une réponse encadrée

L'organisme doit faciliter l'exercice du droit d'accès. Il ne peut pas refuser de donner suite à la demande, sauf à démontrer qu'il n'est pas en mesure, malgré la demande d'informations complémentaires, d'identifier la personne concernée. Il lui appartient de répondre à la demande « dans les meilleurs délais » et, en tout état de cause, « dans un délai d'un mois à compter de la réception de la demande ». Ce délai peut être prolongé de deux mois, si le responsable du traitement parvient à justifier qu'il n'est pas en mesure de tenir le délai d'un mois en raison de la complexité de la demande ou du nombre de demandes dont il fait l'objet. En tout état de cause, il doit informer la personne concernée du report. En ne respectant pas ces obligations, l'organisme serait susceptible d'être sanctionné par la Cnil, après avoir été saisie d'une plainte émanant de la personne concernée. Enfin, l'organisme doit respecter un certain formalisme en ce qu'il doit répondre « d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples ».

Une réponse sous contrainte judiciaire

En cas de refus non motivé et/ou infondé de l'organisme ou en cas de silence de ce dernier à une demande de droit d'accès, la personne

concernée peut utiliser les voies judiciaires pour contraindre le responsable du traitement de s'exécuter. Il est, en effet, possible de demander au juge des référés d'ordonner au destinataire d'une demande de droit d'accès de communiquer les données personnelles à la personne concernée qui en fait la demande. Ainsi, dans une affaire dans laquelle la cliente d'une banque soupçonnait une utilisation frauduleuse en ligne de ses comptes bancaires, celle-ci avait demandé au juge des référés qu'il soit fait injonction à la banque, sur le fondement du droit d'accès, de lui communiquer les logs de connexion de ses comptes. Par une ordonnance du 17 juillet 2014, le président du tribunal de grande instance de Paris a fait droit à sa demande : « Qu'en sollicitant la communication des logs de connexion de ses comptes en ligne, Mme M. interroge sa banque sur l'accès à ses propres comptes et, ainsi, sur des données qui lui sont personnelles, et l'éventualité que cette communication révèlerait une utilisation frauduleuse ne saurait la priver du droit que lui confère l'article 39-1 de la loi du 6 janvier 1978 d'obtenir que lui soient communiquées les données personnelles qu'elle sollicite. »

Il convient de relever, par ailleurs, que l'article 39 de la loi « Informatique et libertés » telle que modifiée par l'ordonnance n° 2018-1125 du 12 décembre 2018 prévoit que : « en cas de risque de dissimulation ou de disparition des données à caractère personnel, le juge compétent peut ordonner, y compris en référé, toutes mesures de nature à éviter cette dissimulation ou cette disparition. » Parmi ces mesures, la personne concernée pourrait donc demander au juge des référés qu'il ordonne au responsable du traitement de lui communiquer une copie des données, afin de garantir leur conservation.

Un droit qui n'est pas absolu

Le respect des « droits et libertés d'autrui »

Il ressort des termes de l'article 15 du RGPD que le droit d'obtenir une copie des données personnelles ne doit pas porter atteinte « aux droits et libertés d'autrui », y compris « au secret des affaires ou à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel ». C'est ce que confirme la Cnil en précisant, au sujet du « droit des tiers », que seules les données de la personne concernée « peuvent être communiquées au titre du droit d'accès ». Autrement dit, il conviendrait, avant de remettre à la personne concernée la copie d'un document (compte-rendu, courriel, etc.) dans lequel son nom apparaîtrait d'anonymiser les mentions dans lesquelles apparaîtrait le nom d'un tiers. A moins que le responsable du traitement ne puisse, au motif que le document concernerait plusieurs personnes nommément désignées, invoquer l'atteinte au droit des tiers pour justifier un refus de communication. Une telle position semble quelque peu excessive…

En tout état de cause, cette limite au droit d'accès ne porte que sur le droit à la copie. Elle ne devrait donc pas être opposée à la personne concernée qui demanderait au responsable du traitement s'il traite des données personnelles la concernant.

Le détournement de finalité

Comme indiqué supra, le législateur européen semble avoir réservé le droit d'accès aux seules personnes concernées qui souhaitent « prendre connaissance du traitement et d'en vérifier la licéité » (considérant 63). Cela signifierait-il qu'une personne exerçant son droit avec une autre motivation que celle d'apprécier la licéité d'un traitement ne serait pas fondée à faire jouer son droit d'accès ? Non, si l'on en croit la position prise par la Cnil dans une affaire dans laquelle un ancien

salarié avait exercé son droit d'accès pour une toute autre raison que le contrôle de la licéité d'un traitement. En effet, le salarié avait exercé ce droit dans le seul objectif d'obtenir de son ancien employeur des données lui permettant d'établir que l'accident de circulation dont il avait fait l'objet était survenu durant sa période d'emploi. En récupérant ses données de géolocalisation, l'ancien salarié espérait ainsi faire reconnaître par le Tribunal des affaires sociales de sécurité sociale le caractère d'accident du travail. Sa demande ayant été rejetée par son ancien employeur, le salarié avait déposé une plainte à la Cnil. Celle-ci a considéré que l'employeur, en refusant de faire droit à la demande de droit d'accès, avait manqué à son obligation.

Cette décision montre que les motifs importent peu et que toute demande de droit d'accès droit être honorée, sauf, bien entendu, à ce que le responsable du traitement puisse invoquer une atteinte aux « droits et libertés d'autrui ».

La question de l'abus de droit

Dans une affaire récente, la question de l'abus de droit a été posée. Il s'agissait d'un expert-comptable stagiaire, qui avait échoué à quatre reprises à l'examen « Comptabilité de la finance stratégique et de la gestion » et qui cherchait à contester les résultats. Ne parvenant pas à obtenir sa copie d'examen, il adressa à l'ordre des experts-comptables une demande de droit d'accès. L'affaire a été portée par la Cour suprême irlandaise devant le Cour de justice de l'Union européenne (CJUE). Après avoir retenu que la copie d'examen attribuée à un candidat et que les éventuelles annotations des examinateurs qu'elle comporte constituent des données personnelles, l'avocat général s'est interrogé sur la question de l'objet du droit d'accès et celle de l'abus de droit. Si celui-ci indique que l'exercice du droit d'accès pourrait, dans un certains cas, être jugé abusif, il affirme que ce n'est pas le cas en l'espèce. Tout d'abord, il se démarque de la position du commissaire à la protection des données et de l'Irlande, selon laquelle l'objectif de la directive sur la protection des données ne serait pas atteint si un droit d'accès au titre de la législation sur la protection des données permettait de contourner les règles relatives à la procédure d'examen. L'avocat général affirme ensuite : « Nous ne voyons pas en quoi consisterait l'avantage indu dont bénéficierait le candidat qui pourrait consulter sa copie en exerçant son droit d'accès. En particulier, le fait que le droit d'accès permet d'obtenir des informations qui n'auraient pas pu être obtenues par une autre voie ne saurait être considéré comme un abus. En effet, si l'accès aux informations à caractère personnel existait déjà, il n'aurait pas été nécessaire d'instaurer un droit d'accès au titre de la législation sur la protection des données. Ce droit d'accès a au contraire pour fonction de permettre à l'intéressé de consulter ses propres données – sous réserve des exceptions visées à l'article 13 de la directive sur la protection des données – lorsqu'il ne dispose pas d'un droit d'accès à un autre titre. »

En conclusion, si le droit d'accès n'est pas absolu en ce qu'il ne doit pas porter atteinte aux droits et libertés d'autrui, il n'est pas pour autant enfermé dans une finalité déterminée. Il peut même être exercé pour obtenir des informations qui n'auraient pas pu être obtenues par la personne concernée par une voie traditionnelle. Bref, on n'a pas fini d'entendre parler de ce droit…

Expertises, février 2019,

Alexandre Fiévée et Maxime Cordier.