

EUROPEAN DATA PROTECTION SUPERVISOR

Note d'information sur les transferts internationaux de données post-Brexit



16 juillet 2019

1. Contexte

En l'état actuel de la situation, le Royaume-Uni, Irlande du Nord comprise, devrait quitter l'UE le 1^{er} novembre 2019 à 00 h 00 (HEC) pour devenir un pays tiers¹.

Si l'UE et le Royaume-Uni signent, avant le 1^{er} novembre 2019, l'[accord de retrait](#) (titre VII) tel qu'il a été négocié fin 2018, le Brexit n'aura pas d'incidence immédiate sur les flux de données vers le Royaume-Uni. L'accord de retrait prévoit l'application du droit de l'UE relatif à la protection des données jusqu'au 31 décembre 2020, cette période pouvant être prolongée de deux années supplémentaires. On entend par droit de l'Union relatif à la protection des données: le règlement général sur la protection des données (RGPD), la directive (UE) 2016/680 en matière de protection des données dans le domaine répressif, la directive vie privée et communications électroniques, et toute autre disposition régissant la protection des données à caractère personnel.

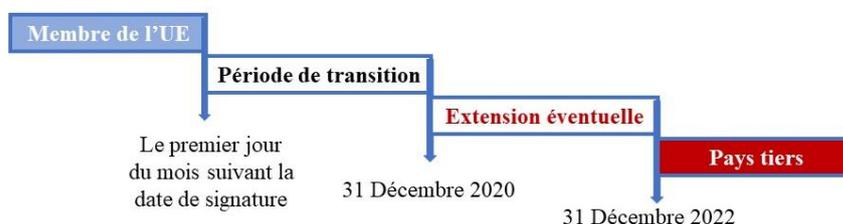


Fig. 1: Calendrier prévu dans l'accord de retrait

Cela étant, un Brexit sans accord aurait des répercussions sur la protection des données à caractère personnel. Dans ce cas de figure, le droit primaire et le droit dérivé de l'UE, y compris le droit relatif à la protection des données, cessent d'être en vigueur au Royaume-Uni. Les transferts de données à caractère personnel vers le Royaume-Uni feront l'objet de conditions spécifiques auxquelles les institutions et les organes de l'Union devront se conformer. Certaines institutions et certains organes possèdent déjà une bonne connaissance des mécanismes de transfert de données existants, dans la mesure où ils transfèrent déjà des données vers des pays tiers hors EEE.



Fig. 2: Calendrier en cas de Brexit sans accord

Le Contrôleur européen de la protection des données (CEPD) s'appuie sur les orientations en la matière fournies par la [Commission européenne](#) et par le [comité européen de la protection des données](#).

¹ Le 7 mai 2019, le gouvernement britannique a confirmé qu'il allait tenir des élections du Parlement européen et que, par conséquent, le Royaume-Uni ne quitterait pas l'UE le 1^{er} juin 2019.

2. Transferts de données au départ d'institutions et d'organes de l'Union vers le Royaume-Uni dans le cas d'un Brexit sans accord

En cas de Brexit sans accord, le flux de données des institutions et organes de l'Union et vers le Royaume-Uni, Irlande du Nord comprise, devra satisfaire aux exigences en matière de transferts internationaux de données définies au chapitre V du règlement (UE) 2018/1725. Par exemple, si une institution ou un organe de l'Union a recours à des sous-traitants installés au Royaume-Uni pour la gestion des voyages pour des missions ou pour la prestation de services informatiques, des garanties juridiques devront être offertes pour le transfert de données à caractère personnel vers le Royaume-Uni.

2.1. Mécanismes de transferts internationaux de données

Le règlement (UE) 2018/1725 prévoit que les transferts de données vers un pays tiers (tel que le Royaume-Uni) sont traités de manière à ce que le niveau de protection garanti par le règlement ne soit pas compromis (article 46). Ce niveau de protection est maintenu pour les transferts ultérieurs, c'est-à-dire les transferts au départ du pays tiers (le Royaume-Uni, par exemple) vers un autre pays tiers ou à une autre organisation internationale. À cette fin, le règlement (UE) 2018/1725 prévoit une série de mécanismes que les responsables du traitement et les sous-traitants pourront choisir afin d'autoriser le transfert vers un pays tiers. Il leur appartient de choisir le mécanisme qui correspond le mieux à leur situation parmi les mécanismes disponibles.

2.1.1 Décisions d'adéquation

Un transfert de données à caractère personnel vers un pays tiers peut avoir lieu lorsque la Commission européenne a décidé que le pays tiers en question assure un niveau de protection adéquat (article 47). Une telle décision d'adéquation a pour effet d'autoriser les flux de données à caractère personnel au départ des institutions et des organes de l'Union vers le pays tiers en question comme si les transferts avaient lieu au sein de l'UE ou de l'EEE.

Cela étant, une telle reconnaissance du cadre juridique du Royaume-Uni ne pourra pas être mise en place avant que ce dernier ne quitte l'UE, et les négociations en la matière prendront un certain temps.

Par conséquent, les institutions et les organes de l'Union étudient l'adoption d'un autre mécanisme de transfert parmi ceux présentés au chapitre V.

2.1.2 Garanties appropriées

Plusieurs mécanismes de transfert de données offrent des garanties appropriées. Toutes les «garanties appropriées» sont répertoriées à l'article 48 du règlement (UE) 2018/1725. Ces dernières ont en commun l'obligation d'assurer des droits opposables et effectifs pour les personnes concernées.

a. Instruments exclusivement à disposition des autorités publiques

En leur qualité d'autorités publiques, les institutions et les organes de l'Union peuvent décider d'utiliser les mécanismes qui, en vertu du règlement (UE) 2018/1725, sont les plus adaptés à leur situation [article 48, paragraphe 2, point a), et article 48, paragraphe 3, point b)].

La première possibilité consiste à utiliser un instrument juridiquement contraignant et exécutoire, comme un accord administratif, un accord international bilatéral ou multilatéral. Un tel accord doit être contraignant et exécutoire pour les parties signataires.

La seconde possibilité consiste à avoir recours à des arrangements administratifs (sous la forme d'un protocole d'accord, par exemple). Bien qu'ils ne soient pas contraignants en tant que tels, ces arrangements garantissent des droits opposables et effectifs aux personnes concernées. Les arrangements administratifs non contraignants doivent faire l'objet d'une autorisation du CEPD.

b. Clauses types de protection des données

Lorsque les institutions et les organes de l'Union interagissent avec des entités privées (par exemple, en externalisant la gestion des voyages pour des missions, les services informatiques ou la formation)², une solution consiste à signer des clauses types de protection des données adoptées par la Commission européenne. Ces contrats offrent les garanties suffisantes supplémentaires au regard de la protection des données qui sont nécessaires dans l'éventualité d'un transfert de données à caractère personnel vers un pays tiers.

Trois ensembles de clauses types de protection des données sont actuellement disponibles (elles demeurent valables en vertu du RGPD jusqu'à leur modification, leur remplacement ou leur abrogation par une décision de la Commission):

- dans l'éventualité d'un transfert d'un responsable du traitement dans une institution ou un organe de l'UE vers un responsable du traitement dans un pays tiers hors UE/EEE (par exemple, au Royaume-Uni), deux ensembles sont disponibles:
 - [2001/497/CE](#);
 - [2004/915/CE](#);
- dans l'éventualité d'un transfert d'un responsable du traitement dans une institution ou un organe de l'UE vers un sous-traitant dans un pays tiers hors UE/EEE (par exemple, au Royaume-Uni), un ensemble est disponible:
 - [2010/87/CE](#).

Il est important de noter que les clauses types de protection des données ne peuvent être modifiées et doivent être signées tel que prévu. Toutefois, ces contrats peuvent être intégrés dans un contrat plus vaste, et des clauses supplémentaires peuvent être ajoutées à la condition qu'elles ne viennent pas contredire, directement ou indirectement, les clauses types de protection des données adoptées par la Commission européenne³.

En cas de modification ultérieure des clauses types de protection des données, celles-ci seront considérées comme des clauses contractuelles ad hoc nécessitant une autorisation préalable du CEPD (voir analyse au point e).

Enfin, le règlement (UE) 2018/1725 prévoit la possibilité de recourir à des clauses types de protection des données adoptées par le CEPD et approuvées par la Commission. Jusqu'à présent, aucune clause de ce type n'a été adoptée.

² CEPD, [Le transfert de données à caractère personnel à des pays tiers et à des organisations internationales par les institutions et organes de l'Union européenne](#), document d'orientation, p. 23-25.

³ Voir la communication suivante de la Commission européenne http://europa.eu/rapid/press-release_MEMO-05-3_fr.htm.

c. Règles d'entreprise contraignantes

Les règles d'entreprise contraignantes sont des politiques de protection des données à caractère personnel auxquelles adhère un groupe d'entreprises (c'est-à-dire, des multinationales) afin d'offrir les garanties appropriées pour les transferts de données à caractère personnel au sein du groupe, y compris à l'extérieur de l'UE ou de l'EEE.

Lorsque le sous-traitant d'une certaine prestation n'est ni une institution ni un organe de l'Union, il peut déjà utiliser des règles d'entreprise contraignantes pour sous-traitants (ces règles d'entreprise contraignantes s'appliquent aux données reçues d'un responsable du traitement établi dans l'UE mais qui n'est pas une entité du groupe, et ensuite traitées par les entités du groupe concernées en tant que sous-traitants et/ou sous-traitant ultérieurs)⁴. Les règles d'entreprise contraignantes autorisées en vertu de la directive 95/46/CE demeurent valables en vertu du RGPD (article 46, paragraphe 5) et sont considérées comme un mécanisme de transfert offrant des garanties suffisantes conformément au règlement (UE) 2018/1725 [article 48, paragraphe 2, point d)]. Elles doivent cependant être mises à jour afin d'assurer leur parfaite conformité avec les dispositions du RGPD.

Avant que tout transfert soit effectué, les futures règles d'entreprise contraignantes devront être approuvées par les autorités nationales de contrôle compétentes, après avoir fait l'objet d'un avis du comité européen de la protection des données (article 47, paragraphe 1, et article 64, paragraphe 3, du RGPD).

d. Codes de conduite et mécanismes de certification

Lorsque le sous-traitant n'est ni une institution ni un organe de l'Union, les codes de conduite ou les mécanismes de certification prévus par le RGPD peuvent être utilisés afin d'offrir les garanties appropriées pour des transferts vers un pays tiers.

Ces outils sont nouveaux dans le cadre du RGPD et, par conséquent, il conviendra de suivre de près les activités du comité européen de la protection des données, qui travaille actuellement à l'élaboration de lignes directrices dans le but de clarifier le contenu et l'utilisation de ces outils.

e. Clauses contractuelles ad hoc

Lorsque les institutions et les organes de l'Union interagissent avec des entités privées, ils peuvent aussi avoir recours à des clauses contractuelles ad hoc qu'ils négocient avec leurs homologues au Royaume-Uni afin d'offrir des garanties suffisantes au regard de leur situation. Avant tout transfert, ces clauses contractuelles sur mesure doivent être autorisées par le CEPD [article 48, paragraphe 3, point a) du règlement (UE) 2018/1725].

2.1.3 Dérogations⁵

En l'absence de décision d'adéquation, les institutions et les organes de l'Union devraient d'abord envisager d'offrir des garanties suffisantes, encadrant le transfert de données à caractère personnel dans le cadre de l'un des mécanismes présentés au point 2.1.2.

⁴ Groupe de travail «Article 29» sur la protection des données, Document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes, WP 256 rev. 1, 28 novembre 2017, disponible sur le [site du comité européen de la protection des données](#).

⁵ Concernant les dispositions similaires du RGPD, voir également les [Lignes directrices 2/2018 relatives aux dérogations prévues à l'article 49 du règlement \(UE\) 2016/679](#) du comité européen de la protection des données.

Les dérogations prévues à l'article 50 du règlement (UE) 2018/1725 sont des exceptions au principe général selon lequel les données à caractère personnel peuvent seulement être transférées vers des pays tiers lorsqu'un niveau de protection approprié est assuré par le pays tiers ou lorsque des garanties appropriées ont été offertes et que les personnes concernées disposent de droits opposables et effectifs. De plus, les transferts fondés sur une dérogation ne sont soumis à aucune autorisation préalable, quelle qu'elle soit, du CEPD, et présentent donc des risques accrus pour les droits et les libertés des personnes concernées. Par conséquent, les dérogations doivent être interprétées de manière restrictive et portent principalement sur des activités de traitement occasionnelles et non répétitives.

Une liste exhaustive des dérogations figure à l'article 50, paragraphe 1, du règlement (UE) 2018/1725, et inclut notamment les situations dans lesquelles:

- la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été dûment informée des risques associés à ce transfert;
- le transfert de données est nécessaire à l'exécution d'un contrat dont la personne concernée est l'une des parties, ou à la mise en œuvre de mesures précontractuelles;
- le transfert de données est nécessaire 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;
- le transfert de données est nécessaire pour des motifs importants d'intérêt public;
- le transfert de données est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice;
- le transfert de données est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, et la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement; ou
- le transfert a lieu à partir d'un registre public.

3. Données transférées avant la date de retrait

Dans un [document](#) exposant sa position sur l'utilisation des données et la protection des informations obtenues ou traitées avant la date de retrait, la Commission arrive à la conclusion que les responsables du traitement et les sous-traitants établis au Royaume-Uni peuvent continuer à traiter les données à caractère personnel transférées avant la date de retrait seulement si ces dernières sont protégées par le droit de l'Union relatif à la protection des données. Cette protection sera garantie si un accord de retrait est conclu.

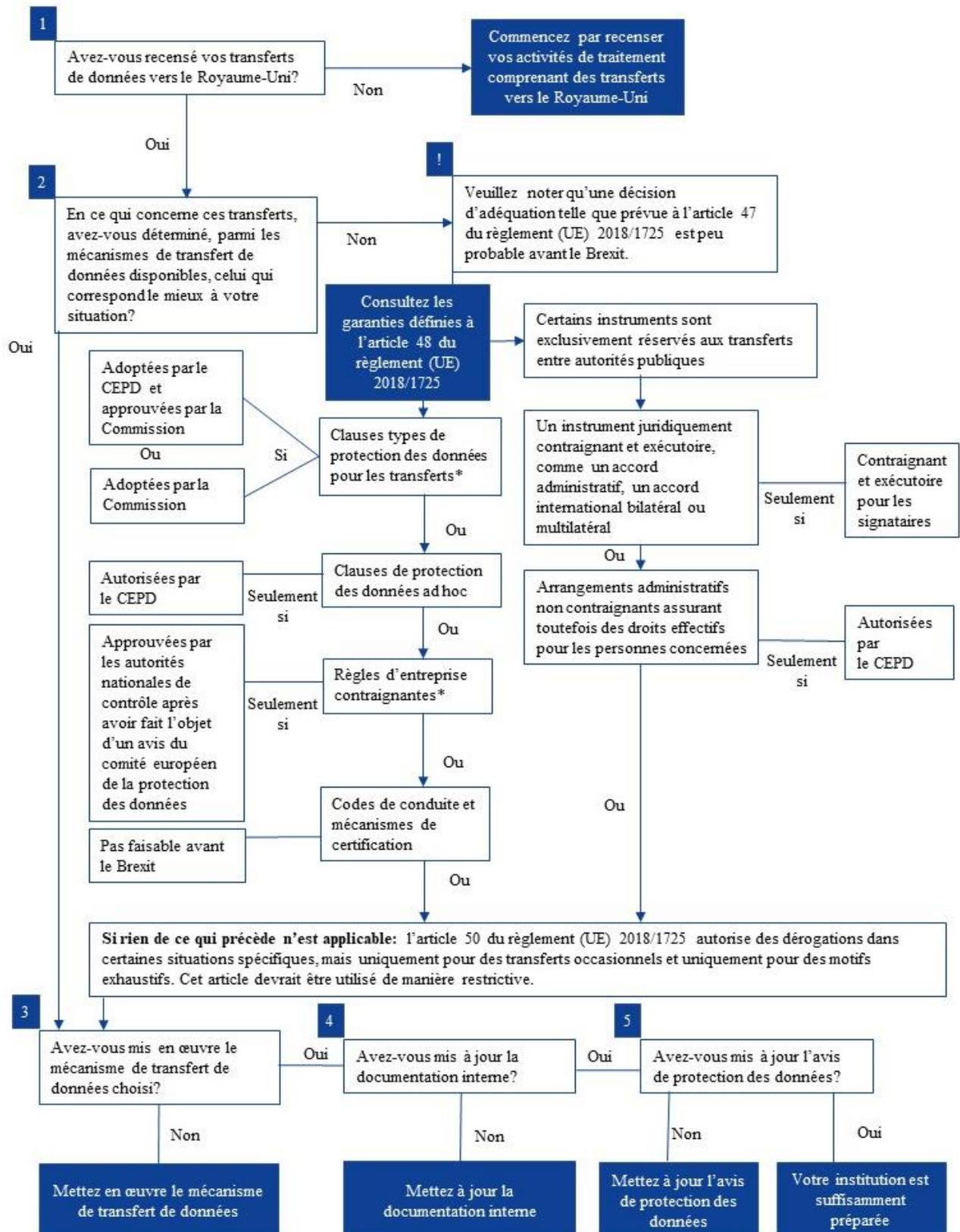
L'évolution de cette question sensible devra être suivie de près et le CEPD pourrait fournir des orientations supplémentaires si cela est jugé nécessaire.

4. Mesures préparatoires

Afin de se préparer à l'éventualité d'un Brexit sans accord, les institutions et les organes de l'Union devraient prendre les mesures suivantes:

- i. recenser leurs activités de traitement;
- ii. parmi les mécanismes de transfert de données disponibles, déterminer celui qui correspond le mieux à leur situation;
- iii. mettre en œuvre le mécanisme de transfert de données choisi avant le 1^{er} juin ou le 1^{er} novembre 2019;
- iv. mettre à jour leur documentation interne;
- v. mettre à jour leur avis de protection des données en conséquence.

4.1. Résumé des mesures à prendre afin de se préparer à l'éventualité d'un Brexit sans accord



* Les règles d'entreprise contraignantes et les clauses contractuelles types (adoptées par la Commission européenne) en vertu de l'ancienne directive 95/46 demeurent valables, mais devront être mises à jour au fil du temps afin d'assurer leur conformité avec le RGPD. En tout état de cause, il conviendra de veiller à ce que les anciennes clauses contractuelles types de la Commission soient conformes au règlement (UE) 2018/1725 avant de les utiliser.