LES RH FACE AU RGPD : LE DROIT D'ACCES AUX DONNEES A CARACTERE PERSONNEL ET LE TRANSFERT DES DONNEES A L'ETRANGER

Blandine ALLIX
Avocat Associé
Flichy Grangé Avocats

Fabien CROSNIER
Avocat Counsel
Flichy Grangé Avocats

Des salariés davantage sensibilisés aux enjeux RGPD, et mieux conseillés. Un monde du travail beaucoup plus ouvert aux échanges avec l'international. Des quantités de données transitant et stockées chaque jour dans nos systèmes d'information, circulant plus vite, plus loin aussi. Les RH sont de plus en plus confrontés aux questions de droit d'accès et de transferts de données dans leur activité quotidienne.

Un état des lieux est donc nécessaire.

Le quotidien des RH de plus en plus bousculé par les enjeux RGPD

Les employeurs sont de plus en plus confrontés à des demandes de droit d'accès aux données à caractère personnel, droit prévu par l'article 15 du Règlement général sur la protection des données (RGPD).

Ces demandes sont exercées le plus souvent par d'anciens salariés dans l'optique de préparer un contentieux à l'encontre de leur employeur.

En parallèle, un grand nombre de situations dans la gestion quotidienne des Ressources Humaines peut conduire, consciemment ou non, à transférer des données vers l'étranger (recherche de reclassement de salariés à l'étranger, enquête interne, stockage de données sur un cloud...). Or, les précautions à prendre peuvent être plus ou moins contraignantes selon l'État vers lequel ces données transitent ou sont exportées.

Compte tenu des sanctions – sévères – applicables, il est indispensable pour les RH d'appréhender ces questions pour les gérer au mieux.

L'état des lieux sur le droit d'accès

Qu'est-ce que le droit d'accès aux données à caractère personnel au sens du RGPD ?

Le droit d'accès, qui était déjà prévu en France par la loi Informatique et Libertés de 1978, est défini à l'article 15 du RGPD (règlt UE 2016/679 du 27 avril 2016) qui précise que « 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 (…) ».

Le droit d'accès est donc triple. Il s'agit :

- d'une part du droit d'obtenir la confirmation que les données de la personne sont traitées ou non ;
- d'autre part du droit d'accès auxdites données à caractère personnel ;

- enfin du droit d'obtenir les informations listées à l'article 15 (finalité du traitement, catégories de données concernées, destinataires des données, droit d'introduire une réclamation auprès des autorités compétentes, etc.).

La notion de données à caractère personnel est pour sa part définie à l'article 4 du RGPD. Elle est assez large puisqu'il s'agit de « toute information se rapportant à une personne physique identifiée ou identifiable ». L'article 4 précise qu'« est réputée être une "personne physique identifiable" une personne qui peut être identifiée directement ou indirectement notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

La CNIL a précisé, dans une publication du 9 mai 2019 ayant pour objet « la demande d'accès au dossier professionnel », que cela vise notamment l'identité (nom, prénom), l'adresse, le numéro de sécurité sociale, la date de naissance, la nationalité, l'état civil, l'expérience professionnelle, la formation, la nationalité, l'évaluation des aptitudes et compétences, le dossier disciplinaire, les données issues d'un dispositif de géolocalisation ou de badges d'accès, le salaire, l'élément ayant servi à prendre une décision à son égard (promotion, augmentation, etc.).

Quelle est la finalité du droit d'accès ?

L'article 63 du RGPD précise que le droit d'accès a pour objet de « prendre connaissance du traitement et d'en vérifier la licéité ».

Le Comité européen de protection des données (CEPD), qui rassemble « les CNIL » des pays de l'Union Européenne, précise dans ses lignes directrices sur le droit d'accès de janvier 2022 qu'il a pour objet, pour la personne qui l'exerce, de « permettre (…) d'avoir le contrôle des données à caractère personnel le concernant », « comprendre comment ses données sont traitées ainsi que les conséquences du traitement et de vérifier l'exactitude des données traitées ».

Enfin, dans son avis du 5 janvier 2022, la CNIL précise qu'il permet « notamment de contrôler l'exactitude des données et au besoin de les faire rectifier ou effacer ».

Quelles sont les sanctions en cas d'atteinte au droit d'accès ?

Des sanctions sont prévues à la fois par le Code pénal et le RGPD.

En effet, l'article R. 625-11 du Code pénal sanctionne par une contravention de 5e classe (soit actuellement 1 500 €) notamment le fait, pour le responsable d'un traitement automatisé de données à caractère personnel, de ne pas répondre à une demande de droit d'accès.

Le RGPD prévoit pour sa part une sanction financière qui peut aller jusqu'à 20 millions d'euros ou 4 % du CA annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu.

Le droit d'accès est-il indépendant des autres modalités pouvant être mises en œuvre par un salarié pour obtenir de son employeur des pièces ?

Le droit d'accès est un droit indépendant.

Cela signifie qu'un employeur responsable de traitement ne peut pas refuser de faire droit à une demande de droit d'accès au motif qu'il a d'ores et déjà communiqué les éléments au salarié dans le cadre d'une communication de pièces dans le contentieux qui les oppose.

Le Conseil d'État l'a confirmé en jugeant que le fait d'avoir communiqué les données dans le cadre d'un litige à la suite d'une sommation de communiquer n'exonère pas de les communiquer à nouveau en cas de demande de droit d'accès (CE 20 octobre 2010, n° 327916).

Le raisonnement doit être le même si les données ont été transmises en exécution d'une décision de justice ordonnant leur communication dans le cadre de l'article 145 du Code de procédure civile.

Est-il possible d'opposer au salarié le fait que sa demande de droit d'accès vise en réalité à préparer un contentieux, détournant ainsi le droit d'accès de sa finalité ?

La CNIL ayant précisé que le droit d'accès a pour objet « notamment de contrôler l'exactitude des données et au besoin de les faire rectifier ou effacer », il serait tentant de considérer que l'exercice par un salarié (ou un ancien salarié) de son droit d'accès dans l'unique but de préparer un contentieux à l'encontre de son employeur détourne la finalité du droit d'accès et qu'il n'y a donc pas lieu d'y faire droit. L'autorité britannique de protection des données a

d'ailleurs considéré qu'il est possible de refuser de faire droit à une demande si la requête est explicitement ou implicitement mal intentionnée.

Cela n'est cependant pas la position du CEPD qui considère que le responsable de traitement n'a pas à juger la raison pour laquelle la personne exerce son droit d'accès. En effet, dans ses lignes directrices sur le droit d'accès de janvier 2022, le CEPD précise expressément que « le responsable de traitement ne devrait pas refuser l'accès au motif que les données pourraient être utilisées par la personne concernée pour se défendre devant un tribunal en cas de licenciement (…) ».

Par conséquent, il n'est pas possible de refuser de faire droit à une demande de droit d'accès au motif que son objectif est uniquement probatoire.

Y a-t-il des limites à ce droit d'accès ?

Le RGPD prévoit plusieurs limites au droit d'accès.

❶ Tout d'abord, la communication des données au salarié qui exerce une demande de droit d'accès suppose que les données à caractère personnel existent.

Aussi, si les données ne sont plus conservées en application de la durée de conservation prévue par l'entreprise ou ont été effacées à la demande du salarié, il peut être indiqué, dans la réponse à la demande de droit d'accès, que les données n'existent plus.

❷ Ensuite, le RGPD précise qu'il est possible de ne pas donner suite à une demande d'accès lorsque celle-ci est « manifestement infondée ou excessive, notamment en raison de son caractère répétitif ».

Selon le CEPD, une demande est considérée comme manifestement infondée lorsque l'information demandée ne constitue pas une donnée personnelle ou ne fait pas l'objet d'un traitement ou n'est pas relative au demandeur mais se rapporte exclusivement à des tiers.

S'agissant de la demande « manifestement excessive, notamment en raison de son caractère répétitif », le CEPD a précisé que ce critère s'apprécie en prenant en compte la périodicité des demandes, les évolutions du traitement entre les demandes (plus les changements sont fréquents, plus les personnes sont fondées à fréquemment accéder aux informations), le niveau de sensibilité des informations en cause. Par ailleurs, la CNIL a précisé que le fait pour une personne de demander la copie de données dont elle dispose déjà, ne peut systématiquement être qualifié d'excessif.

❸ Enfin, l'article 15 du RGPD précise que le droit d'accès ne doit pas porter « atteinte aux droits et libertés d'autrui ». Le considérant 63 du RGPD précise que le droit d'accès « ne devrait pas porter atteinte aux droits ou libertés d'autrui, y compris au secret des affaires ou à la propriété intellectuelle, notamment au droit d'auteur protégeant le logiciel. »

Le secret des affaires, la propriété intellectuelle, le secret des correspondances, la vie privée d'autrui sont, par conséquent, des limites au droit d'accès.

L'employeur qui reçoit une demande d'accès aux données à caractère personnel d'un salarié doit-il suivre certaines formalités pour y répondre ?

Le RGPD prévoit une procédure assez contraignante.

❶ D'une part, l'article 12 du RGPD prévoit un **délai de réponse**. Concrètement, il laisse un mois maximum pour répondre à une demande d'accès.

Il prévoit néanmoins la possibilité de prolonger ce délai de 2 mois maximum compte tenu de la complexité de la demande et du nombre de demandes. Si le responsable de traitement souhaite user de cette dérogation pour porter le délai à trois mois, il doit en informer par écrit la personne concernée dans le délai d'1 mois précité, en expliquant le motif du report.

❷ L'article 12 du RGPD est, d'autre part, **rigoureux sur la forme de la réponse**. Il exige que l'information soit concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples.

En outre, l'information doit être par écrit ou par d'autres moyens, y compris par voie électronique lorsque c'est approprié.

Par ailleurs, elle doit être faite de manière sécurisée. Cela signifie, sur ce dernier point, qu'il est prudent de ne pas se contenter d'envoyer les données à caractère personnel au salarié par e-mail, sans plus de sécurité. L'idéal est de les placer dans une box sécurisée.

❸ Enfin, le RGPD prévoit qu'en cas d'**impossibilité/refus de communiquer**, il convient d'informer la personne des suites sous 1 mois maximum, d'expliquer les motifs de son inaction et enfin de l'informer de la possibilité d'introduire une réclamation auprès de la CNIL et de former un recours juridictionnel.

Quelles sont les règles à respecter si le salarié demande la communication de tous les documents de son dossier professionnel ?

Dans sa fiche de mai 2019 portant sur « L'accès à son dossier professionnel », la CNIL indiquait que « le salarié peut obtenir l'accès et la communication de l'ensemble des données le concernant, qu'elles soient conservées sur support informatique ou papier. Il a ainsi le droit d'accéder aux données relatives à son recrutement, son historique de carrière, l'évaluation de ses compétences professionnelles (entretiens annuels d'évaluation, notation), ses demandes de formation et les éventuelles évaluations de celles-ci, son dossier disciplinaire, l'utilisation de son badge de contrôle d'accès aux locaux, ses données issues d'un dispositif de géolocalisation, tout élément ayant servi à prendre une décision à son égard (une promotion, une augmentation, un changement d'affectation, etc.). Il peut s'agir des valeurs de classement annuel, parfois appelées « ranking », ou de potentiel de carrière, etc. ».

Si elle rappelait que le droit d'accès est un « droit personnel qui ne doit pas porter atteinte aux droits des tiers » et qu'il ne peut s'exercer à l'égard des données protégées par le secret des affaires, la propriété intellectuelle ou encore le secret des correspondances, elle mentionnait que « dans le cas d'un droit d'accès portant sur un rapport circonstancié établi à la suite d'un dysfonctionnement, l'identité des personnes mentionnées dans le document, autres que la personne exerçant son droit, devra être occultée ».

La CNIL laissait ainsi planer le doute sur la possibilité pour un salarié d'obtenir communication de l'intégralité d'un document de son dossier professionnel (dont la CNIL donne une définition large) avec la seule réserve que les données relatives aux tiers soient occultées.

Cependant, dans une note publiée sur son site internet le 5 janvier 2022, la CNIL a indiqué très clairement que « le droit d'accès porte uniquement sur les données personnelles et non pas sur des documents : une personne ne peut donc pas réclamer la communication d'un document sur le fondement du droit d'accès ».

Ainsi, le droit d'accès ne permet pas au salarié qui l'exerce d'exiger la communication d'une copie des documents de son dossier professionnel. Néanmoins, il peut être plus aisé pour le responsable de traitement de communiquer une copie, l'extraction de toutes les données à caractère personnel du salarié pour les communiquer sur un autre support pouvant être un exercice fastidieux.

Et qu'en est-il des courriels ?

Des demandes d'accès avec souvent un objectif caché

La plupart du temps, les demandes de droit d'accès formées par les salariés ou anciens salariés sont assez détaillées. Elles précisent notamment que doit être communiqué l'ensemble des courriels reçus ou adressés par le salarié ainsi que tous les autres courriels pouvant contenir des données à caractère personnel le concernant.

L'objectif caché est, souvent, d'obtenir les courriels que le salarié n'a pas eu le temps de conserver à la suite de son licenciement qui vont lui permettre d'apporter la preuve de certaines demandes aux prud'hommes comme une demande de rappel de salaire pour heures supplémentaires.

La méthode proposée par la CNIL au regard du secret des correspondances

Dans la mesure où l'une des limites du droit d'accès est le secret des correspondances, les employeurs s'interrogent régulièrement sur l'obligation de communiquer tous les courriels, à supposer qu'ils aient été conservés, reçus ou expédiés par le salarié de sa messagerie professionnelle ainsi que ceux échangés en interne qui évoquent le salarié mais dont ce dernier n'est ni expéditeur, ni destinataire.

Dans sa note du 5 janvier 2022, la CNIL propose une méthode en distinguant deux situations.

❶ Si le demandeur du droit d'accès est destinataire ou expéditeur des courriels professionnels, leur communication à l'intéressé est, selon la CNIL, en principe présumée respectueuse des droits des tiers.

Toutefois, si leur communication peut représenter un risque pour les droits des tiers, la CNIL recommande d'essayer, dans un premier temps, de supprimer, d'anonymiser ou de pseudonymiser les données concernant des tiers ou portant atteinte à un secret. Si ces mesures s'avèrent insuffisantes, la CNIL recommande, dans un second temps, de refuser de faire droit à la demande d'accès, en motivant et justifiant sa décision auprès de la personne concernée.

❷ Si le demandeur n'est pas destinataire ou expéditeur des courriels professionnels mais qu'il s'agit de courriels qui évoquent l'intéressé, la CNIL précise que dans cette hypothèse, l'employeur doit trouver un équilibre entre la satisfaction du droit d'accès du salarié et le respect des droits et libertés des autres salariés (notamment le secret des correspondances). Aussi, selon la CNIL, l'employeur doit :

- dans un premier temps, s'assurer que les moyens à mettre en œuvre pour identifier les courriels demandés n'entraînent pas d'atteinte disproportionnée aux droits des salariés, ce qui permet alors de refuser de communiquer ces e-mails si leur obtention suppose le scan de l'ensemble des messageries et que le demandeur refuse de préciser sa demande ;

- dans un second temps, l'employeur doit étudier le contenu des courriels demandés et apprécier la portée de l'atteinte aux droits des tiers en faisant une analyse au cas par cas.

Une méthode « CNIL » qui conduit à un travail de tri colossal pour l'employeur

Force est de constater que cette méthode préconisée par la CNIL amène l'employeur à faire un travail de tri colossal car il l'oblige :

- dans un premier temps, à récupérer, s'ils existent encore, tous les courriels reçus par le salarié dans sa messagerie professionnelle depuis son embauche jusqu'à son départ, tous les courriels expédiés par lui sur cette même période ainsi que – sauf si leur obtention suppose le scan de l'ensemble des messageries de l'entreprise – tous les courriels échangés en interne qui évoquent le salarié ; il est bien évident que plus le salarié a de l'ancienneté, plus le volume de ces e-mails sera astronomique ;

- dans un second temps, à prendre connaissance du contenu de chacun de ces courriels (à moins que l'objet de ces courriels soit identifié comme personnel) afin de s'assurer qu'ils ne contiennent pas de données portant atteinte aux droits et libertés des tiers, ce qui serait le cas si des données relevaient par exemple du secret des affaires de l'entreprise ou de la vie privée d'autrui (comme des données de santé d'un autre salarié) ; cela suppose donc, pour l'employeur, de les examiner un par un et de caviarder toutes les données portant atteinte aux droits et libertés d'autrui.

Au-delà du travail de tri, une méthode qui interroge

Surtout, cette méthode de la CNIL, en ce qu'elle n'écarte pas automatiquement les courriels échangés en interne qui évoquent le salarié mais dont ce dernier n'est ni expéditeur, ni destinataire, interroge.

En effet, l'envoi d'un message électronique de personne à personne via une messagerie professionnelle électronique accessible uniquement par un mot de passe, est une correspondance privée (cf. notamment la position du TGI de Paris dans un jugement du 2 novembre 2000, confirmé sur ce point par la cour d'appel de Paris par arrêt du 17 décembre 2001, RG n° 00/07565).

La CNIL, sur la notion de correspondances privées à propos de l'article 68 de la loi 2016-1321 du 7 octobre 2016 pour une République numérique, régissant le secret des correspondances privées, a elle-même qualifié de correspondance privée « tout message exclusivement destiné à une ou plusieurs personnes physiques ou morales, déterminées et individualisées. L'exemple le plus concret est le courriel échangé entre deux ou plusieurs correspondants, depuis un service de messagerie ».

La seule « dérogation » apportée par la jurisprudence au secret des e-mails échangés en interne via la messagerie professionnelle concerne l'employeur. En effet, dans la mesure où ces courriels sont échangés via des outils professionnels, propriété de l'employeur, ils sont, à l'égard de ce dernier, présumés professionnels ce qui l'autorise à y avoir accès sauf s'ils ont été identifiés par le salarié comme étant personnels. Mais cette dérogation ne s'applique qu'à l'employeur : elle n'a jamais – fort heureusement – été étendue aux autres salariés de l'entreprise qui ne se sont jamais vu conférer la possibilité d'avoir connaissance des échanges internes de leurs collègues.

Dans ce contexte, on ne peut que s'étonner que la CNIL n'ait pas pris une position beaucoup plus catégorique et n'ait pas écarté automatiquement du droit d'accès les e-mails internes évoquant le salarié mais dont il n'est ni expéditeur, ni destinataire. Même s'ils sont susceptibles de contenir des données à caractère personnel concernant le salarié qui exerce son droit d'accès, ces courriels devraient relever du secret des correspondances qui est une limite fondamentale au droit d'accès.

Quelles conséquences pour l'employeur responsable de traitement ? L'anticipation

Le droit d'accès a des conséquences lourdes pour l'employeur qui se retrouve non seulement face une demande qui peut être faite à tout moment sans avoir à se justifier et quelle que soit la finalité, mais surtout à devoir, dans un temps extrêmement court, d'une part récupérer tous les éléments dans lesquels des données à caractère personnel du salarié peuvent figurer, d'autre part trier un volume d'éléments conséquents et au besoin caviarder des données pour ne pas porter atteinte aux droits et libertés des tiers.

L'employeur responsable de traitement doit donc, avant même de recevoir des demandes de droit d'accès, s'organiser en amont pour ne pas être pris au dépourvu.

Connaître ses traitements et sa politique interne en matière de traitement de données (notamment sur les durées de conservation) est essentiel. Cela n'est cependant pas suffisant.

Il semble indispensable de définir en amont une procédure interne de gestion des demandes de droit d'accès, validée par la Direction, répondant notamment aux questions suivantes :

- **qui fait quoi ?** Dans ce cadre, différentes personnes peuvent être désignées en interne selon le rôle attribué : un « chef de projet » – le DRH ? le Directeur juridique ? le DPO (délégué à la protection des données) ? – en charge de superviser le traitement de la demande de droit d'accès, une personne dans le service IT en charge de récupérer les données, des collaborateurs du service juridique ou des ressources humaines en charge de faire le tri des données et le caviardage ;

- **quelle attitude** à adopter sur le contenu des données à communiquer au regard notamment du secret des affaires et du secret des correspondances ? L'idée est de définir une ligne de conduite, notamment sur les courriels ;

- **quelles modalités** sécurisées de transmission des données (accès à une box ?) doit-on mettre en œuvre ?

Cette anticipation permettra au responsable de traitement qu'est l'employeur d'être organisé et réactif. Elle permettra aussi de donner des réponses harmonisées aux différentes demandes de droit d'accès.

L'état des lieux sur les transferts de données à l'étranger en matière RH

Qu'entend-on par « transfert » de données personnelles ?

Le RGPD ne précise pas ce qu'il faut comprendre par « transfert » de données personnelles.

Or, l'enjeu est considérable car tout transfert de données personnelles, quand il se fait vers un État extérieur à l'Espace Économique Européen, nécessite de mettre en place des mesures et vérifications parfois très contraignantes.

Dans le silence du RGPD, le Comité européen de la protection des données (CEPD), organe qui regroupe en quelque sorte l'ensemble des « CNIL » européennes, a donné une définition des « transferts » de données dans des lignes directrices 05/2021 du 18 novembre 2021 (actualisées le 14 février 2023).

Dans ses lignes directrices, le CEPD définit un « transfert » comme le fait, pour un responsable de traitement ou un sous-traitant assujetti au RGPD (« l'exportateur de données »), de transmettre des données personnelles ou de les rendre accessibles à un responsable de traitement ou à un sous-traitant établi dans un pays tiers à l'Espace Économique Européen (EEE), voire à une organisation internationale (« l'importateur de données »), et ce peu important que cet importateur soit lui-même assujetti ou non au RGPD.

Pour le CEPD, un transfert peut ainsi prendre la forme d'un simple accès à distance, par exemple en cas de stockage de données sur un cloud hébergé en dehors de l'EEE. Par ailleurs, l'appartenance de l'exportateur et de l'importateur de données à un même groupe de sociétés n'exclut pas qu'on soit en présence d'un « transfert » de données au sens du RGPD.

En revanche, le CEPD (et la CNIL adopte la même position dans le Guide pratique de l'AITD adopté le 31 janvier 2025) exclut tout transfert dans la configuration particulière d'un salarié en voyage d'affaires qui accède lui-même à

distance avec son ordinateur, depuis un pays tiers, à des données personnelles stockées dans le système d'informations de son employeur établi en Europe.

En fin de compte, la notion de « transfert » au sens du RGPD peut ainsi recouvrir une large palette de situations : télétravail durable depuis l'étranger, audits sociaux, externalisation de la paye, envoi d'un salarié en formation à l'étranger, mais aussi mobilité intra-groupe ou recherche de reclassement nécessitant de transmettre le CV et/ou des informations sur l'état civil du salarié, ou encore enquête interne,…

Y a-t-il des différences selon que des données personnelles sont destinées à être transférées à l'intérieur ou en dehors de l'Espace Économique Européen ?

Le régime juridique des transferts de données diffère considérablement selon que l'État dans lequel des données doivent être transférées, est établi :

- sur le territoire de l'Espace Économique Européen (« EEE ») à savoir l'Union Européenne, l'Islande, la Norvège et le Liechtenstein ;
- ou bien à l'extérieur de cet espace (on parle alors de « pays tiers »).

Dans l'EEE, le principe de libre circulation des données personnelles s'applique.

En revanche, lorsque des données doivent circuler vers un pays tiers, un corps de règles beaucoup plus contraignantes, organisé au chapitre V du RGPD, s'applique. Le transfert de données ne peut alors être mis en œuvre qu'au titre d'un des « outils de transfert » énumérés par le RGPD, à savoir au titre d'une décision d'adéquation couvrant l'État où se situe l'importateur de données, ou, à défaut, au titre de « garanties appropriées » ou d'une dérogation exceptionnellement ouverte par le RGPD.

Y a-t-il des règles « de droit commun » à respecter en tout état de cause quel que soit l'État vers lequel des données personnelles sont transférées ?

Le RGPD prévoit un certain nombre d'obligations « de droit commun » ayant vocation à s'appliquer en tout état de cause, c'est-à-dire que le transfert intervienne vers l'EEE ou vers un pays tiers, et, en cas de transfert vers un pays tiers, quelle que soit la base juridique du transfert (décision d'adéquation, ou garanties appropriées, ou transfert dérogatoire).

Après tout en effet, un « transfert » de données reste une variété de « traitement » de données personnelles (RGPD, art. 4). Et, à ce titre, il doit respecter les principes et obligations prévus par ailleurs pour tout traitement de données personnelles.

Au nombre de ces obligations applicables « en tout état de cause », on trouve par exemple :

- l'obligation de délivrer à la personne concernée par le transfert de données, un certain nombre d'informations couvrant les points énumérés aux articles 13 ou 14 du RGPD ;
- l'obligation de mettre à jour le registre des activités des traitements de l'entreprise en l'enrichissant des informations pertinentes (RGPD, art. 30) ;
- l'obligation de mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté contre les risques de violation de données (pseudonymisation, chiffrement, test,...) (RGPD, art. 32).

Cela signifie qu'à partir du moment où un salarié se retrouve dans une situation où il peut avoir à traiter des données personnelles depuis l'étranger (télétravail, mission temporaire, détachement,…), l'employeur doit s'interroger sur (et donc vérifier) le niveau de risque d'atteinte à ses systèmes d'information pour évaluer s'il y a lieu de mettre en place des mesures de protection adaptées.

- le cas échéant et s'il y a lieu : l'obligation de procéder à une analyse d'impact avant toute mise en œuvre d'un traitement présentant un risque élevé pour les droits et libertés (RGPD, art. 35).

En fonction également du type de traitement de données qu'il souhaite mettre en œuvre, l'employeur devra aussi peut-être informer son CSE au titre de l'article L. 2312-38 du code du travail (information du CSE préalablement à l'introduction ou à la modification de traitements automatisés de gestion du personnel), voire même le consulter au titre de sa compétence générale s'il est susceptible d'en résulter une évolution des conditions d'emploi ou de travail.

Quelles sont les spécificités des transferts de données vers des États tiers à l'Espace Économique Européen ?

L'article 44 du RGPD pose le principe selon lequel tout transfert de données vers un pays tiers ne peut intervenir qu'à condition que les conditions du transfert ne compromettent pas le « niveau » de protection des personnes physiques garanti par le RGPD.

Pour s'en assurer, le chapitre V du RGPD prévoit que des données personnelles ne peuvent être régulièrement transférées vers un pays tiers qu'au titre d'un des trois fondements juridiques qu'il énumère.

❶ Tout d'abord, si le pays tiers vers lequel des données sont transférées est couvert par une décision de la Commission européenne dite « d'adéquation » (constatant que cet État assure un niveau de protection adéquat), le transfert ne peut être mis en œuvre qu'au titre de (et conformément à) cette décision d'adéquation (transferts dits « de l'article 45 » du RGPD).

❷ À défaut, si l'État de destination n'est pas couvert par une décision d'adéquation, le transfert ne peut être mis en œuvre qu'à des conditions beaucoup plus contraignantes, en l'occurrence moyennant la mise en place de « garanties appropriées » (pour l'essentiel, cela veut dire qu'il faut alors conclure un contrat de transfert de données entre l'importateur et l'exportateur de données) (transferts dits « de l'article 46 » du RGPD) ;

❸ En dernier ressort, un transfert vers un pays tiers non-adéquat est exceptionnellement possible dans certains cas dérogatoires (transferts dits « de l'article 49 » du RGPD).

Ces trois outils de transfert sont hiérarchisés : ce n'est qu'à défaut de décision d'adéquation couvrant le pays tiers destinataire que « des garanties appropriées » peuvent (et doivent) être mises en place, sauf à pouvoir se raccrocher aux dérogations ouvertes par l'article 49 du RGPD.

Que se passe-t-il si un exportateur de données veut transférer des données vers un pays tiers à l'égard duquel la Commission européenne a adopté une décision d'adéquation ?

Le premier niveau de vérification à effectuer en présence d'un transfert de données vers un pays tiers, consiste à contrôler si ce dernier est couvert par une décision d'adéquation (État dit « adéquat »), en consultant pour ce faire le site internet de la Commission européenne.

Une décision d'adéquation est un acte pris par la Commission européenne constatant que l'État en question assure une protection des données personnelles substantiellement équivalente à celle issue du RGPD lu à la lumière de la Charte des droits fondamentaux de l'UE (CJUE 16 juillet 2020, aff. C-311/18, « Schrems II », § 94).

Si le pays de destination est couvert par une telle décision d'adéquation, le transfert peut être mis en œuvre aux conditions prévues par cette décision d'adéquation (outre les obligations de droit commun du RGPD décrites plus haut et qui s'appliquent en tout état de cause).

Il faut toujours être vigilant à la manière dont est rédigée la décision d'adéquation car celle-ci n'a pas toujours une portée générale et absolue. La rédaction varie d'un État à l'autre : elle peut très bien n'avoir qu'un champ d'application limité (en excluant notamment certains secteurs d'activité ou certains destinataires de données ou certains types de données personnelles) et/ou conditionner la mise en œuvre du transfert à certaines conditions.

Exemple

S'agissant de la décision d'adéquation vers les États-Unis adoptée par la Commission européenne le 10 novembre 2023, celle-ci ne couvre que les transferts de données vers des entités américaines qui se sont engagées, par un mécanisme d'auto-certification renouvelable annuellement, à respecter un certain cadre réglementaire (l'« EU-US Data Privacy Framework » dit « DPF »), et dont la liste est gérée par le Département du Commerce américain. On parle alors d'organismes « certifiés ».

Cela signifie que si le transfert envisagé intervient en dehors du champ recouvert par la décision d'adéquation, il faudra mettre en place des « garanties appropriées » conformément à l'article 46 du RGPD (sauf à pouvoir se raccrocher aux dérogations exceptionnellement permises par l'article 49 du RGPD).

A ce jour toutefois, seule une minorité d'États est couverte par une décision d'adéquation (Andorre, Argentine, Canada, Îles Féroé, Guernesey, Israël, Île de Man, Japon, Jersey, Nouvelle-Zélande, République de Corée, Suisse, Royaume-Uni, Uruguay et, pour les organismes « certifiés », USA).

Et s'il n'existe aucune décision d'adéquation couvrant l'État vers lequel des données doivent être transférées ?

En l'absence de décision d'adéquation couvrant l'État destinataire des données, un transfert reste (théoriquement) possible à des conditions (beaucoup) plus restrictives.

Ces conditions sont prévues par l'article 46 du RGPD enrichi de l'apport de la jurisprudence européenne, et notamment de l'arrêt de « Schrems II » rendu par la CJUE le 16 juillet 2020 (voir § 5-19).

En synthèse, quatre étapes doivent être successivement suivies (et documentées) par l'exportateur de données.

Étape 1 : mettre en place des « garanties appropriées »

Première étape : il convient de mettre en place des « garanties appropriées », encore appelées « outil de transfert ». L'article 46 du RGPD en dénombre quatre :

❶ **Les clauses contractuelles types (dites « CCT ») :** il s'agit, en synthèse, d'un contrat de transfert de données entre l'exportateur et l'importateur de données. La Commission européenne en propose plusieurs modèles (dits « modules ») selon la configuration rencontrée (décision d'exécution (UE) de la Commission n° 2021/914 du 4 juin 2021).

❷ **Les règles d'entreprise contraignantes (dites « BCR ») :** il s'agit en quelque sorte d'une politique « groupe » de protection des données personnelles, devant respecter un certain cahier des charges prévu à l'article 47 du RGPD (organisation d'une procédure d'instruction des réclamations, formation, audits,…) et complété par des recommandations du CEPD.

En pratique, ce dispositif concerne les transferts vers des filiales de groupes internationaux implantées dans des pays tiers n'offrant pas un niveau de protection adéquat. Dans son considérant 37, le RGPD définit le groupe d'entreprises comme celui constitué d'une entreprise exerçant une influence dominante sur d'autres entreprises du fait, « par exemple », de la détention du capital, d'une participation financière ou des règles qui la régissent, et des entreprises qu'elle contrôle. Il semble donc qu'en cas de transfert entre deux sociétés-sœurs ou cousines sans influence dominante de l'une sur l'autre, il faille se rabattre sur un autre outil juridique.

L'avantage des BCR sur les CCT est d'éviter d'avoir à conclure ponctuellement autant de contrats de transfert de données qu'il peut y avoir de transferts intra-groupes. L'inconvénient est que les BCR, une fois adoptées, doivent ensuite être approuvées dans le cadre d'une procédure associant la CNIL et le CEPD, ce qui prend du temps (entre 18 et 24 mois en moyenne).

❸ **Les codes de conduite approuvés :** il s'agit d'un mécanisme d'adhésion (généralement via des clauses contractuelles) d'un importateur de données à un « Code de conduite ».

Ces « Codes de conduite » sont élaborés par des organismes représentants des catégories de responsables de traitement ou de sous-traitants, ou encore par des associations. Ils doivent être ensuite approuvés par la CNIL et s'être vu reconnaître une validité générale au sein de l'UE par la Commission européenne.

❹ **Les mécanismes de certification :** il s'agit d'un mécanisme de certification de l'importateur de données, attestant qu'il assure des garanties suffisantes, assorti de son engagement d'appliquer des garanties appropriées.

Étape 2 : analyse d'impact du transfert, un exercice délicat

Deuxième étape : la Cour de Justice de l'Union Européenne impose à l'exportateur de données de conduire une Analyse d'Impact du Transfert (TIA).

Il s'agit d'une évaluation destinée à vérifier si, au regard de l'environnement (légal, jurisprudentiel,…) dans le pays tiers où des données personnelles doivent être transférées, l'outil de transfert envisagé pour ce transfert (CCT, BCR selon le cas, etc.) procure, dans cet État, une protection substantiellement équivalente à celle assurée, dans l'EEE, par le RGPD lu à la lumière de la Charte des droits fondamentaux de l'UE (CJUE 16 juillet 2020, aff. C-311/18, « Schrems II », § 134).

Pour le dire autrement, l'exportateur de données va devoir mettre en place une sorte « d'audit » destiné à contrôler que l'importateur des données sera bien, juridiquement, matériellement, effectivement en mesure de respecter les obligations imposées dans l'outil de transfert (ou bien si, par exemple, en raison de programmes gouvernementaux de surveillance ou de renseignements, il pourrait y avoir un risque que les autorités publiques de l'État de destination accèdent clandestinement aux données transférées).

En pratique, il s'agit d'un exercice relativement difficile.

D'une part, cela revient peu ou prou à demander à l'entreprise exportatrice de données, de se livrer à un exercice semblable à celui de la Commission européenne quand elle est amenée à prendre une décision d'adéquation. Or, la Commission européenne a déjà, par le passé, adopté des décisions d'adéquation finalement invalidées par la CJUE. Cela a été le cas à deux reprises de la décision d'adéquation vers les États-Unis dans l'affaire « Schrems ». Ce « chassé-croisé » entre la CJUE et la Commission européenne à propos de la décision d'adéquation vers les États-Unis témoigne bien du niveau de difficulté de l'exercice.

D'autre part, un tel exercice nécessite que l'exportateur de données se fasse communiquer des renseignements d'ordre technique (les barrières de protection à l'entrée pour empêcher l'accès aux données, etc.), ou qu'il puisse accéder à des sources d'information dans le pays tiers (textes légiférés mais aussi jurisprudence locale par exemple) qu'il ne sera pas forcément en mesure, à son niveau, de se procurer facilement, sauf à passer éventuellement par des Conseils juridiques locaux et/ou à mettre à contribution l'importateur (pressenti) de données sur lequel pèse d'ailleurs un devoir de coopération (RGPD, art. 28-3-h).

Pour aider les exportateurs de données dans cet exercice, le CEPD a publié des recommandations le 10 novembre 2020. Il en résulte notamment la nécessité de vérifier plus particulièrement les conditions dans lesquelles les autorités publiques de l'État importateur de données peuvent accéder aux données transférées.

De la même manière, la CNIL s'est mise en ordre de marche pour tenter d'aider les exportateurs de données dans la réalisation de cet exercice en publiant un Guide pratique de l'Analyse d'Impact de Transfert comportant un certain nombre d'éléments méthodologiques.

Reste qu'il s'agit d'un exercice complexe devant la difficulté duquel tous les exportateurs de données ne sont pas forcément outillés de la même manière.

Étape 3 : si nécessaire, mettre en place des garanties supplémentaires

Troisième étape : si le résultat de l'évaluation (voir § 5-22) conclut que le niveau d'efficacité des « garanties appropriées » mises en place risque d'être compromis, l'exportateur de données doit mettre en place des mesures supplémentaires permettant de relever le niveau de protection à un niveau essentiellement équivalent au RGPD lu à la lumière de la Charte des droits fondamentaux de l'UE.

Il va donc être demandé à l'exportateur de données (s'il souhaite toujours mettre en œuvre le transfert) de mettre en place des mesures correctives supplémentaires (contractuelles et/ou techniques et/ou organisationnelles) telles que :

- pseudonymisation ;
- chiffrement ;
- fractionnement des données ;
- clauses imposant à l'importateur de données des obligations spécifique par exemple en matière de transparence et d'information, de certifications, de déclarations régulières de non-injonction, des audits, des mécanismes correctifs, une assistance juridique des personnes concernées… ;
- Etc.

Étape 4 : réévaluation régulière

La quatrième étape consiste à réévaluer régulièrement le niveau de protection des données transférées dans le pays tiers (via notamment des audits).

Les niveaux de protection ne sont pas immuables, et peuvent s'améliorer ou au contraire se dégrader dans le temps.

Et si un exportateur de données veut transférer des données vers un pays tiers qui n'est pas couvert par une décision d'adéquation, mais sans pour autant avoir à mettre en place de « garanties appropriées » ?

En dernier recours, un transfert de données vers un pays tiers non-adéquat reste (théoriquement) possible à condition de se trouver dans l'un des cas dérogatoires listés à l'article 49 § 1, a) à g) du RGPD.

Cela vise notamment le cas où la personne concernée par le transfert a explicitement (et préalablement) consenti audit transfert, à condition toutefois qu'elle ait été préalablement informée « des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées » (risques que

l’exportateur de données ne connaît lui-même pas forcément de façon exhaustive, au risque de se voir reprocher une information incomplète).

C’est encore le cas du transfert « nécessaire à l’exécution d’un contrat entre la personne concernée et le responsable du traitement » ou encore à « la conclusion ou à l’exécution d’un contrat conclu dans l’intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale », mais pour autant que le transfert intervenant sur cette base juridique reste « occasionnel » (considérant 111 du RGPD) ce qui devrait conduire à en limiter les applications.

Et, à titre encore plus subsidiaire, quand aucun de ces dispositifs ne peut être utilisé, un transfert reste encore plus exceptionnellement possible au titre de l’article 49 § 1 alinéa 2 du RGPD, à des conditions encore plus restrictives (transfert ne revêtant pas de caractère répétitif, ne concernant qu’un « nombre limité » de personnes, nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement « sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée » et sous réserve que le responsable du traitement ait évalué toutes les circonstances entourant le transfert de données et qu’il ait offert, sur la base de cette évaluation, des « garanties appropriées » pour la protection des données personnelles).

De façon encore plus restrictive, le RGPD retient dans son considérant 113 que cette base juridique ne peut être utilisée que « dans les cas résiduels dans lesquels aucun des autres motifs de transfert ne sont applicables », ce qui ne devrait pouvoir se rencontre que dans des situations extrêmement marginales (on imagine mal dans quels cas concrètement un exportateur de données pourrait se retrouver en situation d’avoir épuisé successivement tous les autres mécanismes de transfert ci-dessus sans avoir pu en mettre en œuvre aucun).

Au final et devant un tel parcours semé d’embûches, un transfert de données vers un État partie à l’Espace Économique Européen ou a minima couvert par une décision d’adéquation reste à bien des égards la situation la moins insécure à gérer.

Les positions et opinions émises dans cette rubrique n'engagent que leur auteur.

https://www.revue-fiduciaire.com/actualite/points-de-vue/les-rh-face-au-rgpd-le-droit-d-acces-aux-donnees-a-caractere-personnel-et-le-transfert-des-donnees-a-l-etranger