Baker McKenzie.

Tips & Tricks
Transferts de données

ROADMAP D'ANALYSE DES TRANSFERTS SELON LE CEPD

Cliquez sur chaque étape pour en savoir plus

ÉTAPE 1
Cartographier ses transferts

ÉTAPE 2
Identifier les outils de transferts utilisés

CCT / BCR / Code de conduite/ certification / →

Décision d'adéquation ou dérogation >> **OK**

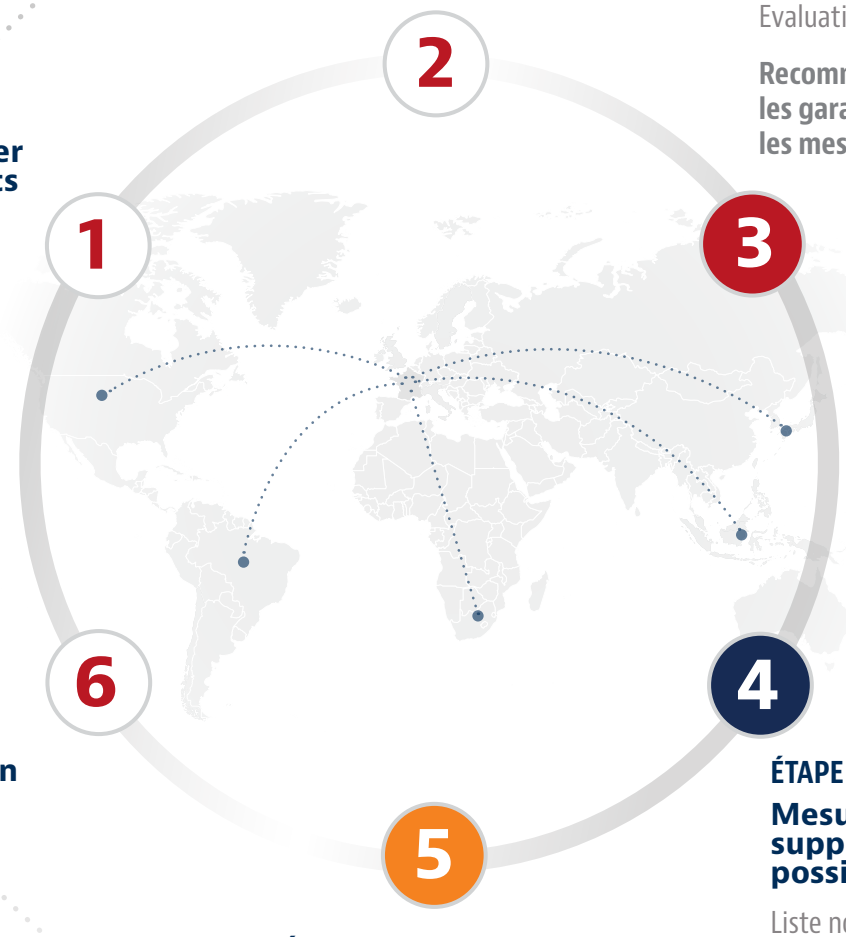
ÉTAPE 3
Efficacité de l'outil dans le pays de destination ?

Evaluation des lois locales

Recommandations 02/2020 sur les garanties essentielles pour les mesures de surveillance

Oui, protection essentiellement équivalente >> **OK**

Non >> mesures supplémentaires nécessaires



ÉTAPE 4
Mesures supplémentaires possibles?

Liste non exhaustive

>> **Recommandations 01/2020, Annexe 2**

Oui >> 5
Non >> **stop** aux transferts.

ÉTAPE 5
Mise en oeuvre des mesures supplémentaires

Conditions de mise en oeuvre

>> **Recommandations 01/2020, Annexe 2**

ÉTAPE 6
Réévaluation régulière

Notre équipe est N°1 en IT & Internet et protection des données - Chambers Global & Legal 500 2020 : elle vous accompagne en matière contractuelle, réglementaire et contentieuse, dans vos projets innovants, complexes et souvent internationaux, la transformation digitale, la communication électronique, les données personnelles et la cybersécurité. Nous contacter: par-itc@bakermckenzie.com

Baker McKenzie.

Tips & Tricks
Transferts de données

Transferts de données #1

ROADMAP D'ANALYSE DES TRANSFERTS SELON LE CEPD: ÉTAPES 1 & 2

» Comprendre s'il est possible de **poursuivre ou d'effectuer de nouveaux transferts de données** sans prendre de mesures additionnelles

» Respecter le principe **d'accountability**

Étape 1
Cartographier ses transferts

Objectif

Connaitre les flux de données et notamment les transferts de données hors de l'Espace Économique Européen.

Tips pour cartographier ses transferts plus facilement

» Reprendre les informations répertoriées dans le registre de traitement ;

» Reprendre les éléments figurant dans les politiques de confidentialité.

Tricks : Les transferts à ne pas oublier

» **tout transfert ultérieur**, par exemple, si vos sous-traitants en dehors de l'EEE transfèrent les données personnelles que vous leur avez confiées à un sous-traitant ultérieur dans un autre pays tiers ;

» **tout accès à distance** depuis un pays tiers (p.ex. en cas de maintenance) et/ou tout stockage dans un cloud situé en dehors de l'EEE (se référer aux contrat avec vos partenaires).

Étape 2
Identifier les outils de transfert utilisés

Objectif

Distinguer les transferts qui se reposent sur les outils qui ne nécessitent pas de mesures de protection complémentaires, des autres (étude de l'efficacité de l'outil dans les pays importateurs, et mesures supplémentaires).

Distinguer les outils de transferts utilisés

Si vos transferts sont fondés sur les outils suivants, vous n'avez pas besoin d'aller plus loin dans les recommandations du CEPD :

» Décision d'adéquation (p.ex. Argentine, Israël, Japon, Nouvelle-Zélande);

» Dérogations de l'article 49 RGPD (p.ex. consentement, le transfert est nécessaire pour des motifs importants d'intérêt public) (attention, application restrictive des dérogations d'après le CEPD, 2/2018).

Si vos transferts sont fondés sur les outils suivants, vous devez tenir compte des Recommandations 1/2020 **procéder à L'etape 3** > Analyse de l'efficacité de l'outil de transfert utilisé :

» Clauses Contractuelles Types ou ad-hoc

» Règles d'Entreprise Contraignantes (BCR)

» Autres: Code de conduite, Certifications, etc

Baker McKenzie.

Tips & Tricks
Transferts de données

Transferts de données #2

ROADMAP D'ANALYSE DES TRANSFERTS SELON LE CEPD: ÉTAPES 3 & 4

- Analyser **l'efficacité de l'outil d'encadrement** des transferts dans le pays tiers : clauses contractuelles types (CCT), les règles d'entreprise contraignantes (BCR), un code de conduite ou une certification
- Justifier de **l'effectivité de garanties appropriées** pour tout transfert de données à caractère personnel grâce à la mise en œuvre de mesures supplémentaires

Étape 3
Évaluer les lois applicables aux transferts

Objectif

Identifier d'éventuelles lois ou pratiques dans les pays de destination qui pourraient nécessiter la mise en place de mesures supplémentaires d'encadrement du transfert.

Analyse du niveau de protection

- L'effectivité des droits des personnes dans le cadre du transfert est-elle garantie en pratique ou nécessite-t-elle des mesures supplémentaires ?
- Le recours effectif des personnes en cas d'accès aux données par les autorités publiques est-il garanti conformément aux Recommandations 02/2020 du CEPD?

Tenir compte en particulier des circonstances suivantes dans l'analyse des lois et pratiques

- **finalités** des transferts et traitements
- nature et qualification des **entités impliquées** et secteur d'activité
- **catégories de données** transférées et de **personnes** concernées
- **type de transfert** (p.ex. stockage ou accès)
- **format** de la donnée (en clair, pseudonymisée, chiffrée, etc.)
- possibilités de **transfert ultérieur vers un autre pays** hors UE

Étape 4
Étudier les éventuelles mesures supplémentaires à mettre en œuvre

Objectif

Si des lois ou pratiques applicables aux transferts remettent en cause l'efficacité de l'outil d'encadrement des transferts, évaluer quelles mesures supplémentaires mettre en œuvre pour y remédier et garantir l'effectivité des garanties appropriées.

Exemples de mesures organisationnelles, techniques ou contractuelles (Annexe 2 des Recommandations 01/2020 du CEPD

- Le chiffrement de données sans accès de l'importateur aux clefs de déchiffrement (Use Case 1)
- La pseudonymisation de données, sans transfert des informations additionnelles nécessaires à la ré-identification des personnes et en assurant la protection de celles-ci (Use Case 2)
- Le chiffrement de données en transit (Use Case 3)
- Le recours à un destinataire de données sujet à une protection légale particulière (Use Case 4)
- Architectures de traitements impliquant plusieurs sous-traitants et garantissant contre l'accès aux données (Use Case 5)

Le CEPD liste également des cas où aucune mesure ne saurait suffire

L'effectivité des mesures supplémentaires pour garantir le niveau de protection des droits peut être assurée si certaines conditions sont réunies et nécessite une analyse au cas par cas.

ROADMAP D'ANALYSE DES TRANSFERTS SELON LE CEPD: ÉTAPES 5 & 6

» Mettre en œuvre les mesures supplémentaires

» Réévaluer régulièrement le niveau de protection des données

Étape 5
Mise en œuvre des mesures supplémentaires

Objectif

Mettre en place des procédures internes adaptées aux outils de transferts utilisés et aux mesures supplémentaires adoptées.

» Il est nécessaire de **distinguer** la mise en œuvre des mesures supplémentaires **selon les outils de transferts utilisés:**

1. Mesures s'ajoutant aux Clauses Contractuelles Types (CCT)

Une **autorisation de l'autorité de contrôle:**

n'est pas nécessaire tant que vos mesures supplémentaires (i) ne contredisent pas les CCT et (ii) sont suffisantes pour garantir que le niveau de protection des données requis n'est pas compromis ;

est nécessaire lorsque vous modifiez les CCT ou lorsque vos mesures supplémentaires contredisent les CCT.

Tip 1 : documenter les raisons pour lesquelles les clauses supplémentaires ne contredisent pas les CCT.

Tip 2 : se rapprocher d'organisation sectorielles ou professionnelles afin d'obtenir une position commune de la CNIL en la matière.

2. Mesures s'ajoutant aux Règles d'Entreprise Contraignantes (BCR) et clauses contractuelles ad hoc

L'impact précis de l'arrêt Schrems II sur ces outils de transfert est toujours en discussion d'après le CEPD. Le CEPD doit fournir plus de détails dès que possible, notamment sur la nécessité éventuelle d'inclure des engagements supplémentaires dans les BCR.

Tip : au sein des BCR, les clauses d'audit peuvent être mises en œuvre pour recenser le nombre de demandes d'accès aux données formées par des autorités étrangères, ainsi que les suites ayant été données à ces demandes.

Étape 6
Réévaluation régulière du niveau de protection

Objectif

S'assurer que le niveau de protection des données n'est pas remis en cause par des évolutions réglementaires ou technologiques.

» La réévaluation régulière du niveau de protection permet de prévenir la réalisation des risques et de réagir rapidement et efficacement lors de leur éventuelle survenance.

» La fréquence et l'importance des contrôles doivent être déterminées en fonction des risques liés aux transferts.

» La veille doit être établie à deux niveaux

1 quant à l'importateur des données, afin de s'assurer qu'il respecte les engagements pris dans le cadre de l'outil de transfert,

2 quant au pays tiers dans lequel a lieu le transfert, afin de s'assurer que les éventuelles évolutions réglementaires ne remettent pas en cause votre analyse initiale.

» Anticiper dès maintenant la mise en place de mécanismes permettant de suspendre un transfert ou d'y mettre fin rapidement en cas de remise en cause du niveau de protection des données.

» **Tip :** Prévoir des solutions alternatives aux transferts devant être suspendus ou interrompus au sein d'un plan de continuité.

» Les réévaluations doivent être soigneusement documentées et pourrons être présentées en cas de contrôle d'une autorité de protection des données.

» En cas de coresponsabilité, définir avec le responsable conjoint vos rôles respectifs dans la réévaluation.

» Retrouvez très vite notre prochain épisode de nos Tips & Tricks Transferts de Données, sur le nouveau projet de clauses contractuelles types.