



## DONNÉES PERSONNELLES

# Le Royaume-Uni adopte ses clauses contractuelles types

Les clauses contractuelles types adoptées récemment par l'ICO constituent à la fois un instrument de compétitivité économique et une menace pour le statut d'adéquation du Royaume-Uni.

Depuis la publication des nouvelles clauses contractuelles types par la Commission européenne le 4 juin 2021<sup>1</sup>, les exportateurs de données du Royaume-Uni se trouvaient dans une situation paradoxale où malgré le Brexit, ils devaient continuer à utiliser les anciennes versions des clauses contractuelles types qui étaient désormais obsolètes dans l'Union européenne.

L'arrêt Schrems II<sup>2</sup> a non seulement invalidé le Privacy Shield mais a également examiné en détail la validité des clauses contractuelles types invoquées par Facebook<sup>3</sup> pour justifier le transfert des données de M. Schrems vers les Etats-Unis. Si la Cour n'a pas invalidé ces clauses, elle a néanmoins affirmé qu'elles ne suffisaient pas par elles-mêmes à assurer la conformité d'un transfert de données au RGPD. En effet, la Cour a affirmé que les éléments pertinents du système juridique du pays concerné devaient également être pris en compte avant toute exportation et que les autorités de contrôle pouvaient interdire les transferts fondés sur des clauses contractuelles types si elles estimaient que ces clauses ne sont pas ou ne peuvent pas être respectées dans le pays tiers. Suite à cette décision, la Commission a entamé une procédure très rapide de révision des trois versions existantes de clauses contractuelles types,

qui s'est conclue le 4 juin 2021 par la publication des nouvelles clauses contractuelles types<sup>4</sup> (« CCT »), dont le préambule se réfère directement à l'arrêt Schrems. Pendant cette période, le Brexit est devenu effectif le 31 décembre 2020 et si le Royaume-Uni était toujours lié par la jurisprudence Schrems II, la décision de la Commission adoptant les nouvelles CCT n'y avait aucun effet.

L'Information Commissioner Office (« ICO »), l'autorité de contrôle britannique, a donc alors indiqué que pour les transferts hors du Royaume-Uni, seules les anciennes versions des CCT, adoptées par la Commission européenne avant le Brexit, pouvaient être utilisées. L'ICO a lancé une consultation sur les nouvelles clauses contractuelles types qu'elle entendait adopter entre le 11 août et le 11 octobre 2021, dont résulte le modèle d'International Data Transfer Agreement (« IDTA ») qui est entré en vigueur au Royaume-Uni le 21 mars dernier. Les anciennes clauses de l'Union européenne, qui ne peuvent plus être utilisées pour de nouveaux contrats depuis le 27 septembre 2021 et devront être remplacées pour les contrats en cours à compter du 27 septembre 2022 voient cependant leur existence prolongée au Royaume-Uni jusqu'au 21 septembre prochain pour les nouveaux contrats et jusqu'au 21 mars 2024 pour les contrats en cours.

L'adoption de l'IDTA est un premier exemple intéressant de l'exercice par les autorités britanniques de leur pouvoir de divergence, qui permet de s'interroger sur les meilleures façons de faire respecter les principes du droit de la protection des données personnelles, essentiels pour que le Royaume-Uni conserve le bénéfice de l'adéquation, tout en améliorant la compétitivité de ses entreprises et l'effectivité des garanties accordées par les clauses contractuelles types sans perdre le bénéfice de sa décision d'adéquation<sup>5</sup>.

## Des différences de structuration intéressantes

Tout d'abord, l'ICO propose, pour les exportateurs de données qui ont déjà conclu des SCC, de conclure un simple Addendum à ces SCC pour gérer les transferts de données ayant le Royaume-Uni pour origine. L'Addendum prévoit simplement le remplacement des références aux dispositions du RGPD par des références aux dispositions correspondantes dans la réglementation britannique. Cet instrument, pensé pour les groupes de sociétés qui disposent de filiales à la fois dans l'Union européenne et au Royaume-Uni, est une première manifestation de la flexibilité manifestée par les autorités britanniques, désireuses de faire de leur réglementation des données personnelles un véritable avantage compétitif en simplifiant au maximum les formalités

pour les entreprises. Dans le cadre de l'adéquation, il pourrait être intéressant pour la Commission européenne de prévoir un instrument similaire.

L'IDTA, comme l'Addendum, semble de premier abord plus pédagogique et plus pratique que les SCC. Au lieu de renvoyer en annexe les informations spécifiques sur les données transférées par les parties, il les place au début du contrat, dans une présentation beaucoup plus claire. Il prévoit aussi que les parties puissent indiquer la périodicité applicable à la revue des mesures de sécurité dont elles sont convenues. Ces mesures de sécurité, pour lesquelles l'Annexe III des SCC se borne à donner des exemples, font l'objet d'une description beaucoup plus détaillée dans l'IDTA, puisqu'il distingue entre les mesures de sécurité applicables à la transmission des données, à leur hébergement, à leur traitement, les mesures organisationnelles adoptées ainsi que les mesures de sécurité techniques minimum applicables.

L'IDTA ne prévoit pas des modules selon les différents types de transferts comme les SCC mais demande aux parties de spécifier au début du document si elles agissent en tant que responsable, sous-traitant ou sous-traitant de second rang. Ceci rend le document beaucoup plus clair et lisible que les SCC. Les obligations du sous-traitant au titre de l'article 28 du RGPD ne sont pas traitées par l'IDTA mais doivent être spécifiées par les parties dans un autre document, ce qui accorde plus de liberté aux parties que les clauses prévues à cet effet pour les sous-traitants dans les SCC. Plusieurs sections de l'IDTA permettent de prévoir que toute modification du contrat de sous-traitance modifiera de plein droit l'IDTA, sans que les parties aient besoin de conclure un avenant. L'IDTA conclu entre les parties est également amendé de plein droit lors de toute modification de l'IDTA par l'ICO. Ces deux clauses de coordination constituent une réelle économie de temps et d'argent pour les entreprises évitant des processus

de signature longs et coûteux. Comme les SCC, l'IDTA permet une gestion multipartite mais ajoute la possibilité de désigner des « *lead parties* », autorisées à prendre des décisions au nom de l'ensemble d'une catégorie de parties.

Finalement, l'IDTA ne se limite pas aux seuls 4 cas mentionnés par les SCC (responsable à responsable, responsable à sous-traitant, sous-traitant à sous-traitant d'un rang inférieur et sous-traitant à responsable) mais permet également les transferts entre sous-traitants de même rang instruits par un même responsable, ce qui est une des lacunes des SCC.

Ce nouvel instrument semble donc plus complet et plus flexible que les SCC et avoir été conçu dans un but de simplification de la gestion de ces documents complexes.

### **Des obligations très similaires**

Puisqu'ils résultent à l'origine d'une même législation et répondent à la même jurisprudence, l'IDTA et les SCC comportent par nature des obligations très similaires. Selon les deux documents, les parties doivent documenter les traitements effectués sur les données transférées et fournir une copie des clauses à toute personne concernée qui en fait la demande, s'assurer de l'exactitude des données transférées et prendre toutes mesures techniques et organisationnelles appropriées pour garantir la sécurité des données.

L'exportateur de données doit faire des démarches raisonnables pour s'assurer que l'importateur peut respecter ses obligations. L'importateur doit traiter les données uniquement pour la finalité convenue, limiter la durée de leur traitement à cet objet, prendre des mesures appropriées pour remédier à toute violation et notifier toute violation à l'exportateur ainsi qu'aux personnes concernées en cas de risque pour leurs droits et libertés. Alors que les SCC prévoient que l'importateur doit dans ce cas notifier directement à l'autorité de contrôle

compétente, l'IDTA prévoit uniquement qu'il doit tenir un registre des violations à leur disposition.

Si l'importateur est responsable de traitement, il doit informer les personnes concernées de ses coordonnées, de l'objet du traitement qu'il compte effectuer et des destinataires des données, les CCT requérant en plus une information sur le droit d'obtenir une copie des clauses, sur les données transférées ainsi que sur les transferts ultérieurs qu'il compte effectuer.

Les transferts ultérieurs de données de l'importateur sont soumis à l'autorisation préalable de l'exportateur, sauf dans le cas de l'importateur responsable de traitement qui doit cependant s'assurer d'avoir mis en œuvre des garanties similaires à celles du transfert initial. De même, le recours à des sous-traitants ultérieurs n'est encadré et soumis à l'autorisation de l'exportateur dans les deux documents que pour les sous-traitants, les responsables de traitement devant simplement s'assurer que leurs sous-traitants ne traitent les données que sur leurs instructions.

Concernant l'exercice de leurs droits par les personnes concernées, les deux instruments exemptent logiquement l'importateur sous-traitant de toute obligation à ce sujet, à l'exception d'une obligation de transmission de la demande au responsable, tandis que les importateurs responsables de traitement doivent permettre l'exercice de ces droits. L'IDTA ajoute une précision intéressante en prévoyant que la communication entre l'importateur de données et la personne concernée se fera en anglais, ce qui est une réelle avancée pour l'effectivité des droits des personnes concernées. D'un autre côté, cette obligation est bien moins onéreuse pour les importateurs de données lorsqu'elle concerne uniquement la langue anglaise que si elle couvre les 24 langues officielles de l'Union européenne. Une alternative pourrait être la solution envisagée par le Digital Services Act,

qui prévoit la désignation de langues officielles de l'Union européenne utilisées par les fournisseurs de services qui seront clairement indiqués aux utilisateurs.

### Des divergences qui semblent difficiles à réconcilier

Cependant, il existe des différences qui montrent clairement la volonté du législateur britannique de rendre sa juridiction plus attractive pour les entreprises. Ainsi, en cas de transfert de responsable à responsable, si l'importateur soumis aux SCC ne peut traiter les données transférées que sur la base du consentement, la défense de ses droits en justice ou la sauvegarde d'intérêts vitaux de la personne concernée, aucune limitation semblable n'existe dans l'IDTA, qui permet à l'importateur responsable de traiter les données sur la base du contrat ou de ses intérêts légitimes, sous réserve qu'il se limite à l'objet du transfert.

Le point le plus important de ces deux instruments, et la raison de la révision des anciennes SCC, concerne bien évidemment l'interaction entre d'une part les législations étrangères auxquelles l'importateur de données est soumis et d'autre part ses engagements contractuels. Les deux instruments prévoient une obligation de notification à l'exportateur en cas de demande d'accès aux données des autorités du pays d'importation, lorsque cela est légalement possible, et de tenue d'un registre des demandes d'accès de ces autorités, mis à la disposition de l'autorité de contrôle du pays d'exportation. L'obligation d'information est plus large dans les SCC puisqu'elle concerne également tout accès direct aux données par les autorités dont l'importateur a connaissance, alors que l'IDTA la limite aux demandes d'accès effectuées par ces autorités qui sont juridiquement contraignantes et dispense même de notifier les demandes d'accès pour lesquelles il existe des motifs significatifs de penser qu'elles sont illégales. De plus, les SCC imposent à l'importateur de données

une obligation de contrôler la légalité de la demande de divulgation et, si des motifs raisonnables « en vertu de la législation du pays de destination, des obligations applicables en vertu du droit international et des principes de courtoisie internationale » de contestation existent, de procéder à cette contestation. Les SCC vont très loin dans le détail de cette obligation, puisqu'elles obligent l'importateur de données à exercer toutes les voies d'appel disponibles et à demander des mesures provisoires pour bloquer l'accès aux données tant qu'il n'a pas été statué sur la question. Finalement l'analyse juridique effectuée et les procédures intentées doivent être documentées et l'importateur soumis aux SCC s'engage à ne fournir que le minimum d'informations autorisées lorsqu'il répond à une demande de divulgation. Les SCC imposent donc aux importateurs de données des obligations beaucoup plus étendues et onéreuses que celles de l'IDTA en cas d'accès ou de demande d'accès aux données par ses autorités nationales.

Similairement, alors que les SCC obligent les parties à garantir que la législation du pays d'importation n'empêchera pas l'importateur de s'acquitter de ses obligations, énumèrent de façon précise et détaillée les facteurs à prendre en compte dans cette analyse et imposent aux parties de la documenter, l'IDTA se borne à obliger l'importateur de données à fournir toute information nécessaire à l'exportateur afin que celui-ci puisse procéder à son analyse de risque. Dans son projet d'évaluation des risques liés aux transferts internationaux<sup>6</sup>, l'ICO reconnaît qu'elle « ne s'attend pas que vous deveniez des experts des régimes internationaux de surveillance » et conseille, si l'exportateur ne peut pas se faire une opinion du risque lié à un pays, de se poser la question de la probabilité qu'un tel accès se produise. Ceci est en contradiction flagrante avec les recommandations du Comité européen de la protection des données, qui disposent que « En l'absence de législation régissant les conditions dans lesquelles

les autorités publiques peuvent accéder à des données à caractère personnel, si l'exportateur souhaite toujours procéder au transfert, il devrait examiner d'autres facteurs objectifs et pertinents et ne pas se fonder sur des facteurs subjectifs, tels que la probabilité que les autorités publiques accèdent aux données d'une manière qui n'est pas conforme aux normes de l'UE. L'exportateur devrait procéder à cette évaluation avec toute la diligence requise et la documenter soigneusement, étant donné qu'il sera tenu responsable de la décision qu'il pourrait prendre sur cette base »<sup>7</sup>. Après une lecture conjuguée de l'IDTA et des recommandations de l'ICO concernant les analyses de risques des transferts internationaux, les transferts vers les Etats-Unis semblent poser des problèmes beaucoup plus limités qu'en appliquant les SCC et les recommandations du CEPD.

Le dernier point, qui semble difficilement conciliable, concerne la législation et la juridiction applicable. En effet, l'IDTA et l'Addendum ne peuvent être soumis qu'à la juridiction et aux droits anglais, écossais ou irlandais tandis que les SCC ne peuvent être soumises qu'au droit et à la juridiction d'un pays de l'Union européenne (à l'exception des transferts de sous-traitant à responsable qui peuvent être soumis au droit de tout pays qui reconnaît des droits au tiers bénéficiaire mais demeurent soumises à la juridiction d'un Etat membre). Ceci pose un problème fondamental d'articulation entre les deux instruments, que l'Addendum a cherché à résoudre. Ainsi, par exemple en cas de transfert de données d'un groupe de sociétés européennes et britannique vers les Etats-Unis couvert par des CCT et l'Addendum, si des données européennes sont tout d'abord transférées vers le Royaume-Uni en application de la décision d'adéquation, elles sont ensuite transférées vers les Etats-Unis en application de l'Addendum, soumis au droit britannique et à la juridiction des tribunaux britanniques. Cependant, l'Addendum dispose qu'il prévaut sur les SCC

sauf si les termes des SCC accordent une plus grande protection aux personnes concernées, ce qui leur permettra donc d'intenter un recours contre l'importateur de données dans un Etat membre de l'Union en application de l'article 11 des SCC. Par contre, si le transfert a d'abord lieu d'Europe vers le Royaume-Uni en application de la décision d'adéquation, puis du Royaume-Uni vers les Etats-Unis en application d'un IDTA conclu entre une société britannique et une société américaine, les personnes concernées européennes ne peuvent exercer un recours contre l'importateur ou mettre en jeu sa responsabilité que selon le droit britannique et les juridictions du Royaume-Uni, ce qui est un désavantage considérable pour les personnes concernées européennes, même si elles conservent un droit de recours effectif.

L'examen de l'IDTA révèle à la fois les opportunités et les risques que la volonté britannique de divergence suite au Brexit crée pour le RGPD. D'un côté, les autorités britanniques font preuve d'un véritable pragmatisme et proposent un instrument plus clair, qui répond mieux aux besoins des entreprises. Le RGPD dans sa forme actuelle a été rédigé il y a désormais dix ans. Alors qu'aucun projet de réforme ne semble être examiné par les autorités européennes, les autorités britanniques ont affiché une volonté très agressive de réformer leur législation sur la protection des données dans un sens plus favorable à la compétitivité des entreprises. Dans le cadre de la consultation lancée le 10 septembre 2021<sup>9</sup>, le gouvernement britannique a ainsi

formulé de nombreuses propositions qui vont au cœur des principes du RGPD : introduction d'une liste exhaustive d'intérêts légitimes qui ne devraient pas être admissibles sans les évaluer par rapport aux intérêts et droits fondamentaux des personnes concernées, simplification des traitements des données à des fins de recherche scientifique et d'intelligence artificielle, redéfinition du rôle des délégués à la protection des données et des analyses d'impact, suppression de l'obligation de tenir des registres... Si ces propositions semblent pour certaines excessives, il est néanmoins sain que le RGPD fasse l'objet d'un réexamen après six années et que des solutions alternatives puissent être examinées. D'un autre côté, la volonté du gouvernement britannique d'utiliser la réglementation de la protection des données comme un avantage comparatif fait peser un véritable risque sur la cohérence de la réglementation européenne, qui pourrait conduire la Commission à revoir rapidement la décision d'adéquation dont bénéficie le Royaume-Uni. Le Royaume-Uni a fait part de sa volonté d'utiliser ses pouvoirs pour adopter des décisions d'adéquation à court terme concernant l'Australie, la Colombie, le Centre Financier International de Dubaï et Singapour, et à plus long terme le Brésil, l'Inde, l'Indonésie et le Kenya. L'IDTA ou ces décisions d'adéquation pourraient constituer un véritable cheval de Troie pour les données personnelles de l'Union européenne, tout d'abord transférées hors de l'Union vers le Royaume-Uni sous le régime de la décision d'adéquation puis du Royaume-Uni vers des pays envers lesquels ces transferts

seraient impossibles sous les SCC sans garanties additionnelles. Le Royaume-Uni devra trouver un équilibre entre sa volonté affirmée d'utiliser sa liberté retrouvée suite au Brexit et le risque de perdre le bénéfice de la reconnaissance de son niveau adéquat, estimé à près de 1,6 milliards de livres<sup>9</sup>.

## Marc LEMPERIERE

Avocat associé

ALMAIN

### Notes

- (1) Décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil (texte présentant de l'intérêt pour l'EEE).
- (2) Cour de justice de l'Union européenne, Data Protection Commissioner contre Facebook Ireland Ltd, Maximilian Schrems, 16 juillet 2021, C311-18.
- (3) Décision 2010/87/UE de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil.
- (4) Décision d'exécution (UE) 2021/914 de la Commission du 4 juin 2021 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil (texte présentant de l'intérêt pour l'EEE), C/2021/3972.
- (5) Décision d'exécution de la Commission du 28 juin 2021 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni, C/2021/4800.
- (6) ICO, Draft International transfer risk assessment and tool, août 2021.
- (7) CEPD, Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE, 10 novembre 2020.
- (8) Department for Digital, Culture, Media and Sport ; « Data, a new Direction », 10 septembre 2021,
- (9) New Economics Foundation, UCL European Institute, « The cost of data inadequacy, the economic impact of the UK failing to secure an adequacy decision », novembre 2020,



Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld [sr@expertises.info](mailto:sr@expertises.info)