Brève sur le Brexit

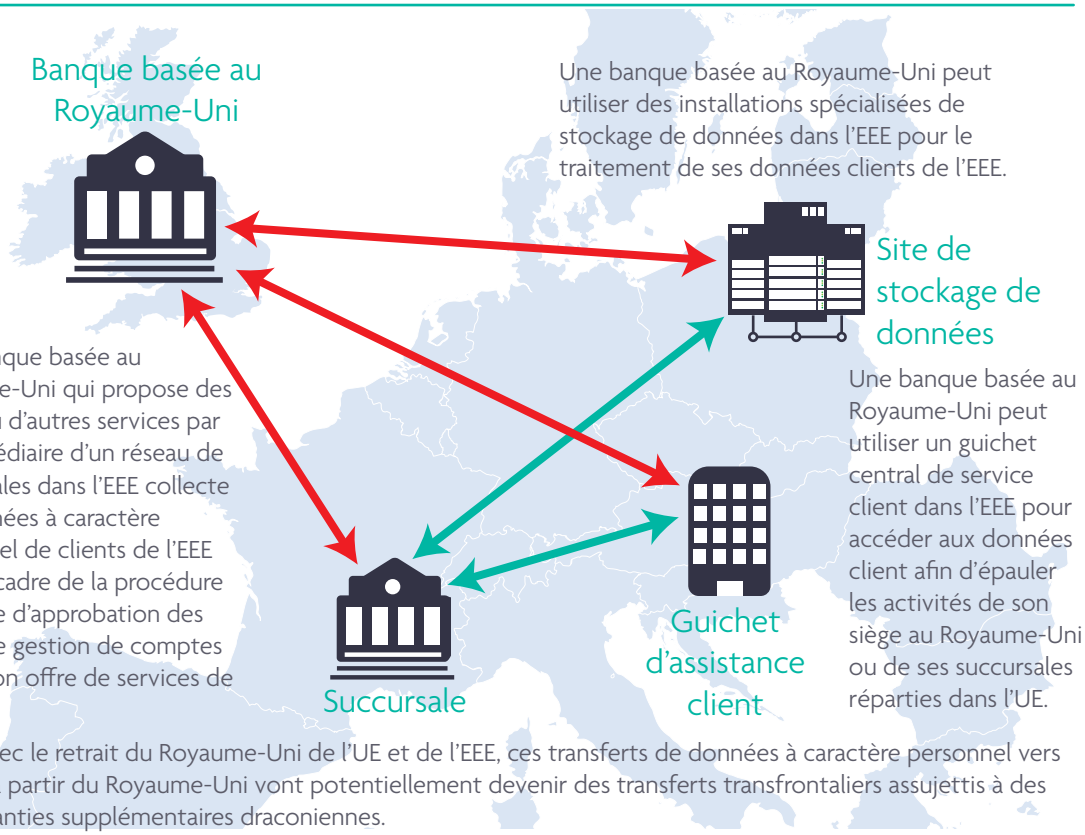
Protection et transfert de données

Faits saillants

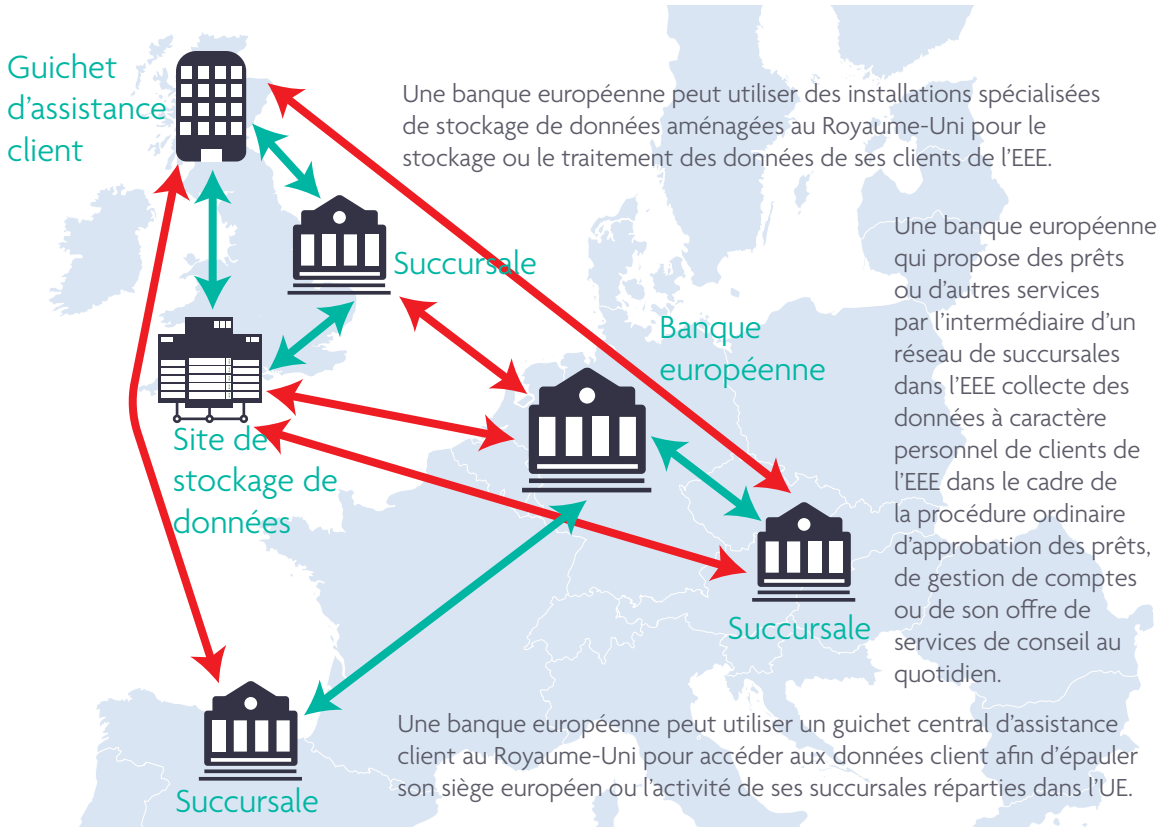
- Le transfert de données à caractère personnel entre divers lieux fait partie intégrante des activités bancaires actuelles. Les sociétés de services financiers stockent et traitent des données à caractère personnel de manière numérique au quotidien dans le cadre de leurs activités, ce qui engobe le fonctionnement des comptes des particuliers et des entreprises, l'offre de crédits, les opérations sur titres, les investissements, la prévention de la criminalité financière ainsi que la gestion du personnel.
- Au sein de l'UE et de l'EEE, le traitement des données à caractère personnel est régi par le régime de protection des données personnelles de l'UE qui protège la vie privée des personnes et d'autre droits d'information. Ce régime permet le transfert de données à caractère personnel à l'intérieur de l'EEE. De nombreuses banques et autres sociétés de l'UE ont profité de ce cadre pour rationaliser le traitement de ces données ou pour offrir un service client ou des fonctions de back-office à partir d'un nombre restreint d'emplacements au sein de l'UE et/ou de l'EEE.
- Suite au retrait du Royaume-Uni de l'UE, l'UE et le Royaume-Uni ont un intérêt commun à assurer l'efficacité du transfert des données dans un monde de plus en plus numérisé où les transferts de données font partie intégrante des activités quotidiennes.
- L'UE applique d'importantes mesures de sauvegarde sur les données à caractère personnel qui sont transférées en dehors de l'UE. Mais la tâche n'est pas des moindres, elle est lourde à administrer et peut exposer l'Union européenne à des contestations judiciaires. L'UE remplacera ces restrictions par une permission générale de transférer des données dès lors que les normes de protection des données d'un autre pays s'avèrent « adéquates ».
- Mais pour que le Royaume-Uni et l'UE conviennent du caractère respectivement adéquat de leurs régimes de protection des données après la sortie du Royaume-Uni de l'UE, la démarche n'a rien d'évident. L'expérience vécue avec les États-Unis pour avaliser les cadres de protection des données présage d'un parcours potentiellement semé d'embûches.
- Même si une décision adéquate peut être entérinée, il faudra du temps pour y parvenir. Il faudra sûrement en passer par des mesures de transition.
- Sans une décision d'adéquation, ou même avant, en l'absence de mesures de transition en place pour combler l'écart, les sociétés devront imaginer de nouveaux mécanismes pour garantir la conformité aux restrictions sur le transfert des données à caractère personnel entre le Royaume-Uni et l'UE. Il sera donc essentiel pour les entreprises de tous les secteurs - ainsi que pour les tierces parties au niveau de leur chaîne d'approvisionnement- de réexaminer leur conformité puisqu'il n'existe pas qu'un seul modèle pour parvenir à cette conformité. La tâche pourrait-être ardue et impliquer la délocalisation de certaines opérations.
- Ces problématiques ont des implications conséquentes qui s'étendent bien au delà des services bancaires et financiers. Toutes les entreprises qui transfèrent des données à caractère personnel entre l'UE et le Royaume-Uni seront potentiellement affectées.
- Un cadre sera également requis pour s'assurer que les transferts de données entre le Royaume-Uni et les pays hors de l'UE peuvent se poursuivre en toute sécurité et avec efficacité.

UK Finance Quick Briefs sont une série d'articles courts rédigés pour informer les lecteurs sur les principaux enjeux commerciaux, règlementaires et politiques autour du Brexit. Alors qu'elles se concentrent sur les activités bancaires, bon nombre des questions examinées ont une résonance plus large. Chaque BB peut être lue seule ou en corrélation avec d'autres articles de la série. Il est prévu d'élargir la série à d'autres sujets d'importance dès qu'ils seront identifiés. Pour plus d'informations, veuillez visiter: www.ukfinance.org.uk/quickbriefs

Transfert de données au sein et à l'extérieur du marché unique



Banque basée dans l'UE



Transfert de données au sein du marché unique de l'UE

Le transfert de données à caractère personnel entre différents emplacements fait partie intégrante de tous les services bancaires actuels. Les banques et autres sociétés de services financiers stockent et traitent les données à caractère personnel de manière numérique au quotidien dans le cadre de leurs activités, ce qui englobe, entre autres, l'offre de crédits, les opérations sur titres, les investissements, les audits de vérifications préalables clients, le fonctionnement des comptes des particuliers et des entreprises et la mise en conformité avec les exigences règlementaires telles que prévention du blanchiment de capitaux et financement du terrorisme. Elles déplacent ces données d'un endroit à un autre, souvent en vue de leur traitement par des centres spécialisés. Il peut s'agir des données individuelles de clients, des données relatives à leurs collaborateurs ou d'entreprises clientes en lien, par exemple, avec les dirigeants ou les employés de l'entreprise cliente. Dans une économie où la numérisation va s'augmenter, le transfert de données au sein d'une entreprise ou entre des entreprises est le quotidien d'un vaste éventail de secteurs d'activité, bien au delà des seules sociétés de services bancaires et financiers.

Comment les données à caractère personnel sont-elles transférées au sein du marché unique de l'UE ?

De nombreuses banques et autres sociétés dans l'UE ont rationalisé le stockage de données ou leur traitement, ainsi que la prestation de services au client ou leurs fonctions de back-office, pour les regrouper dans des lieux centralisés au sein de l'UE.

Au sein de l'UE et de l'EEE, le transfert de données à caractère personnel transfrontalier est régi par le régime de protection des données de l'UE, ce qui permet également d'effectuer des transferts à l'intérieur de l'EEE. Au cœur de ces transferts, la Directive sur la protection des données à caractère personnel (DPD) fixe des normes minimales d'accès, de stockage, de traitement et de transfert des données à caractère personnel des personnes de l'UE/l'EEE afin de protéger leurs droits et leurs intérêts, en particulier leur vie privée. À condition que les entreprises respectent ces exigences de protection des données, elles sont libres de faire circuler ces données à caractère personnel de clients ou d'employés entre les pays membres de l'UE et de l'EEE Non seulement ces transferts sous-tendent un large éventail d'activités, mais ce cadre a permis à de nombreuses banques et autres entreprises de l'UE de travailler plus efficacement en rationalisant le stockage ou le traitement de leurs données ou pour offrir un service client ou des fonctions de back-office à partir de lieux centralisés dans l'UE. Le cadre de protection des données de l'UE fait actuellement l'objet d'un réexamen.

La Directive DPD sera remplacée à la mi-2018 lorsque le nouveau Règlement général sur la protection des données (RGPD) de l'UE entrera en vigueur. Le RGPD introduit des exigences plus strictes pour les entreprises dans bien des domaines. Il centralise un nombre d'aspects en matière de protection des données au niveau de l'UE, y compris la responsabilité d'évaluer l'adéquation des cadres de protection des données pour les pays tiers. Le RGPD introduit également un système plus centralisé de règlementation et un mécanisme d'arbitrage entre les autorités nationales en charge de la protection des données en cas de litige. Cependant, il continue à fournir un niveau élevé de liberté en ce qui concerne la liberté de circulation des données entre les entreprises ou autres organisations au sein de l'UE et de l'EEE - sous réserve de règles de protection rigoureuses pour les données à caractère personnel et particulièrement pointilleuse sur la protection des données à caractère personnel dites « sensibles » qui se rapportent à la santé, au casier judiciaire ou à l'origine raciale ou ethnique.

Comment les données à caractère personnel sont-elles transférées hors de l'UE ?

En quittant l'UE et l'EEE, le Royaume-Uni sort du cadre de protection des données personnelles de l'UE. La DPD et le RGPD permettent le transfert les données des personnes en dehors de l'EEE à condition que ces données bénéficient d'un niveau de protection adéquat. L'UE autorise de tels transferts de deux manières:

- À travers une série de garanties supplémentaires mises en œuvre par les entreprises qui transfèrent des données vers des pays en dehors de l'EEE. Parmi ces mesures figurent tout un éventail d'obligations potentiellement complexes en sus de la pratique normale de protection des données, y compris des exigences visant à solliciter le consentement du client pour le transfert de leur données en dehors de l'EEE ou l'utilisation de modèles de contrats spéciaux pour autoriser les transferts de données transfrontaliers (voir tableau 1 : Comparaison des options de transfert de données) ou.
- Grâce à une évaluation des règles relatives à la protection des données dans la

Les mesures de transition sont nécessaires pour éviter l'effet « saut de la falaise » dans la circulation des données entre l'UE et le Royaume-Uni.

juridiction vers laquelle les données sont transférées, qui les jugera adéquates au regard des normes de l'UE en termes légaux, pratiques et de surveillance. Il s'agit essentiellement d'une variante des jugements « d'équivalence » (voir BB # 4 : Qu'est-ce que l'équivalence et comment ça marche ?) qui sont une caractéristique commune aux règles de l'UE dans d'autres domaines. Cette évaluation est actuellement menée par la Commission européenne et alimentée par les autorités nationales en charge de la protection des donnée de l'UE, un modèle qui est largement conservé en vertu des nouvelles règlementations. Un nombre de pays tiers, notamment la Suisse, l'Argentine, Israël et le Canada, ont reçu ce statut d'adéquation. celui-ci a même été accordé à l'UE elle-même par une ensemble de pays qui normalement bornent leurs transferts de données à leurs frontières.

Implications - alternatives et saut de la falaise

S'assurer d'une décision d'adéquation avec l'UE sur la protection des données peut être compliqué.

Une sortie de l'UE exige des protections adaptées au Royaume-Uni pour les données des personnes de l'UE/l'EEE et vice versa, ainsi qu'un moyen efficace de transférer les données à caractère personnel entre les juridictions. Le Royaume-Uni et l'UE ont tout intérêt à garantir la pérennité de leurs transferts de données dans un monde de plus en plus numérisé, où les transferts de données sont inscrits dans le quotidien de toutes les entreprises.

En théorie, le droit de déplacer ces données d'une juridiction à l'autre pourrait expirer du jour au lendemain dès la sortie du Royaume-Uni de l'UE. Cette situation créerait de graves perturbations dans les entreprises, auprès des clients et des employés car la prestation des services est tributaire de cette liberté de mouvement. Lever l'incertitude sur ce point ne sera possible qu'au terme de mesures de transition ou de la détermination de l'adéquation du Royaume-Uni et de l'UE pour ce qui est de leurs régimes respectifs de protection des données.

Sans certitudes en amont de la sortie du Royaume-Uni, les entreprises de l'UE des 27 et du Royaume-Uni devront garantir la conformité en utilisant des dispositions de sauvegarde alternatives pour les transferts de données. Cependant, toutes ces dispositions ont leurs inconvénients (voir tableau 1 : Comparaison entre les options de transfert de données). Par conséquent, et afin qu'elles puissent poursuivre le traitement nécessaire, les entreprises vont devoir déplacer les activités de traitement des données entre des pays, envisager la relocalisation de leurs centres de traitement des données et/ou mettre en œuvre d'autres procédures pour contourner les obstacles aux transferts transfrontaliers de données à caractère personnel.

Une décision d'« adéquation» de l'UE

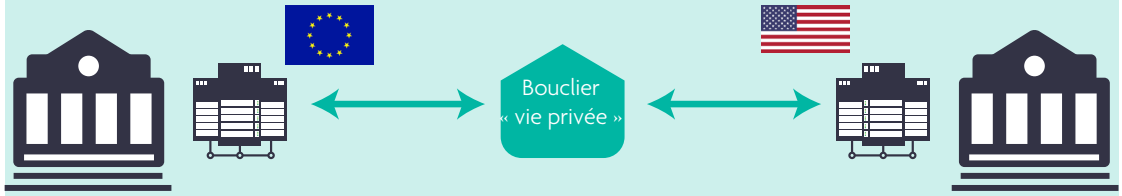
Obtenir la détermination d'une telle adéquation de la part de l'UE nécessitera de la part du Royaume-Uni de maintenir un alignement suffisant de son cadre de protection des données sur celui de l'UE afin qu'il soit jugé de nature comparable. Cela suppose une évaluation qui s'étend au delà des seules lois relatives à la protection des données et peut s'avérer sinueux (voir encadré 1 : Les États-Unis, le Royaume-Uni et l'adéquation de la protection des données du point de vue de l'UE).

Le RGPD n'est qu'une des multiples facettes pour lesquelles le Royaume-Uni devra attentivement envisager l'alignement de sa pratique avec la protection des données telle qu'elle est appliquée dans l'UE. Une autre sera la transposition des cadres en matière de cybersécurité contenus dans la Directive sur la sécurité des réseaux et de l'information (SRI). Celle-ci génère, pour les entreprises - y compris les banques et les sociétés d'infrastructure de marché - un devoir d'auto-protection contre les cyberattaques et des protocoles de partage des données sur les cyberattaques entre autorités de l'UE, Le Royaume-Uni a besoin de développer des mécanismes de coopération similaires, à l'extérieur de l'UE. De plus, un alignement continu sur les normes de la Directive SRI pourrait faire partie d'un futur jugement d'adéquation de l'UE sur la protection des données telle qu'elle est pratiquée au Royaume-Uni.

Encadré 1 : Les États-Unis, le Royaume-Uni et l'adéquation de la protection des données du point de vue de l'UE

2000 L'accord sur la Sphère de sécurité conclu entre l'UE et les États-Unis prévoit un cadre juridique pour les entreprises américaines qui les autorise à transférer des données à caractère personnel de l'UE/l'EEE vers les États-Unis sous couvert des principes auto-réglementés de protection des données.

2015 L'accord dit de la Sphère de sécurité est invalidé par la CJUE pour insuffisance de garanties de protection des données. Les évaluations de l'UE en vue de l'adéquation des États-Unis au titre de la Directive sur la protection des données continuent d'identifier de fortes variations quant aux protections offertes, entre les deux régimes.



2016 L'UE et les États-Unis négocient l'accord Bouclier « vie privée » contenant des engagements personnalisés sur la protection des données de la part des États-Unis pour les données à caractère personnel de l'UE/EEE afin de parvenir à des conclusions d'adéquation pour le régime américain. Cet accord peut toujours être contesté devant les juridictions de l'UE.

On est en droit d'attendre qu'en tant qu'ancien État membre de l'UE, il serait facile pour le Royaume-Uni d'être jugé par l'UE comme adéquat aux fins des règles de protection des données. Attention aux surprises ! Le gouvernement britannique s'était montré défavorable à certaines exigences du RGPD et il fera vraisemblablement usage de sa discrétion nationale, autorisée par le Règlement, dans de nombreux domaines. Par exemple, en février 2016, le gouvernement britannique avait annoncé son retrait d'une disposition du RGPD restreignant la divulgation de données à caractère personnel à des juridictions ou autorités de réglementation étrangères. Même si une telle flexibilité est permise à l'intérieur de l'UE - un compromis accordé au Royaume-Uni en tant qu'État membre avec des réserves bien ancrées dans ce domaine - en tant que pays tiers, de telles différences éclaireront les perspectives de jugement d'adéquation par l'UE. Les antécédents récents en matière de transfert de données entre l'UE et les États-Unis mettent en lumière les éventuels risques et perturbations pour les entreprises.

- L'UE et les États-Unis ont en effet tenté d'aplanir les divergences en matière de pratique relative à la protection des données avec un accord sur mesure reposant sur les engagements des États-Unis à protéger les données des citoyens de l'EEE : la Sphère de sécurité. Compte tenu des carences législatives des États-Unis en matière de protection générale des données, cet encadrement était nécessaire. Il a ainsi permis aux entreprises américaines soumises à la règlementation de la FTC (Federal Trade Commission) de le signer et de convenir d'être liées par les principes de protection des données de ce cadre. Cet accord UE-États-Unis a été renversé devant les tribunaux et a conduit les entreprises de l'UE qui s'appuyaient dessus pour partager en toute légalité des informations avec les homologues américaines, à se retrouver par inadvertance en violation des exigences relatives à la protection des données . Elles ont dû, à la hâte, revoir et mettre à jour leurs

contrats avec les entreprises américaines - une tâche éminemment complexe. Certaines sociétés n'ont pas été en mesure de s'adapter et ont été mises à l'amende par les autorités européennes en charge de la protection des données.

- L'accord, quasi copie conforme de remplacement - le Bouclier « vie privée » - a pour but de pallier les carences de la Sphère de sécurité. Cependant, il a été juridiquement contesté au motif qu'il ne s'est pas concrétisé et que les autorités en charge de la protection des données ont exprimé des inquiétudes similaires. Il est peu certain que le Bouclier « vie privée » soit renversé, mais il pourrait se renforcer en fonction des actions de la nouvelle Administration américaine. De nombreuses sociétés américaines présentes dans l'UE ont effectivement choisi de ne pas s'appuyer sur le Bouclier « vie privée » compte tenu de son avenir incertain. Alors que les entreprises, y compris celles du secteur financier, non régies par la FCC, peuvent mettre en place des arrangements et des protections pour permettre le partage des données, cela pourrait bien s'avérer plus difficile, plus onéreux et plus risqué juridiquement parlant.

La Sphère de protection et le Bouclier « vie privée » montrent bien à quel point il est difficile de parvenir à une décision d'adéquation si elle est indispensable, et souligne les problèmes qui pourraient être soulevés lors de discussions entre le Royaume-Uni et l'UE sur la question de l'adéquation. Si les autres États membres identifient que des éléments plus larges du cadre juridique et d'application de la loi du Royaume-Uni ne sont pas compatibles avec les principes correspondants de l'UE, il pourrait en découler des récusations de décisions d'adéquation auprès de la Cour de justice de l'Union européenne (CJUE) ou des pressions politiques à l'encontre du maintien de la position d'adéquation du Royaume-Uni.

Établissement d'un nouveau cadre britannique pour les transferts de données transfrontaliers

Le Royaume-Uni devra également remplacer les cadres existants de transfert des données créés lors de la précédente reconnaissance de l'UE des régimes de protection des données dans d'autres pays.

Le Royaume-Uni a besoin d'établir un nouveau cadre pour le transfert de données transfrontalier qui soit couvert par la règlementation de l'UE.

Transfert de données à caractère personnel du Royaume-Uni vers l'UE/l'EEE

Le Royaume-Uni devra développer son propre cadre pour reconnaître l'adéquation des règles de protection des données de l'UE relatives au transfert de données à caractère personnel du Royaume-Uni vers l'UE/l'EEE. Cela concerne tant les banques que les autres entreprises au Royaume-Uni si elles souhaitent transférer des données à caractère personnel de personnes au Royaume-Uni vers des centres de services ou d'autres sites implantés dans l'UE/l'EEE aux fins de traitement ou stockage.

Transfert de données à caractère personnel du Royaume-Uni vers d'autres pays

Le Royaume-Uni devra également remplacer les cadres existants qui régissent le transfert de données créés par les précédents régimes européens de reconnaissance de la protection des données dans des pays comme l'Argentine, le Canada, Israël, la Nouvelle-Zélande et la Suisse. Il devra également examiner son propre cadre de protection des données avec les États-Unis. Le Royaume-Uni pourrait avoir besoin de devenir partie au Bouclier « vie privée » ou d'établir son propre accord bilatéral afin de garantir une protection en bonne et due forme pour les données à caractère personnel britanniques et faciliter leur transfert. En l'absence d'un tel accord bilatéral, les entreprises du Royaume-Uni devront employer des garanties alternatives pour protéger les transferts. Ces dernières sont susceptibles d'être complexes, potentiellement moins robustes et chronophages à administrer. La robustesse des régimes britanniques, en particulier avec les États-Unis, peut être un élément déterminant de la volonté de l'UE à reconnaître l'e caractère adéquat du propre cadre du Royaume-Uni.

Transfert de données à caractère personnel provenant d'autres pays vers le Royaume-Uni

Le régime propre au Royaume-Uni devra également être évalué par un certain nombre de pays qui imposent leurs propres restrictions sur le transfert transfrontalier de données à caractère personnel, y compris des marchés comme le Japon et Israël. Certains pays de l'UE consultent la liste des pays « adéquats »pour alimenter leur propre liste de pays dont la protection est jugée adéquate, si bien que les conclusions de l'UE envers le Royaume-Uni pourraient influer sur les résultats d'autres pays en dehors de l'UE.

Tableau 1: Comparaison entre les options de transfert de données

Champ d'application pour transférer des données à caractère personnel...	
...à l'intérieur de l'EEE et de l'UE ou à partir de l'EEE et de l'UE vers des pays tiers disposant d'une décision d'adéquation par rapport à leur protection des données.	Les données à caractère personnel peuvent être transférées librement entre ces pays, à condition de satisfaire aux exigences relatives à la protection des données dans les deux juridictions.
...à partir de l'EEE et de l'UE vers des pays extérieurs ne disposant pas d'une décision d'adéquation par rapport à leur protection des données.	Lorsqu'aucune décision de l'UE en matière d'adéquation de la protection des données n'est pas en place pour un pays hors de l'EEE, les entreprises peuvent tout de même transférer des données à caractère personnel vers des entités basées dans ces pays, à condition que ces pays aient mis en œuvre une panoplie de garanties supplémentaires. Il peut s'agir de : • Modèles de contrats. S'ils sont légalement en mesure de passer un contrat les uns avec les autres, l'expéditeur des données et le destinataire peuvent convenir d'un modèle de contrat sur les conditions de la protection des données aux fins de leur transfert entre eux. Ce modèle contractuel soulève certaines questions pour les banques et leurs succursales, qui font partie d'une même entité. De même, certaines banques sont susceptibles d'avoir des centaines, voire des milliers de contrats à examiner si elles choisissent cette approche. En outre, un litige sur la légitimité du modèle de contrat est actuellement en cours d'examen par les tribunaux. • Règles d'entreprise contraignantes. Lorsqu'une entreprise peut démontrer aux autorités chargées de la protection des données de l'UE que des niveaux élevés de protection des données sont respectés de manière cohérente et solide par toutes ses opérations mondiales, elle peut être reconnue comme offrant une garantie suffisante de protection des données à caractère personnel pour permettre le transfert transfrontalier de données entre différentes entités qui constituent cette entreprise. Ces mesures peuvent être complexes et prendre beaucoup de temps à concevoir et sécuriser. Elles doivent être constamment actualisées. • Déclarations et demandes d'autorisation client supplémentaires. Les entreprises peuvent solliciter le consentement formel d'un client pour le transfert de ses données hors de l'UE. Toutefois, cela pose problèmes pour de nombreux types de transfert. Par exemple, si un transfert est requis aux fins de la règlementation, une banque ne peut pas courir le risque de se voir refuser le consentement par le client concerné ni que ce dernier retire son consentement à une date ultérieure pour les transferts suivants. La banque se retrouverait ainsi en violation de ses obligations.

Voir également

BB # 1 Rester ou quitter le marché unique de l'UE
BB # 2 Une sortie ordonnée de l'UE|
BB # 3 Qu'est-ce que le passeport pourquoi est-ce important?
BB # 4 Qu'est-ce que l'équivalence et comment ça marche?
BB # 6 L'heure de l'adaptation - la nécessité de dispositions transitoires