Les données de surveillance peuvent-elles être hébergées chez un prestataire hors Union européenne ?

Réponse courte

L'hébergement des données issues d'un dispositif de surveillance chez un prestataire **hors Union européenne** est possible mais soumis à des **garanties juridiques renforcées**, dans la lignée de l'encadrement de la sous-traitance vidéosurveillance : décision d'adéquation de la Commission européenne, **clauses contractuelles types** (CCT) ou **règles d'entreprise contraignantes** (BCR). Depuis l'arrêt **Schrems II** (2020), un transfert vers les États-Unis exige une **analyse d'impact des transferts** (TIA) et des mesures supplémentaires concrètes.

Compte tenu de la sensibilité des données (images, logs, géolocalisation), le choix d'un prestataire **européen** ou **hébergé en UE** est fortement recommandé. Toute défaillance dans l'encadrement du transfert international expose l'employeur à des sanctions au titre du RGPD applicable en entreprise jusqu'à 4 % du chiffre d'affaires mondial et à des actions individuelles des salariés.

Définition

Le **transfert international de données** désigne tout transfert de données à caractère personnel depuis l'Union européenne vers un pays tiers ou une organisation internationale (article 44 du RGPD). Il inclut l'hébergement chez un prestataire cloud étranger, l'accès à distance par une équipe technique non européenne ou la mise à disposition à une maison-mère hors UE.

L'**arrêt Schrems II** (CJUE, 16 juillet 2020) a invalidé le Privacy Shield et impose une évaluation au cas par cas de la protection effective des données dans le pays de destination.

Questions fréquentes

Faut-il informer les salariés du transfert international des données de surveillance ?

Oui, la mention explicite du transfert international est obligatoire dans la note d'information remise aux salariés et au registre des traitements. La transparence permet l'exercice des droits prévus par les articles 44 à 49 du RGPD.

Peut-on héberger les images de vidéosurveillance chez un prestataire américain ?

Oui, mais avec garanties juridiques renforcées : décision d'adéquation, clauses contractuelles types (CCT 2021) ou règles d'entreprise contraignantes. Depuis Schrems II (CJUE, 16 juillet 2020), une analyse d'impact des transferts (TIA) avec mesures supplémentaires est obligatoire.

Pourquoi privilégier un hébergement européen pour les données de surveillance ?

Pour limiter la complexité de mise en conformité Schrems II et éviter l'analyse d'impact des transferts. Le choix d'un prestataire européen est fortement recommandé compte tenu de la sensibilité des données (images, logs, géolocalisation).

Qu'a changé l'arrêt Schrems II pour les transferts de données vers les États-Unis ?

L'arrêt CJUE du 16 juillet 2020 a invalidé le Privacy Shield et impose une évaluation case-par-case de la protection effective des données. Les CCT seules ne suffisent plus : une analyse d'impact des transferts avec mesures supplémentaires concrètes est exigée.

Quelle amende risque un transfert international non conforme ?

L'amende RGPD peut atteindre 4 % du chiffre d'affaires mondial, avec possible action conjointe de plusieurs autorités européennes en cas de transfert massif. La nullité du contrat de sous-traitance peut également être prononcée.

Quelle est la mesure technique la plus efficace pour sécuriser un transfert hors UE ?

Le chiffrement de bout en bout avant transfert avec clés conservées au Luxembourg ou dans l'UE neutralise la plupart des accès locaux par les autorités du pays tiers. C'est la mesure supplémentaire la plus efficace (recommandations CEPD 01/2020).

Quelles bases juridiques pour transférer des données de surveillance hors UE ?

Quatre bases possibles : décision d'adéquation de la Commission européenne, clauses contractuelles types (CCT 2021, Décision UE 2021/914), règles d'entreprise contraignantes (BCR) ou dérogation exceptionnelle au sens de l'article 49 RGPD.

Conditions d’exercice

Sans décision d'adéquation pour le pays de destination, les clauses contractuelles types ne suffisent plus seules depuis Schrems II : une analyse d'impact des transferts (TIA) avec mesures supplémentaires concrètes est obligatoire.

Condition	Exigence
Base de transfert	Décision d'adéquation, clauses contractuelles types (CCT 2021), BCR ou dérogation exceptionnelle
Analyse d'impact des transferts (TIA)	Évaluation de la législation du pays tiers et des risques d'accès par les autorités locales
Mesures supplémentaires	Chiffrement de bout en bout, pseudonymisation, partition des données quand les CCT ne suffisent pas
Information des salariés	Mention explicite du transfert international dans la note d'information
Documentation	Trace écrite de l'évaluation et de la base juridique du transfert
Réexamen périodique	Réévaluation de la situation juridique du pays de destination

Modalités pratiques

Le chiffrement avant transfert avec clés conservées au Luxembourg neutralise la plupart des accès locaux par les autorités du pays tiers et constitue la mesure supplémentaire la plus efficace.

Démarche	Précision
Cartographie des flux	Identification de tous les transferts internationaux liés aux données de surveillance
Choix de la base juridique	Décision d'adéquation prioritaire ; à défaut, CCT 2021 de la Commission européenne
Analyse d'impact (TIA)	Étude documentée de la législation locale, particulièrement pour les États-Unis et la Chine
Contrat de sous-traitance	Article 28 RGPD complet ; clauses sur la sécurité, la confidentialité, les sous-traitants ultérieurs
Mesures techniques	Chiffrement avant transfert, gestion des clés en UE, pseudonymisation des données identifiantes
Notice d'information	Mention dans la note remise aux salariés et au registre des traitements
Audit du prestataire	Vérifications régulières de la conformité, droit d'audit contractualisé

Pratiques et recommandations

Privilégier dès la conception un prestataire européen ou un hébergement souverain UE pour limiter la complexité de mise en conformité.

Documenter rigoureusement l'analyse d'impact des transferts (TIA) avec les sources juridiques consultées et la justification des mesures supplémentaires retenues.

Chiffrer les données avant transfert avec gestion des clés conservée au Luxembourg ou dans l'UE pour neutraliser tout accès local par les autorités du pays tiers.

Inscrire chaque transfert international dans le registre des traitements avec base juridique, destinataires et garanties retenues.

Informer clairement les salariés du recours à un prestataire hors UE et des garanties mises en place, dans la notice d'information.

Réexaminer annuellement la situation juridique des pays de destination et l'efficacité des mesures supplémentaires.

Cadre juridique

Référence	Objet
Art. 44 à 49 du RGPD	Transferts internationaux de données
Décision (UE) 2021/914	Clauses contractuelles types pour les transferts (CCT 2021)
CJUE, 16 juillet 2020 (Schrems II)	Évaluation case-par-case des transferts vers les États-Unis
Recommandations 01/2020 CEPD	Mesures supplémentaires aux outils de transfert
Loi modifiée du 1er août 2018	Cadre national luxembourgeois
Lignes directrices CNPD	Position nationale sur les transferts internationaux

Un transfert international non conforme expose à une amende RGPD jusqu'à 4 % du chiffre d'affaires mondial et à une action conjointe de plusieurs autorités européennes en cas de transfert massif. La nullité du contrat de sous-traitance peut être prononcée et toute preuve issue du dispositif rendue inopposable.