Comprendre les transferts de données dans le cadre du RGPD

OneTrust

PRIVACY, SECURITY & GOVERNANCE

eBOOK | AOÛT 2021

TABLE DES MATIÈRES

CLAUSE DE NON-RESPONSABILITÉ

OneTrust

PRIVACY, SECURITY & GOVERNANCE

LES CCT DE LA COMMISSION EUROPÉENNE

Les nouvelles clauses contractuelles types (CCT) de la Commission européenne

Le 4 juin 2021, la Commission européenne a adopté deux séries de clauses contractuelles types (CCT) modernisées, fortement attendues. La validité des CCT a été remise en question à la suite de la décision de la CJUE dans l'affaire Schrems II, en juillet 2020, et la Commission a publié son ensemble de projets de CCT révisés pour consultation publique en novembre. Comme prévu, la Commission a maintenant publié ses CCT finalisées pour le transfert de données personnelles vers des pays tiers (CCT de pays tiers). La Commission a également adopté et publié ses CCT à utiliser entre les responsables du traitement et les sous-traitants en vertu de l'article 28 du RGPD. Les deux nouvelles séries de CCT sont censées être plus étroitement alignées sur le RGPD et « offriront une plus grande prévisibilité juridique aux entreprises européennes et aideront en particulier les PME à garantir le respect des exigences en matière de transferts sécurisés de données, tout en permettant aux données de circuler librement par-delà les frontières, sans barrières juridiques ».

Nouvelles CCT de pays tiers et transparence du traitement des données

Les nouvelles CCT de pays tiers visent à adopter une approche standardisée et pré-approuvée afin d'offrir un point d'entrée unique, de la flexibilité, et de s'assurer que les entreprises sont en mesure de répondre aux exigences en matière de protection des données dans le cadre de leurs transferts de données. Selon le communiqué de presse de la Commission européenne, une période de transition de 18 mois sera prévue pour les responsables du traitement et les sous-traitants qui s'appuient sur les précédentes séries de CCT.

Les CCT des pays tiers publiées par la Commission adoptent une approche modulaire pour refléter la diversité des scénarios modernes de transfert de données, dont notamment ceux entre responsables de traitement, entre responsables de traitement et sous-traitants, entre sous-traitants, ainsi que ceux entre sous-traitants et responsables de traitement. Les CCT des pays tiers réglementeront également le recours à des sous-traitants secondaires, le cas échéant. Chacun des modules contient des clauses détaillées relatives aux exigences en matière de :

- Limitation des finalités
- Transparence
- Exactitude et minimisation des données
- Limitation du stockage
- Sécurité
- Transferts ultérieurs

La Commission souligne que les parties doivent déclarer qu'elles ont bien pris en compte plusieurs éléments, dont les lois et pratiques du pays tiers de destination. Différents facteurs doivent également être pris en considération, notamment l'expérience pratique pertinente et documentée de cas antérieurs de demandes de divulgation émanant d'autorités publiques, ou l'absence de telles demandes, couvrant une période suffisamment représentative.

La Commission a également mis l'accent sur la transparence du traitement, en soulignant l'obligation pour les personnes concernées de recevoir une copie des clauses contractuelles types et d'être informées des catégories de données à caractère personnel traitées, du droit d'obtenir une copie des clauses contractuelles types et de tout transfert ultérieur.

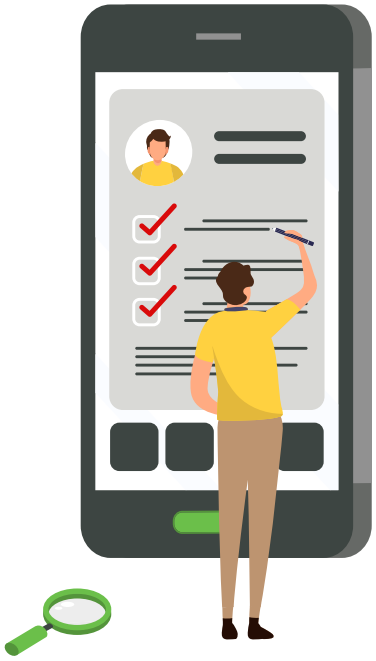
La vice-présidente chargée des valeurs et de la transparence, Vera Jourová, a déclaré : « Nous souhaitons rester ouverts et permettre aux données de circuler dans toute l'Europe, à condition que la protection afférente circule avec elles. Les clauses contractuelles types modernisées contribueront à atteindre cet objectif. Elles offrent en effet aux entreprises un outil utile pour garantir le respect de la législation sur la protection des données, tant dans le cadre de leurs activités au sein de l'UE que dans celui des transferts internationaux. C'est une solution nécessaire dans un monde numérique interconnecté où le transfert de données se fait en quelques clics ».

Alors que les discussions se poursuivent autour d'un éventuel Bouclier de protection 2.0, les nouvelles CCT de pays tiers adoptées par la Commission européenne apporteront aux organisations la clarté tant attendue sur la modernisation de ce mécanisme de transfert. Cependant, la mise à jour des CCT pour les transferts vers des pays tiers et des CCT au titre de l'article 28 du RGPD représentera une charge administrative importante pour les organisations.

UNE LISTE DE CONTRÔLE POUR LES NOUVELLES CCT

Liste de contrôle en cinq étapes pour réagir aux nouvelles CCT de la Commission européenne

La Commission a expliqué que ses nouvelles CCT offriront une plus grande prévisibilité juridique aux entreprises européennes et aideront les petites et moyennes entreprises à se conformer aux exigences requises par le RGPD en matière de transferts de données sécurisés. Cette liste de contrôle aidera les organisations à réagir aux nouvelles CCT. Elle présente certaines des mesures clés que vous pouvez prendre afin de réviser les contrats existants, de tirer parti des outils de conformité au RGPD existants et de sensibiliser vos services internes aux nouvelles clauses.



1. Actualisation de votre cartographie des données

- ☐ Réalisez un inventaire des données et cartographiez vos flux de données
- ☐ Identifiez les flux internationaux de données à caractère personnel vers des responsables du traitement ou des sous-traitants situés dans des pays tiers en dehors de l'EEE
- ☐ Déterminez lequel des quatre modules décrits dans les nouvelles CCT est applicable
- ☐ Documentez les efforts raisonnables déployés pour mettre en œuvre des mesures techniques de garanties appropriées
- ☐ Réalisez une évaluation de l'impact du transfert

Avantages des solutions OneTrust : La cartographie des données OneTrust peut aider votre organisation à établir et à maintenir une carte des flux de données actualisée ainsi qu'un registre complet des activités pour aider à démontrer la responsabilité dans le cadre du RGPD.

2. Amendements aux contrats

- ☐ Consultez les experts juridiques appropriés pour déterminer la manière la plus efficace de traiter les mises à jour contractuelles
- ☐ Actualisez les modèles de contrats pour qu'ils s'alignent sur les nouvelles CCT
- ☐ Évaluez le traitement manuel des mises à jour contractuelles, et/ou
- ☐ Envisagez un système de gestion des contrats pour les mises à jour contractuelles à grande échelle

Avantages des solutions OneTrust : La gestion des risques fournisseurs OneTrust utilise des modèles d'EIT prédéfinis pour évaluer les lois du pays tiers, en collaboration avec l'importateur, et stocker tous les documents et contrats mis à jour dans le dossier du fournisseur pour faciliter la gestion des contrats.

3. Tirer parti de votre processus de Gestion des droits des personnes pour les nouveaux droits individuels

- ☐ Élaborez et/ou mettez à jour les procédures de réception et de traitement des demandes d'accès des consommateurs
- ☐ Mettez en place des mécanismes pour vérifier l'identité des personnes concernées par les données
- ☐ Mettez en œuvre les outils appropriés pour supprimer les informations personnelles concernant d'autres personnes

Avantages des solutions OneTrust : Automatisez et gérez le cycle de vie complet des demandes de droits à la vie privée, de la réception à l'exécution. L'automatisation des demandes de droits à la vie privée de OneTrust utilise la technologie Targeted Data Discovery™ et des capacités de suppression automatique des données pour aider à simplifier le processus de Gestion des droits des personnes.

OneTrust
PRIVACY, SECURITY & GOVERNANCE

UNE LISTE DE CONTRÔLE POUR LES NOUVELLES CCT

4. Sensibilisation et formation en interne

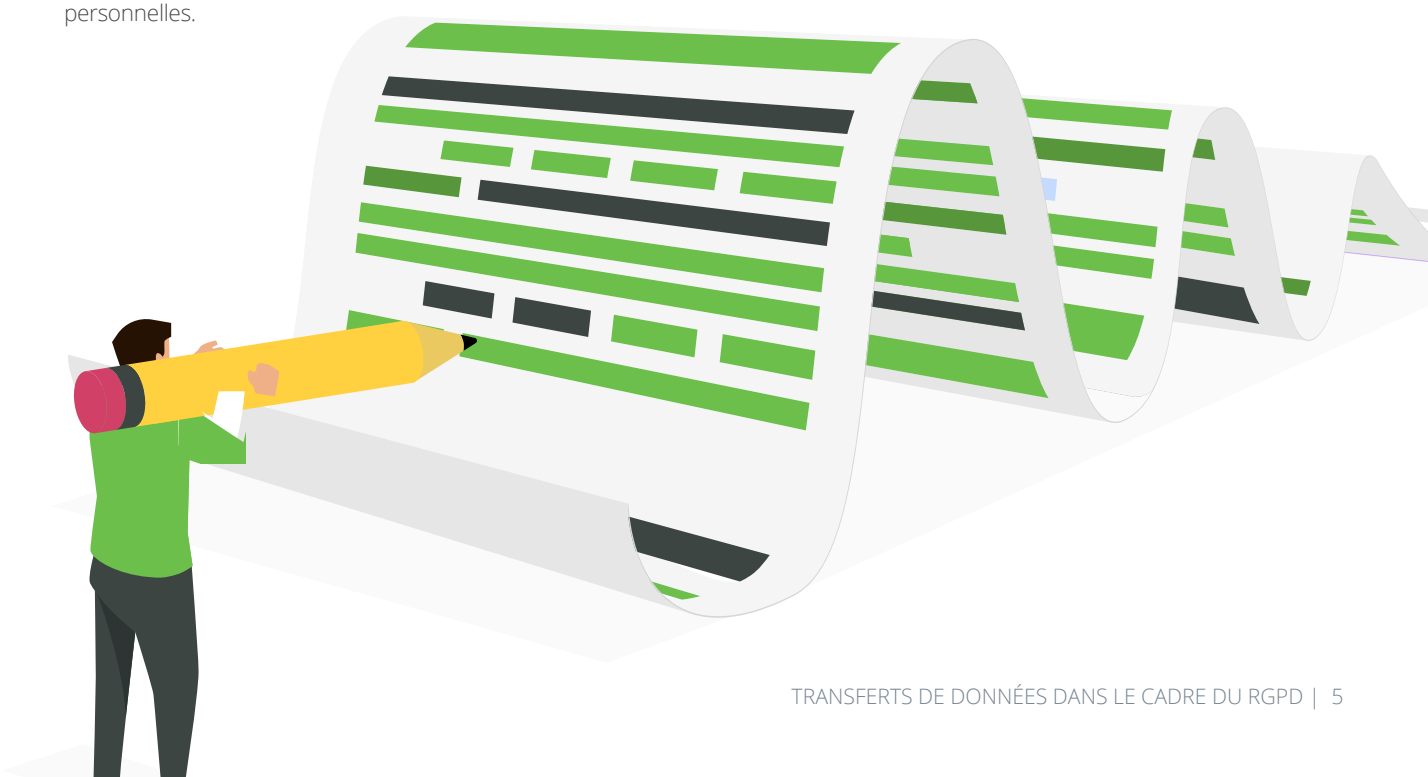
- ☐ Veillez à ce que les membres de votre organisation comprennent les nouvelles CCT et la nouvelle terminologie qui pourrait leur être présentée
- ☐ Identifiez et formez les employés chargés de traiter les demandes des personnes concernées
- ☐ Déployez le processus des CCT en interne pour promouvoir l'adhésion de l'organisation aux nouvelles CCT en tant que projet à long terme

Avantages des solutions OneTrust : La formation et sensibilisation OneTrust propose une vaste bibliothèque de cours sur la protection des données personnelles et la protection des données visant à doter vos employés des connaissances requises pour être en mesure de traiter les données de manière appropriée dans le cadre de scénarios divers et variés.

5. Revoir et contrôler périodiquement les clauses

- ☐ Tenez-vous au fait des nouveaux développements et des mises à jour, y compris les orientations des autorités de contrôle locales
- ☐ Soyez en mesure de démontrer les progrès réalisés dès que cela est raisonnablement possible
- ☐ Élaborez des règles d'automatisation pour réévaluer régulièrement les fournisseurs

Avantages des solutions OneTrust : OneTrust DataGuidance est constitué d'une équipe de plus de 40 analystes internes, spécialistes de la protection des données personnelles, et de plus de 800 experts juridiques pour aider les utilisateurs à comprendre les lois, les réglementations et les normes mondiales en matière de protection des données personnelles.



OneTrust
PRIVACY, SECURITY & GOVERNANCE

LA FEUILLE DE ROUTE EN SIX ÉTAPES DU CEPD

Le 18 juin 2021, le CEPD a adopté ses recommandations finales sur les mesures supplémentaires relatives au transfert de données vers un pays tiers afin d'aider les exportateurs de données à rester en conformité avec la législation européenne sur la protection des données. L'un des thèmes centraux des recommandations finales du CEPD porte sur la responsabilité dans le cadre de transferts de données. Une feuille de route en six étapes a été établie pour aider les organisations à évaluer les pays tiers, et à identifier et mettre en œuvre les mesures supplémentaires appropriées pour pouvoir transférer légalement des données en dehors de l'EEE.

Étape 1 : Connaître vos transferts

La première étape de la feuille de route du CEPD consiste à bien connaître vos transferts de données. Cela signifie qu'il faut comprendre exactement où votre organisation envoie les données pour pouvoir respecter les obligations de responsabilité prévues par le RGPD et déterminer si des mesures supplémentaires sont nécessaires dans le cadre dudit transfert. Le CEPD suggère que les organisations consultent d'abord leur registre des activités de traitement au titre de l'article 30 afin d'établir une cartographie des transferts internationaux de données. La cartographie et l'enregistrement des transferts de données permettent aux organisations de protéger les données au moyen de garanties appropriées et de mettre en évidence toute lacune en matière de protection des données dans leurs activités de transfert, afin d'y remédier avant que le transfert n'ait lieu. Plus important encore, le CEPD souligne que « connaître ses transferts est une première étape essentielle pour remplir les obligations qui incombent à l'exportateur de données en vertu du principe de responsabilité ».

Outre le registre au titre de l'article 30, le CEPD souligne que les informations fournies aux personnes concernées en vertu de l'article 13 concernant l'intention de transférer des données à caractère personnel vers un pays tiers peuvent également aider à cartographier avec précision vos activités de transfert de données. Il est également important de tenir compte des transferts ultérieurs potentiels des sous-traitants vers les sous-traitants secondaires dans les pays tiers, mais aussi du principe de minimisation des données et de la localisation de l'infrastructure des fournisseurs de services Cloud.

Étape 2 : Identifier les outils de transfert sur lesquels vous vous appuyez

Après avoir cartographié vos transferts de données, le CEPD recommande d'identifier les outils de transfert sur lesquels chaque activité de transfert s'appuie pour être légale au regard du RGPD. Le chapitre V du RGPD décrit les outils appropriés pour le transfert de données vers un pays tiers, parmi lesquels figurent les décisions d'adéquation, les garanties appropriées et les dérogations.

Les décisions d'adéquation sont approuvées par la Commission européenne dans le but de reconnaître qu'un pays tiers offre un niveau adéquat de protection des données à caractère personnel. Les décisions d'adéquation de la Commission européenne sont susceptibles de porter sur des transferts de données vers un pays entier ou des secteurs spécifiques, comme c'est le cas au Canada où la décision d'adéquation s'applique uniquement au secteur commercial. Une décision d'adéquation signifie que les données à caractère personnel peuvent circuler légalement de l'UE vers le pays tiers sans qu'il soit nécessaire de prévoir des garanties supplémentaires.

Les pays actuellement considérés comme conformes par la Commission européenne sont Andorre, l'Argentine, le Canada (organisations commerciales), les îles Féroé, Guernesey, Israël, l'île de Man, le Japon, Jersey, la Nouvelle-Zélande, la Suisse, le Royaume-Uni et l'Uruguay.

En l'absence d'une décision d'adéquation de la Commission européenne, les garanties appropriées prévues à l'article 46 du RGPD peuvent être utilisées par les exportateurs de données pour s'assurer que les données à caractère personnel faisant l'objet du transfert bénéficieront d'un niveau de protection substantiellement équivalent.

Les outils de transfert prévus à l'article 46 incluent :

- Les clauses contractuelles types (CCT) ;
- Les règles d'entreprise contraignantes (BCR) ;
- Le code de conduite ;
- Le mécanisme de certification ; et
- Les clauses contractuelles ad hoc.

LA FEUILLE DE ROUTE EN SIX ÉTAPES DU CEPD

En conclusion, le CEPD indique que, en l'absence d'une décision d'adéquation et de garanties appropriées découlant de l'article 46, les données à caractère personnel peuvent être transférées vers un pays tiers à condition de satisfaire à l'une des dérogations visées à l'article 49 du RGPD. Cela inclut l'obtention du consentement explicite de la personne concernée pour le transfert proposé ou les situations dans lesquelles le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement. Il est important de noter que le CEPD souligne que l'article 49 a un « caractère exceptionnel » et doit être interprété de manière restrictive.

Étape 3 : Évaluer si les outils de transfert de l'article 46 du RGPD sont efficaces au regard de toutes les circonstances du transfert

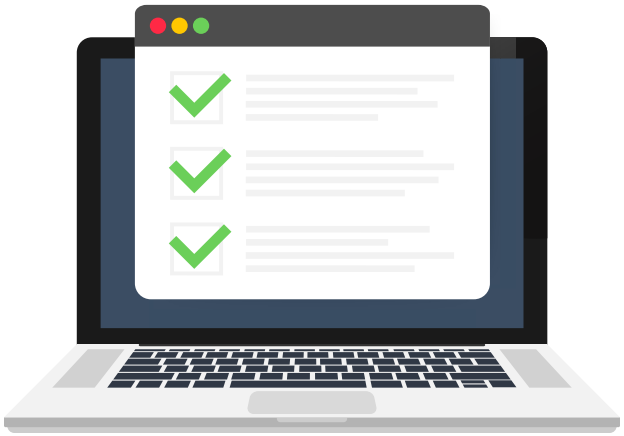
En l'absence d'une décision d'adéquation, l'article 46 du RGPD décrit plusieurs outils de transfert proposant des garanties appropriées que les exportateurs de données peuvent utiliser pour transférer des données à caractère personnel vers un pays tiers. Toutefois, le CEPD souligne dans la troisième étape de ses recommandations finales que les organisations doivent évaluer les lois et les pratiques du pays tiers susceptibles d'avoir un impact sur l'efficacité de l'outil de transfert sur lequel elles s'appuient.

Lors de l'évaluation d'un pays tiers, le CEPD met l'accent sur la prise en compte du contexte juridique spécifique du transfert de vos données, notamment :

- La finalité du transfert ;
- Les entités impliquées dans le traitement des données ;
- Le secteur dans lequel le transfert a lieu ;
- Les catégories de données à caractère personnel ;
- La localisation des données stockées ou la possibilité d'accéder à distance aux données stockées dans l'UE ;
- Le format des données ;
- La possibilité de transferts ultérieurs du pays tiers vers un autre pays tiers.

Lorsqu'il s'agit d'évaluer la législation d'un pays tiers, les exportateurs de données, en collaboration avec l'importateur de données, sont encouragés à évaluer si la législation présente des risques tels que l'accès illimité aux données à caractère personnel par les autorités publiques, ainsi qu'à vérifier si la législation qui répond aux normes européennes est réellement appliquée dans la pratique. Les exportateurs de données doivent également examiner si les pratiques dans le pays tiers sont nécessaires et proportionnées en vue de garantir les objectifs d'une société démocratique, tels que décrits à l'article 23 du RGPD, et doivent tenir compte de l'expérience pratique de l'importateur. Si la législation du pays tiers n'est pas couramment appliquée ou si les pratiques du pays tiers ne sont pas conformes aux protections de l'outil de transfert sur lequel vous vous appuyez, le CEPD indique que vous devez suspendre le transfert jusqu'à ce que des mesures supplémentaires adéquates soient mises en œuvre.

Dans un troisième scénario dans lequel vos données ou l'importateur de données sont susceptibles de relever de la « législation problématique », les exportateurs de données ont trois options : suspendre le transfert, appliquer des mesures supplémentaires ou poursuivre le transfert sans mesure supplémentaire, à condition que l'exportateur de données puisse démontrer qu'il est raisonnable de croire que la « législation problématique » ne sera pas appliquée dans la pratique.



OneTrust
PRIVACY, SECURITY & GOVERNANCE

LA FEUILLE DE ROUTE EN SIX ÉTAPES DU CEPD

Étape 4 : Adopter des mesures supplémentaires

Si, après avoir effectué une évaluation du pays tiers, il apparaît que l'outil de transfert prévu à l'article 46 et sur lequel vous vous appuyez est inefficace au regard de la législation et des pratiques de ce pays, les exportateurs de données devront adopter des mesures supplémentaires pour garantir la mise en œuvre d'un niveau de protection des données substantiellement équivalent à celui de la législation de l'UE.

L'annexe 2 des recommandations finales du CEPD présente plusieurs mesures supplémentaires que les exportateurs de données peuvent adopter, notamment :

- Des mesures techniques
  - Le cryptage et la pseudonymisation
  - Le traitement fractionné
- Des mesures contractuelles supplémentaires
  - L'obligation contractuelle d'utiliser des mesures techniques spécifiques
  - Des clauses de transparence
  - Donner aux personnes concernées les moyens d'exercer leurs droits
- Des mesures organisationnelles
  - Des politiques internes de gouvernance des transferts, en particulier avec des groupes d'entreprises
  - Des mesures de transparence et de responsabilité
  - Des méthodes organisationnelles et mesures de minimisation des données
  - L'adoption de normes et de bonnes pratiques

Dans ses recommandations finales, le CEPD indique que l'exportateur de données peut adopter plusieurs mesures supplémentaires pour garantir un niveau de protection substantiellement équivalent, le cas échéant. Toutefois, il incombe à l'exportateur de données de garantir que toute mesure supplémentaire adoptée est efficace aux fins du transfert spécifique et que cette question doit être examinée au cas par cas. Dans certains cas, il se peut également qu'aucune mesure supplémentaire ne soit appropriée et que les exportateurs de données doivent suspendre le transfert, voire même envisager d'y mettre fin.

Étape 5 : Étapes de procédure si vous avez identifié des mesures supplémentaires efficaces

Après avoir entrepris une évaluation du pays tiers et identifié les mesures supplémentaires efficaces pour obtenir un niveau de protection des données substantiellement équivalent pour le transfert de données, le CEPD indique que des étapes de procédure supplémentaires peuvent être nécessaires en fonction de l'outil de transfert de l'article 46 sur lequel vous vous appuyez.

Clauses contractuelles types (CCT)

Dans le cas de l'adoption de mesures supplémentaires en plus des CCT, le CEPD indique que l'autorité de contrôle compétente n'aura pas besoin d'être consultée dans les cas suivants :

- les mesures complémentaires ne sont pas en contradiction avec les CCT
- le niveau de protection offert par les CCT tel que prévu par le RGPD n'est pas remis en cause
- les clauses additionnelles ne peuvent être interprétées d'une manière qui affecte les droits et obligations énoncés par les CCT
- l'absence d'ambiguïté des clauses et les niveaux suffisants de protection des données sont démontrables

Le CEPD attire toutefois l'attention sur le fait que les autorités de contrôle demeurent habilitées à ordonner une révision des clauses. Les autorités de contrôle devront être consultées si l'une des mesures supplémentaires contredit les conditions initiales des CCT ou si les conditions initiales doivent être modifiées pour assurer un niveau suffisant de protection des données.

LA FEUILLE DE ROUTE EN SIX ÉTAPES DU CEPD

Règles d'entreprise contraignantes (BCR) et clauses contractuelles ad hoc

Le CEPD attire l'attention sur le fait que l'arrêt de la CJUE dans l'affaire Schrems II est pertinent dans le cas des BCR et de tout autre mécanisme de transfert où la législation d'un pays tiers peut avoir un impact sur les niveaux de protection des données offerts par ce mécanisme. Cela est dû au fait que les outils de transfert décrits à l'article 46, paragraphe 2, du RGPD sont considérés comme étant de nature contractuelle et ne sont donc pas contraignants pour les autorités publiques d'un pays tiers. Dans le cas des mécanismes de transfert relevant de l'article 46, paragraphe 2, les recommandations du CEPD prévoient que l'évaluation du pays tiers doit déterminer si des mesures supplémentaires appropriées peuvent être adoptées pour assurer un niveau de protection des données substantiellement équivalent.

Étape 6 : Réévaluer à des intervalles appropriés

Dans la sixième et dernière étape de la feuille de route du CEPD, il est précisé que la responsabilité est une exigence permanente pour les organisations en vertu de l'article 5, paragraphe 3, du RGPD. Les entreprises doivent donc mettre en place les mesures appropriées pour pouvoir surveiller en permanence l'état de la législation et des pratiques des pays tiers afin de s'assurer qu'elles disposent de garanties suffisantes et de mesures supplémentaires pour leurs transferts de données.

Le CEPD souligne également que si les mesures supplémentaires utilisées pour protéger les données à caractère personnel lors d'un transfert de données s'avèrent inefficaces en raison d'un changement dans la législation d'un pays tiers, ou si l'importateur de données n'a pas respecté ses engagements relatifs à l'outil de transfert sur lequel vous vous appuyez, des processus appropriés doivent être mis en place pour « suspendre ou mettre fin rapidement aux transferts ».

OneTrust
PRIVACY, SECURITY & GOVERNANCE

MÉCANISMES DE TRANSFERT DES DONNÉES AU NIVEAU MONDIAL

UE/EEE et adéquation de l'UE

La libre circulation des données à caractère personnel au sein de l'Union européenne (UE) et de l'Espace économique européen (EEE) est un objectif central du RGPD.

Conformément à l'article 45, paragraphe 1, du RGPD, les données à caractère personnel peuvent être transférées vers un pays tiers ou une organisation internationale sans autorisation spécifique de la Commission si l'entité en question assure un niveau de protection adéquat.

UE/EEE et adéquation de l'UE

Andorre*
Argentine*
Australie**
Autriche
Belgique
Bulgarie
Canada***
Collectivité de Saint-Martin
Croatie
Chypre
République tchèque
Danemark
Estonie
Îles Féroé*
Finlande
France
Allemagne
Gibraltar
Grèce
Guadeloupe
Guernesey*
Hongrie
Islande
Irlande
Île de Man*
Israël*
Italie
Japon*
Jersey*
Lettonie
Liechtenstein
Lituanie
Luxembourg
Malte
Martinique
Pays-Bas
Nouvelle-Zélande*
Norvège
Pologne
Portugal
Roumanie
Réunion (Région d'outre-mer de la France)
Slovaquie
Slovénie
Corée du Sud****
Espagne
Suède
Suisse*
Royaume-Uni*
Uruguay*

*Jugé adéquat par la Commission européenne
**Dossiers nominatifs des passagers uniquement
***S'applique uniquement aux données soumises à la loi PIPEDA
****En attente d'adoption

Système CBPR de l'APEC

Le système CBPR de l'APEC facilite la libre circulation des données entre ses membres. Il offre aux organisations un moyen sûr, fiable et efficace de transférer des informations personnelles d'une juridiction à l'autre et offre des garanties appropriées concernant les données à caractère personnel.

Les participants au système sont tenus de désigner un agent responsable qui supervisera l'application des principes du CBPR de l'APEC, et ils peuvent également demander la certification d'un agent responsable reconnu.

Système CBPR de l'APEC

Australie*
Canada (loi fédérale)*
Japon
Mexique*
Philippines*
Singapour
Corée du Sud*
Taïwan*
États-Unis (loi fédérale)
*Aucun agent responsable désigné

Règles d'entreprise contraignantes (BCR)

Les BCR constituent une garantie appropriée pour les entreprises implantées sur le territoire de l'UE afin de faciliter les transferts transfrontaliers de données entre leurs différentes entités intra-organisationnelles. Les BCR doivent être juridiquement contraignantes pour chaque membre du groupe organisationnel et doivent être approuvées par l'autorité de contrôle compétente de l'UE.

OneTrust
PRIVACY, SECURITY & GOVERNANCE

DÉCISIONS D'ADÉQUATION CONCERNANT LE ROYAUME-UNI

La Commission européenne a adopté deux décisions d'adéquation concernant le Royaume-Uni. L'une en rapport avec le RGPD et l'autre avec la directive en matière de protection des données dans le domaine répressif. Suite à la sortie du Royaume-Uni de l'Union européenne le 1er janvier 2021, un accord provisoire de commerce et de coopération a été conclu. Cet accord protégeait les flux internationaux de données entre les deux juridictions et devait expirer le 31 juin 2021. Les décisions d'adéquation de la Commission européenne signifient que le Royaume-Uni est considéré comme disposant « d'un niveau de protection substantiellement équivalent à celui garanti en vertu de la législation de l'Union » et que les données à caractère personnel peuvent circuler librement entre le Royaume-Uni et l'UE. Pour la première fois, les décisions d'adéquation de la Commission européenne comportent une « clause de caducité » qui signifie que les décisions expireront automatiquement quatre ans après leur entrée en vigueur.

S'exprimant sur les deux décisions d'adéquation de la Commission européenne, Didier Reynders, Commissaire à la Justice, a déclaré : « Au terme de plusieurs mois d'examens minutieux, nous pouvons aujourd'hui donner l'assurance aux citoyens de l'Union européenne que leurs données à caractère personnel seront protégées lorsqu'elles seront transférées vers le Royaume-Uni. Il s'agit d'un volet essentiel de notre nouvelle relation avec le Royaume-Uni. Il est important pour assurer la fluidité des échanges et une lutte efficace contre la criminalité. La Commission suivra de près la manière dont le système britannique évoluera à l'avenir et nous avons renforcé nos décisions pour y parvenir et pour intervenir si nécessaire. L'Union européenne dispose des normes les plus élevées en matière de protection des données à caractère personnel et ces normes ne doivent pas être compromises lorsque ces données sont transférées vers l'étranger ».

Conséquences de la décision d'adéquation concernant le Royaume-Uni

Le communiqué de presse de la Commission européenne souligne que le régime de protection des données du Royaume-Uni continue d'appliquer les mêmes règles que celles en vigueur avant sa sortie de l'UE et que des éléments essentiels du RGPD et de la directive sur l'application de la loi ont été intégrés dans son système juridique depuis sa sortie de l'UE.

Dans sa décision, la Commission européenne a souligné que le système juridique britannique offre de solides garanties en ce qui concerne les données à caractère personnel auxquelles les autorités publiques ont accès, notamment :

- La collecte de données par les services de renseignement est soumise à l'autorisation préalable d'un organe judiciaire indépendant
- Toute mesure doit être nécessaire et proportionnée aux objectifs qu'elle entend atteindre
- Toute personne estimant avoir fait l'objet d'une surveillance illégale peut intenter une action devant l'Investigatory Powers Tribunal (tribunal chargé des pouvoirs d'enquête au Royaume-Uni)

En outre, les deux décisions d'adéquation de la Commission européenne concernant le Royaume-Uni comportent, pour la première fois, une « clause de caducité » en vertu de laquelle les décisions d'adéquation sont soumises à un délai strict de quatre ans à compter de leur entrée en vigueur. Au terme de ces quatre années, la décision d'adéquation peut être renouvelée par la Commission européenne, à condition que le Royaume-Uni continue à démontrer un niveau de protection des données substantiellement équivalent. Au cours de ces quatre années, la Commission européenne a le pouvoir d'intervenir si le Royaume-Uni s'éloigne de son niveau actuel de protection des données.

OneTrust
PRIVACY, SECURITY & GOVERNANCE

FAQ SUR LES TRANSFERTS DE DONNÉES

Que dois-je prendre en compte dans l'évaluation d'un pays tiers ?
Dans les recommandations du CEPD sur les mesures supplémentaires pour les transferts de données, on peut lire : « L'évaluation de l'exportateur devrait porter principalement sur la législation du pays tiers qui est pertinente pour son transfert et l'outil de transfert visé à l'article 46 du RGPD utilisé, et qui pourrait compromettre son niveau de protection ».

Le CEPD souligne en particulier les considérations relatives à la législation des pays tiers concernant l'accès aux données par les autorités publiques à des fins de surveillance. En l'absence de législation spécifique relative à l'accès aux données par les autorités publiques, d'autres « facteurs objectifs et pertinents » doivent être pris en compte. Ceux-ci peuvent inclure des engagements pour que les droits des personnes concernées puissent continuer à être effectivement appliqués et que les garanties relatives à un outil de transfert au titre de l'article 46 puissent être effectivement appliquées, dont notamment un droit de recours pour les personnes concernées en cas d'accès à leurs données par les autorités publiques du pays tiers.

Qu'est-ce que l'équivalence substantielle ?
Les organisations qui transfèrent des données vers ou depuis un pays tiers doivent évaluer si les garanties utilisées (par exemple, les CCT ou les BCR) offrent un niveau de protection équivalent à celui offert par la législation européenne avant que le transfert n'ait lieu. Des mesures supplémentaires peuvent être adoptées pour assurer que les garanties appropriées et les mécanismes de transfert utilisés pour transférer les données sont « substantiellement équivalents » au niveau de protection offert par la législation européenne.

Que devons-nous faire si notre sous-traitant transfère des données vers les États-Unis ?
Le CEPD recommande de rester vigilant et de vérifier si un sous-traitant a l'intention de transférer ou transfère actuellement des données vers les États-Unis. Bien que l'autorisation du responsable du traitement doive être demandée pour le recours à un sous-traitant secondaire dans un pays tiers, le CEPD note qu'il convient d'être prudent quant à ces autorisations, car les transferts ne peuvent être qu'implicites.

Le CEPD précise encore : « Si vos données peuvent être transférées vers les États-Unis et qu'aucune mesure supplémentaire ne peut être fournie pour s'assurer que le droit des États-Unis n'affecte pas le niveau de protection substantiellement équivalent, tel qu'il est garanti dans l'EEE par les outils de transfert, les dérogations prévues à l'article 49 du RGPD ne s'appliquent pas non plus ; la seule solution consiste à négocier une modification ou une clause supplémentaire à votre contrat pour interdire les transferts vers les États-Unis. Les données doivent être stockées, mais également administrées ailleurs qu'aux États-Unis.

Si vos données peuvent être transférées vers un autre pays tiers, vous devez également vérifier que la législation en vigueur dans ce pays tiers est conforme aux exigences de la Cour et au niveau de protection des données à caractère personnel escompté. Si aucun arrangement convenable n'est trouvé en matière de transfert vers un pays tiers, les données à caractère personnel ne doivent pas être transférées en dehors du territoire de l'EEE et toutes les activités de traitement doivent être réalisées dans l'EEE ».

OneTrust
PRIVACY, SECURITY & GOVERNANCE

FAQ SUR LES TRANSFERTS DE DONNÉES

Le Bouclier de protection des données Suisse-États-Unis a-t-il été affecté par l'affaire Schrems II ?
Suite à la décision de la CJUE et à un examen minutieux, le Préposé fédéral à la protection des données et à la transparence (PFPDT) a confirmé que le Bouclier de protection des données Suisse-États-Unis « n'offrait pas un niveau de protection des données adéquat [...] pour la communication de données de la Suisse vers les États-Unis ». Le PFPDT note toutefois que le Bouclier de protection des données demeure en vigueur et peut offrir une protection spécifique des droits des personnes concernées. En outre, le PFPDT remarque que son évaluation du Bouclier de protection des données Suisse-États-Unis est sujette à des décisions divergentes rendues par les tribunaux suisses.

Un nouveau Bouclier de protection ou Bouclier de protection 2.0 verra-t-il le jour ?
Le Département du Commerce des États-Unis et la Commission européenne ont entamé des discussions afin d'évaluer la possibilité de renforcer le Bouclier de protection des données UE-États-Unis afin de satisfaire aux dispositions prévues par la décision rendue dans l'affaire Schrems II. Le 25 mars 2021, le commissaire européen à la justice et le secrétaire américain au commerce ont publié une déclaration commune indiquant que ces négociations seront intensifiées et ont déclaré que « ces négociations soulignent [...] notre reconnaissance mutuelle de l'importance que revêtent les flux de données transatlantiques pour nos citoyens, nos économies et nos sociétés respectifs ». Malgré ce regain d'attention, il se pourrait qu'un certain délai s'écoule encore avant qu'un Bouclier de protection des données UE-États-Unis amélioré ou une nouvelle version ne soient finalisés, étant donné que la négociation du Bouclier de protection des données UE-États-Unis actuel a duré plus de deux ans.

Qu'est-ce qu'une évaluation de l'impact du transfert (EIT) ?
Une évaluation de l'impact du transfert est un examen des risques potentiels posés par le transfert de données de l'UE vers un pays tiers. Cette évaluation doit être réalisée par l'exportateur et l'importateur de données. Les EIT doivent déterminer si les outils de transfert prévus par l'article 46 et les mesures supplémentaires utilisées offrent un niveau de protection des données substantiellement équivalent à celui prévu par la législation européenne.

OneTrust
PRIVACY, SECURITY & GOVERNANCE

AVANTAGES DES SOLUTIONS ONETRUST

OneTrust aide à la fois les importateurs et les exportateurs de données à concrétiser les lignes directrices du CEPD avec un ensemble amélioré d'outils, de conseils et de modèles. Pour les exportateurs de données, les Solutions OneTrust relatives à l'affaire Schrems II aident la mise en œuvre de la feuille de route en six étapes du CEPD, notamment avec des modèles prédéfinis servant à évaluer les pays tiers, à exécuter des évaluations d'impact des transferts (EIT) et à évaluer l'efficacité des mesures supplémentaires. Du côté des importateurs de données, OneTrust aide la mise en œuvre de programmes holistiques de protection des données personnelles et de sécurité par l'intermédiaire de la plateforme de protection des données personnelles, de sécurité et de gouvernance des données OneTrust, pour faire en sorte que les processus opérationnels, les mesures de contrôle techniques et les mécanismes de conformité appropriés soient déployés dans l'entreprise.

CARTOGRAPHIER LES TRANSFERTS
Cartographie des données | Gestion des risques fournisseurs

VÉRIFIER LES OUTILS DE TRANSFERT
Cartographie des données | Gestion des risques fournisseurs

ÉVALUER L'EFFICACITÉ
EIT | DataGuidance

ADOPTER DES MESURES
Cartographie des données | Gestion des risques fournisseurs

METTRE À JOUR LES CONTRATS
Gestion des risques fournisseurs

SURVEILLER ET RÉÉVALUER
Gestion des risques fournisseurs | DataGuidance

ÉLABORER LA DOCUMENTATION
Gestion des politiques et des avis

CRÉER VOTRE PROFIL DE CONFIANCE
Héberger la documentation stratégique relative aux échanges

AUTOMATISATION DES RÉPONSES EIT
Répondre et partager la documentation

OneTrust
PRIVACY, SECURITY & GOVERNANCE

OneTrust

PRIVACY, SECURITY & GOVERNANCE

À propos de OneTrust

OneTrust est la société la plus dynamique sur Inc. 500 et la plateforme de référence pour générer la confiance. Plus de 10 000 clients, dont la moitié des entreprises du classement Fortune 500, utilisent OneTrust pour transformer la confiance en un avantage concurrentiel, en mettant en œuvre des workflows flexibles indispensables en matière de protection des données personnelles, de sécurité, de gouvernance de données, de GRC, de risque tiers, d'éthique, de conformité et de programmes ESG.

Les produits OneTrust sont soutenus par 150 brevets et optimisés par les technologies d'intelligence artificielle et d'automatisation de l'outil OneTrust Athena™. Nos offres comprennent le logiciel de gestion de la protection des données personnelles OneTrust, la découverte et la classification basées sur l'IA OneTrust DataDiscovery™, le logiciel de veille de données OneTrust DataGovernance™, le référentiel de risques tiers OneTrust Vendorpedia™, la gestion intégrée des risques OneTrust GRC, le logiciel d'éthique et de conformité OneTrust Ethics, la gestion du consentement et des préférences utilisateurs OneTrust PreferenceChoice™, le logiciel de gouvernance, social et environnemental OneTrust ESG et la recherche réglementaire OneTrust DataGuidance™.

Selon le rapport d'IDC Worldwide Data Privacy Management Software Market Shares Report, datant de 2020, « OneTrust est sans conteste le leader du marché et ne montre aucun signe de ralentissement ou de stagnation ».

OneTrust a levé un total de 920 millions de dollars de financement pour une valorisation de 5,3 milliards de dollars auprès d'Insight Partners, Coateu, TCV, SoftBank Vision Fund 2 et Franklin Templeton.

L'équipe de OneTrust en pleine expansion, composée de 2 000 employés, est basée à Atlanta et à Londres. L'entreprise dispose également de plusieurs sites internationaux situés à Bangalore, Melbourne, Seattle, San Francisco, New York, São Paulo, Munich, Paris, Hong Kong et Bangkok.

Pour en savoir plus, consultez le site OneTrust.com ou retrouvez-nous sur LinkedIn, Twitter et YouTube.

Pour plus d'informations, rendez-vous sur OneTrust.com.