Leto

CASSE-TÊTE RGPD : COMMENT TRANSFÉRER DES DONNÉES HORS UE ?

NOS CONSEILS

LETTRE JURIDIQUE

SOMMAIRE

LES POINTS CLÉS

À PROPOS DE LETO

NOTRE HISTOIRE

La protection à la vie privée est gage de transparence et de respect dans la relation avec les autres. Mais la mise en pratique n'est pas toujours simple. Cela peut faire peur.

C'est la raison pour laquelle nous avons créé Leto.

Une solution qui vient concilier simplicité, clarté et efficacité dans le respect des données personnelles d'une entreprise.

POUR NOUS, LA PROTECTION DE LA VIE PRIVÉE EST UN DROIT FONDAMENTAL.

Benjamin Lan Sun Luk et Édouard Schlumberger, fondateurs de Leto

1. INTRODUCTION

Vous travaillez avec des entreprises hors UE ?
Alors, protégez les données que vous transférez...

INTRODUCTION

Choisir un sous-traitant en Afrique du Sud. Embaucher des salariés chinois. Utiliser un logiciel américain. L’internationalisation des échanges économiques et l’usage grandissant des technologies favorisent la circulation rapide des données hors de l’Union européenne (UE).

Pour autant, le RGPD continue de s’appliquer drastiquement. Dans ces conditions, est-il encore possible de travailler avec des entreprises étrangères ? La réponse est oui à condition que le niveau de protection soit suffisant et approprié.

Dans ce guide pratique, nous allons donc vous expliquer les enjeux relatifs au transfert des données hors UE afin que vous puissiez anticiper les contraintes réglementaires, mais aussi business, qui s’imposent à vous.

2. TRANSFERTS HORS UE ET RGPD

Êtes-vous vraiment concernés ?
Pour le savoir, il suffit de savoir si vous remplissez les critères...

TRANSFERTS HORS UE ET RGPD : DE QUOI PARLE-T-ON ?

a) Transfert de données hors UE : quelle définition ?

En l’absence de définition légale, la CNIL a décidé d’adopter une interprétation large de la notion de transferts hors UE. Sont donc concernées “toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l’Union européenne”.

La territorialité est ainsi le pilier principal de la définition. Vous l’avez deviné : le RGPD veille au sort des données qui traversent les frontières de l’UE.

b) En quoi êtes-vous concerné ?

Qui est visé ?

Si votre entreprise est considérée comme responsable de traitement (RT) ou sous-traitant (ST), alors la réglementation vous vise explicitement.

- Le responsable de traitement est la personne morale ou physique qui détermine les finalités et les moyens d’un traitement. En somme, il s’agit de toute entité qui manipule des données à caractère personnel.
- Le sous-traitant est la personne physique ou morale qui traite des données pour le compte d’un autre organisme, dans le cadre d’un service ou d’une prestation. Bien évidemment, c’est ce point qui est souvent problématique pour une entreprise qui travaille avec des interlocuteurs qui sont hors UE.

Quel est l’espace géographique concerné ?

On va s’intéresser ici au champ d’application territorial du RGPD. Pour cela, il existe deux critères alternatifs à garder en tête : le critère d’établissement ou le ciblage des données.

Le critère d’établissement suppose l’exercice effectif et réel d’une activité au moyen d’un dispositif stable comme une succursale ou une filiale ayant la personnalité juridique.

Attention : l’absence d’établissement sur le territoire de l’Union ne signifie pas que les activités de traitement effectuées par un RT ou un ST situés dans un pays tiers seront exclues du champ d’application du RGPD. C’est là où intervient le ciblage !

Le critère de ciblage désigne la situation dans laquelle le RT ou le ST non établis sur le territoire de l’UE traite des données concernant :

i) L'offre de produits ou de services aux personnes qui se trouvent sur le territoire de l'UE en dehors de toute considération de nationalité ou de résidence

Cela signifie que si vous êtes une entreprise qui cible intentionnellement le territoire de l’UE, même si votre produit et votre service sont achetés par un touriste coréen, alors vous êtes concerné par le RGPD.

Au contraire, si le traitement est lié à un service qui n’est offert qu’à un marché situé à l’extérieur de l’Union, mais que le service est utilisé lorsque ces personnes entrent dans l’Union, le traitement correspondant ne sera pas soumis aux dispositions du RGPD.

Exemple : si un abonné australien d’une application 100% australienne passe des vacances en Allemagne et continue à utiliser ladite application, le ciblage est pour ainsi dire accidentel.

ii) Le suivi du comportement dans l'UE de ces personnes, qu’un paiement ou non soit exigé, est l’autre critère alternatif

Ici, si le responsable du traitement poursuit une finalité spécifique de collecte et de réutilisation ultérieure des données pour une analyse comportementale ou technique de profilage, alors le critère de ciblage est rempli.

Cela englobe un large éventail d’activités de suivi comme : la publicité personnalisée, la géolocalisation, en particulier à des fins de commercialisation ou bien encore le tracking grâce aux cookies, etc.

iii) Que se passe-t-il si le sous-traitant est établi en dehors de l’UE ?

La grande question à se poser : les activités de traitement du sous-traitant «sont-elles liées» aux activités de ciblage du responsable du traitement ? Si la réponse est oui, alors le RGPD déploiera tous ses effets !

c) Qu'est-ce qu'un transfert ?

Comment identifier un transfert ?

Maintenant que nous savons reconnaître le territoire sur lequel le RGPD s’applique, interrogeons-nous sur le “transfert”.

Quels sont les critères sur lesquels les responsables du traitement et les sous-traitants de l’UE peuvent-ils s’appuyer pour déterminer si une opération de traitement constitue un transfert ?

Il y en a trois et ils sont cumulatifs :

1. l'exportateur de données (un responsable du traitement ou un sous-traitant) est soumis au RGPD ;
2. l’exportateur de données transmet ou met les données à caractère personnel à la disposition de l’importateur de données (un autre responsable du traitement, responsable conjoint du traitement ou sous-traitant) ;
3. l’importateur de données se trouve dans un pays tiers ou est une organisation internationale.

Observation : le comité européen de la protection des données considère que la collecte effectuée directement auprès des personnes concernées dans l’UE de leur propre initiative ne constitue pas un transfert.

Cas pratiques

Situation n°1 - Je travaille avec un sous-traitant hors UE

Je suis une société française et je crée un logiciel SAAS à destination de la France, de la Belgique et du Luxembourg. Je décide de sous-traiter une partie du développement technique en Inde. Pour cela, je dois leur transférer l'adresse de mes abonnés.

Que se passe-t-il pour moi sachant que je transmets des données personnelles ?

Il y a bien évidemment un transfert hors UE puisque :

- l'exportateur de données est la société française
- l'importateur de données est la société indienne

Situation n° 2 - Je suis une entreprise hors UE qui collecte des données personnelles d’Européens

Je suis une entreprise américaine et je propose des sneakers sur le marché européen (avec expédition). Je collecte des données lorsqu’une personne effectue un achat notamment pour envoyer la marchandise. Je propose aussi l'inscription à une newsletter.

Est-ce que géographiquement, je suis concernée par le RGPD ?

La réponse est oui puisque je cible spécifiquement le marché français (critère de ciblage vu précédemment).

Que se passe-t-il pour moi sachant que je collecte des données personnelles ?

Il n’y a pas transfert comme nous l’avons vu précédemment au regard de la position du comité européen de la protection des données car :

- l'exportateur de données est la société américaine
- l'importateur de données = néant puisque c’est le consommateur qui achète directement auprès de la société américain

Situation n°3 - Je suis un sous-traitant hors UE

Je suis un sous-traitant brésilien de produits exotiques. J’ai deux gros clients : un qui est Brésilien et l’autre qui est Français. Tous les produits commandés sont distribués en Europe.

Avec mon client brésilien (responsable de traitement), les activités de traitement effectuées par moi, le sous-traitant, sur instruction du responsable du traitement, sont liées à l’offre de biens aux personnes concernées dans l’Union. Donc, territorialement le RGPD s’applique. Pour autant, est-ce qu’il y a transfert des données hors UE ?
La réponse est oui puisque les 3 critères sont remplis.

Avec votre client français, il est évident que le RGPD s’applique (critère d’établissement). Il y a aussi transfert des données hors UE puisque vous êtes importateur de données dans un pays tiers.

Situation n°4 - J’ai des salariés hors UE

Je suis une entreprise française spécialisée dans l’impression photo et mon marché est européen. J’ai toutefois des salariés en Turquie qui s’occupent du produit final. Ces derniers m’envoient leurs données pour que je puisse établir des fiches de paie.

Ici, le RGPD s’applique, mais il n’y a pas transfert puisque l’entreprise française n’exporte pas des données mais en importe.

Situation n°5 - Je suis une filiale européenne d’une maison mère hors UE (ex-É.-U.)

La maison mère est une énorme start-up aux États-Unis, mais elle a développé deux filiales à Berlin et à Paris. Les salariés doivent donc transmettre leurs données à caractère personnel au Siège.

Ici, il y a transfert puisque la start-up est implantée dans l’UE et qu’à ce titre, la filiale est soumise au RGPD. Cette dernière est ici exportatrice et l'importateur est la maison mère. Il y a donc bien transfert.

Observation : qu’il y ait “transferts” ou non, le RGPD s’applique quoi qu’il en soit. L’intérêt de cette qualification permet tout simplement de définir le bon régime juridique.

Lorsqu’il n’y a pas “transferts”, les dispositions “pertinentes” du RGPD s’appliquent à partir du moment où l’entreprise est concernée par le champ d’application territorial du RGPD (selon le critère d’établissement ou le critère de ciblage).

Lorsqu’il y a transferts hors UE, un autre cadre réglementaire s’applique (le chapitre V du RGPD, pour être exact). C’est ce que nous allons vous expliquer dans le chapitre suivant.

3. EN CAS DE TRANSFERTS HORS UE

Transférer hors UE ?
C’est possible à condition que le pays ou l’entreprise destinataires assurent un niveau de protection suffisant et approprié...

QUE FAIRE EN CAS DE TRANSFERTS HORS UE ?

a) Un grand principe

Alors qu'entre États membres de l'UE, les données peuvent circuler librement, à charge pour lesdits États de respecter les dispositions du RGPD les concernant, quel est le grand principe qui régit les données qui sont transférées hors UE ?

En principe, il est interdit de transférer des données en dehors de l'Espace Économique Européen (EEE = UE+Islande, Norvège, Liechtenstein) SAUF si le pays ou l'entreprise destinataires assurent un niveau de protection suffisant et approprié.

b) Un niveau de protection suffisant : application concrète

Il existe une décision d’adéquation

Vous transférez des données hors UE ? La première question à vous poser : existe-t-il, oui ou non, une décision d’adéquation ?

Une décision d’adéquation est une décision prise par la Commission Européenne qui estime que l’État tiers offre un niveau de protection approprié après examen global de la législation en vigueur dans ledit Etat.

Si cette décision existe, plus de problème ! Dans ce cas de figure, les transferts vers un pays tiers « adéquat » seront assimilés à un transfert de données au sein de l’UE.

Pays offrant un niveau de protection approprié : Andorre, Argentine, Canada (pour les traitements soumis à la loi canadienne « Personal Information Protection and Electronic Documentation Act », autrement dit les traitements “commerciaux”), les îles Féroé, Guernesey, Israël, l’île de Man, Jersey, la Nouvelle-Zélande, Suisse, Uruguay, Corée du Sud, Royaume-Uni.

Pas de décision d’adéquation : les garanties appropriées prennent le relais

En l’absence de décision d’adéquation, un transfert peut avoir lieu grâce à la mise en place de garanties appropriées et à la condition que les personnes dont les données personnelles sont transférées disposent de droits opposables et de voies de droit effectives.

Les transferts hors UE reposent sur des fondements juridiques variés.

i) Règles internes d’entreprises (BCR)

Les règles d’entreprise contraignantes (communément appelées BCR) permettent à des groupes d’entreprises d’encadrer juridiquement leurs transferts de données hors de l’Union européenne (UE) tout en leur offrant la possibilité d’engager une démarche de mise en conformité globale à l’échelle de tout le groupe.

Les BCR constituent un outil d'encadrement global des transferts hors UE. C’est une alternative à d’autres outils permettant d’encadrer des transferts tels que les Clauses Contractuelles Types.

Observation : les autorités de protection des données sont en charge de l’évaluation et de la validation de ces conventions.

ii) Clauses contractuelles types adoptées par une autorité de contrôle et approuvées par la Commission européenne

Concrètement, la CNIL met à disposition les modèles de CCT adoptés par ladite commission. Ces derniers couvrent plusieurs situations :

- transfert de responsable de traitement à responsable de traitement ;
- transfert de responsable de traitement à sous-traitant ;
- transfert de sous-traitant à sous-traitant ;
- transfert de sous-traitant à responsable de traitement.

Toutefois, il incombe à l'exportateur et à l'importateur de données d'évaluer en pratique si la législation du pays tiers permet de respecter le niveau de protection requis par le droit de l’UE et les garanties fournies par les CCT. À défaut des mesures additionnelles devront être mises en place.

Observations :

- **les CCT ne peuvent pas être utilisées si l’importateur est soumis au RGPD (rendez-vous sur la partie compétence territoriale !) ;**
- **en cas de clause “ad hoc” (qui est une clause qui modifie les CCT approuvées par la Commission européenne), la CNIL devra donner son autorisation de transfert.**

iii) Code de conduite

Il s'agit d'un outil de conformité sectoriel **juridiquement contraignant : il s'impose à ceux qui y adhèrent**. L'élaboration d'un code de conduite repose sur une démarche sectorielle qui doit être initiée par une association, une fédération, ou un organisme représentant des catégories de responsables de traitement ou de sous-traitants.

Actuellement, il existe le code de conduite des fournisseurs d'infrastructures cloud relatif à la protection des données (**Cloud Infrastructure Service Providers Europe**).

Quelques exemples d'organismes agréés :

- Bureau Veritas Italia Spa
- EY CERTIFYPOINT
- Laboratoire national de métrologie et d'essai (LNE)

iv) Mécanisme de certification

La certification permet d'établir qu'un produit, un service, un processus ou un système de données ont été évalués conformes aux critères d'un référentiel préalablement approuvé par la CNIL ou par le Comité européen de la protection des données. La certification est un outil juridiquement contraignant pour ceux qui choisissent de s'engager dans cette démarche.

Exemple : une banque propose à ses clients un service en ligne qui leur permet de consulter et gérer leurs comptes. Pour obtenir la certification, le processus de traitement des données (adhésion au service, échanges, etc.) devra absolument respecter le référentiel.

À date, il existe très peu d'acteurs de certification et peu d'entreprises qui ont démarré cette démarche.

v) Un arrangement administratif

C’est un texte juridiquement contraignant et exécutoire pris pour permettre la coopération entre autorités publiques (Mémorandum of Understanding dit MOU ou MMOU, convention internationale…).

Exemples d’arrangements administratifs : Bureau Veritas Certification France, CESI certification, etc.

Pays n’offrant pas un niveau de protection approprié pour lesquels les garanties appropriées sont nécessaires : tous les pays qui ne figurent pas dans la liste citée précédemment, c’est-à-dire qui ne bénéficient pas de décision d’adéquation.

Concernant les États-Unis, l’arrêt Schrems II de la CJUE en date du 16 juillet 2020 a invalidé la décision d’adéquation à l’égard des États-Unis (Privacy Shield). D’après cette décision, pour transférer des données aux États-Unis, il faut adopter des garanties accompagnées de mesures de protection supplémentaires. Toutefois, dans un communiqué de presse en date du 25 mars 2022, la Commission indique que des discussions ont eu lieu avec le gouvernement américain pour la mise en place d’un nouveau cadre transatlantique. Affaire à suivre.

Les mesures de protection supplémentaires nécessaires

Les responsables du traitement ou les sous-traitants, agissant en tant qu'exportateurs, sont chargés de vérifier, au cas par cas et en collaboration avec l'importateur dans le pays tiers, si le droit ou la pratique du pays tiers compromettent l'efficacité des garanties appropriées.

Si tel n'était pas le cas, l'adoption de mesures supplémentaires serait requise. Parmi elles, on trouve :

- le format des données à transférer (c'est-à-dire en texte clair, pseudonymisées ou chiffrées) ;
- la longueur et la complexité du flux de traitement de données, le nombre d'acteurs intervenant dans le traitement et la relation entre eux ;
- la possibilité que les données puissent faire l'objet de transferts ultérieurs, dans le même pays tiers, voire vers d'autres pays tiers.

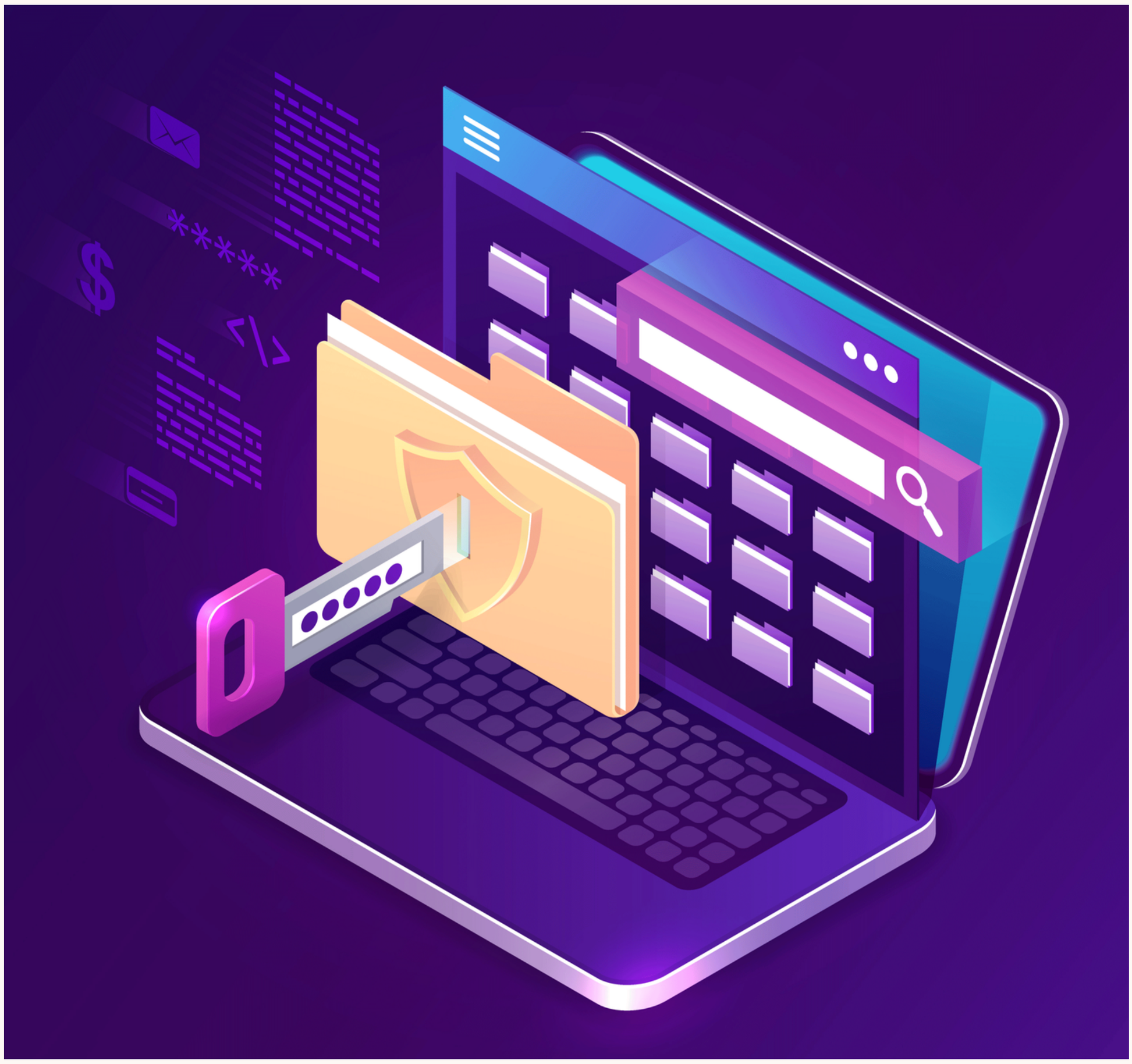
Cette liste n'est pas exhaustive. Nous vous invitons à lire les recommandations de l'EDP qui vous informe sur les mesures contractuelles, techniques et organisationnelles à appliquer.

Observation : si les mesures supplémentaires s'avéraient insuffisantes, vous seriez tenu de suspendre ou de mettre fin au transfert de données personnelles.

c) Les exceptions : quand peut-on s’affranchir du niveau de protection suffisant ?

Que se passe-t-il si un États tiers est dépourvu de décision d’adéquation ou de garanties appropriées ?

A priori, la situation est mal engagée. Heureusement, certaines dérogations existent, mais elles font l’objet d’une interprétation stricte. Ainsi, les transferts concernés doivent passer un test de nécessité, c’est-à-dire être occasionnels, non répétitifs et absolument nécessaires.



Cas 1 / La personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées.

Exemple : une entreprise française de montres de plongée collecte les adresses de ses clients pour livrer les articles commandés. Cette entreprise est rachetée par une entreprise australienne (État tiers) qui souhaite transférer les données à caractère personnel de ses clients à une entreprise située en Indonésie (État tiers) lorsqu'il s'agit de créer des modèles sur mesure. Pour que ce transfert soit valable en vertu de la dérogation relative au consentement, le client final doit donner son consentement à ce transfert spécifique au moment où celui-ci est envisagé.

Cas 2/ Le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à sa demande.

Exemple : une agence de voyage de luxe française spécialisée dans l’organisation de safaris sélectionne des lodges en Tanzanie ainsi que des tours opérateurs locaux. Afin de pouvoir délivrer l’offre promise, le transfert des données par l’agence de voyage est donc nécessaire aux fins du contrat car, dans ce cas, il existe un lien suffisamment étroit et important entre le transfert de données et la finalité du contrat (l’organisation du voyage du client)

Cas 3/ Le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale.

Exemple : une entreprise de costume traditionnel reçoit un client qui demande entre autres un gilet particulier dont le savoir-faire n’existe que chez un couturier situé au Liban. Il a été convenu que le gilet sera envoyé directement au domicile du client. Pour l’exécution de ce contrat, l’artisan demande certaines données pour accomplir sa tâche (comme les mensurations du client) et l’adresse (pour l’envoi de la commande). Dans ce cadre, l’exception est tout à fait admise.

Cas 4/ Le transfert est nécessaire pour des motifs importants d'intérêt public.

Exemple : échange international de données entre services chargés des questions relatives à la santé publique, par exemple aux fins de la recherche des contacts des personnes atteintes de maladies contagieuses.

Cas 5/ Le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice.

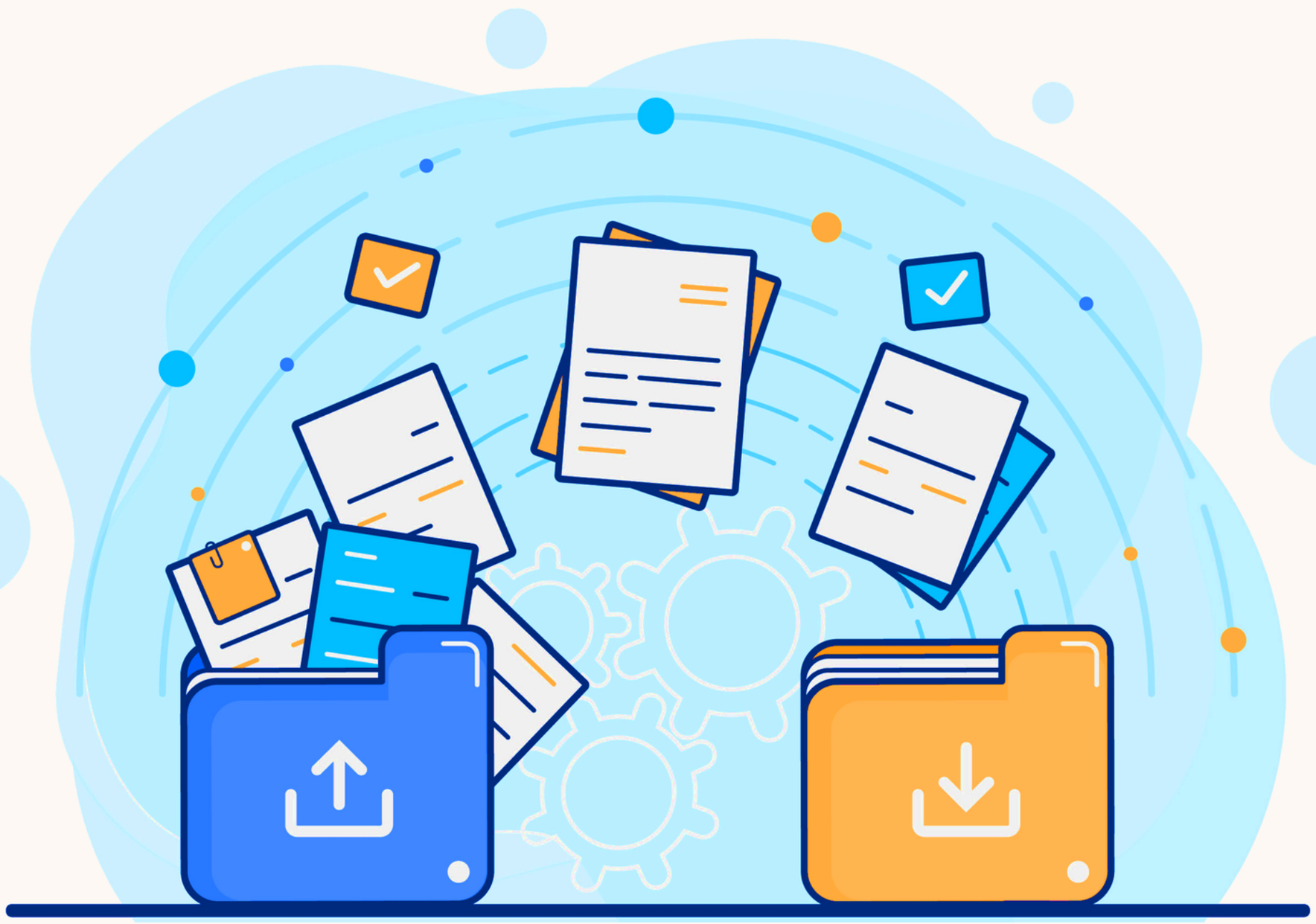
Exemple : la dérogation peut s’appliquer à un transfert de données afin de permettre à la personne concernée de se défendre par exemple dans les enquêtes antitrust, corruption, délit d’initié, etc.

Cas 6/ Le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement.

Exemple : une personne grièvement blessée en Argentine, dans le coma, dont le diagnostic vital est engagé, est hospitalisée. Une opération est nécessaire pour le maintenir en vie mais ce patient souffre d’une maladie chronique au regard des médicaments retrouvés sur lui. Les chirurgiens argentins ont besoin d’en savoir plus sur sa pathologie et seul son médecin en France (qui est considéré comme exportateur) est capable de donner les informations.

Cas 7/ Le transfert a lieu au départ d'un registre qui est légalement destiné à fournir des informations au public et est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime.

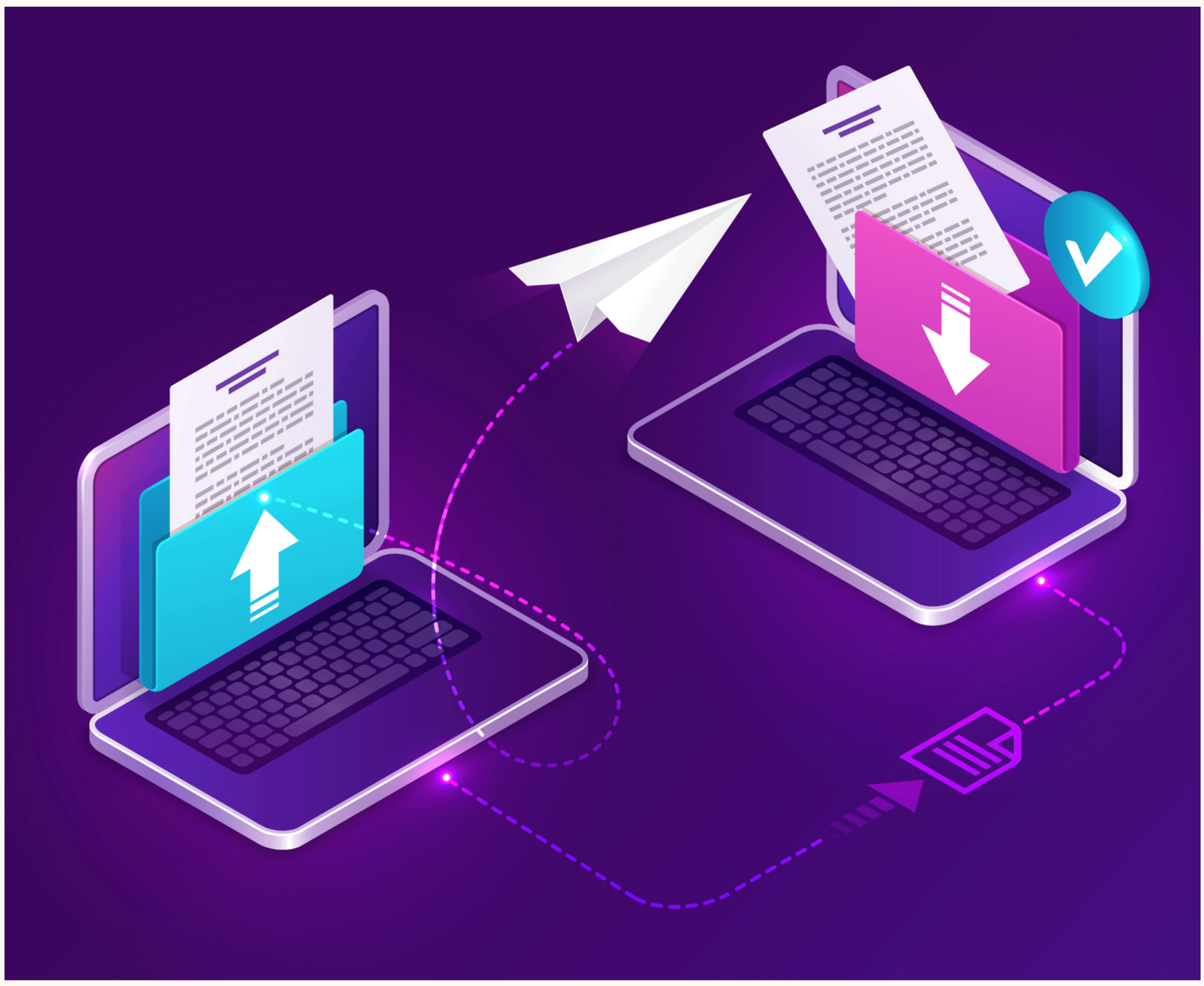
Exemple : registres d’entreprises, registres d’associations, registres de condamnations pénales, registres de propriétés (foncières) et registres de véhicules publics. Un transfert qui s’effectue au titre de cette dérogation ne peut porter sur la totalité des données à caractère personnel ni sur des catégories entières de données à caractère personnel contenues dans le registre. Les exportateurs de données, au moment d’évaluer si le transfert est approprié, doivent toujours prendre en considération les intérêts et les droits de la personne concernée.



Derniers recours : lorsqu'aucune de ces dérogations n'est applicable, il est possible de procéder au transfert sous réserve de respecter des conditions cumulatives.

Le transfert :

- ne revêt pas de caractère répétitif,
- ne touche qu'un nombre limité de personnes concernées,
- est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée,
- et si le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et a offert, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel.



d) Comment choisir ses sous-traitants ?

Étape 1 : vérifier si le pays importateur respecte le RGPD

Recenser les transferts : exhaustivité et classement

Il est bon de rappeler que la définition d’une donnée personnelle est large puisqu’il s’agit de toute information, informatisée ou non, relative à une personne physique susceptible d’être identifiée directement ou indirectement.

Exemples : un nom, une photo, une adresse postale, une adresse mail, un numéro de téléphone, un matricule interne, une adresse IP, un identifiant de connexion informatique, un identifiant de base de données, mais aussi les images issues d’une vidéosurveillance, d’un système de paiement, etc.

Concrètement, pour être exhaustif, pensez à énumérer :

- toutes les catégories de personnes dont vous possédez les données : clients, prospects, visiteurs de votre site, salariés, etc.
- tous les prestataires, comme les outils et les services, auxquels vous faites appel et qui nécessitent un transfert de données hors UE.

Cette étape est indispensable et elle est même requise puisque vous avez pour obligation de tenir un registre des activités de traitement.

La bonne nouvelle ?

Leto vous aide à dresser automatiquement l'inventaire des données personnelles présentes dans votre organisation de manière automatisée.

Choisir de préférence un prestataire dans l'UE ou provenant d'un pays reconnu comme adéquat.

Dans l'idéal et si vous en avez la possibilité, privilégiez des prestataires situés dans l'UE ou dans un pays reconnu comme adéquat.

À défaut, vous aurez pour mission d'évaluer la législation du pays tiers vers lequel les données sont transférées et éventuellement de mettre en œuvre, en plus des garanties appropriées (comme les CCT), des mesures supplémentaires pour assurer un niveau suffisant de protection des données.

Exemple 1 : préférez Matomo à Google Analytics

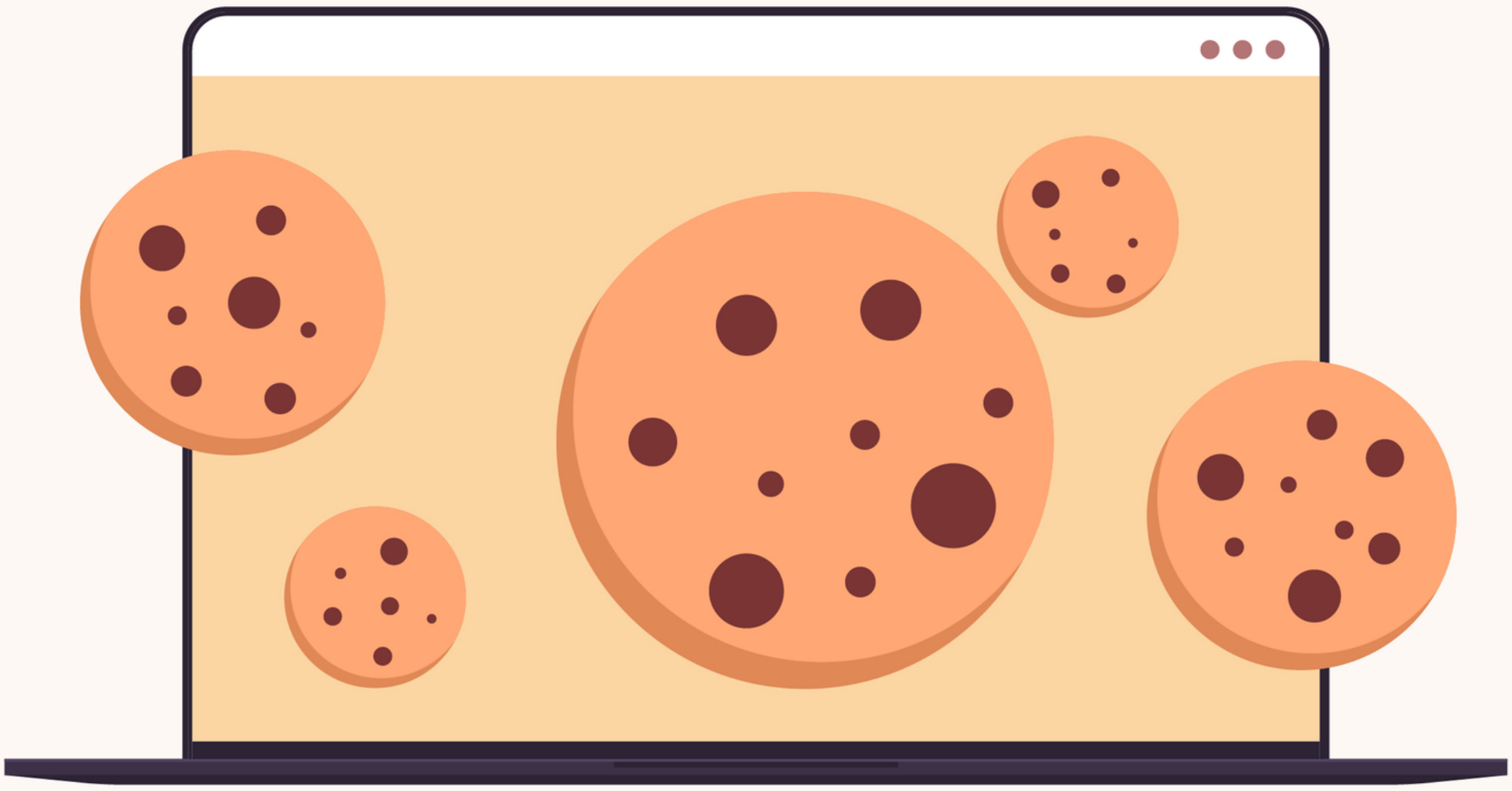
Il a ainsi été reproché à Google Analytics d'obtenir l'adresse IP de l'internaute ainsi que de nombreuses informations sur son terminal permettant l'accès à sa navigation sur l'ensemble des sites ayant recours à Google Analytics. La simple mise en œuvre de clauses contractuelles types n'est évidemment pas suffisante pour que Google Analytics soit en conformité avec le RGPD.

Une solution possible est celle de l'utilisation d'un proxy pour éviter tout contact direct entre le terminal de l'internaute et les serveurs de l'outil de mesure. Mais, au regard de la complexité de la solution, mieux vaut préférer Matomo recommandé par la CNIL.

Exemple 2 : éliminez le bandeau de cookies et adoptez Plausible

Chez Leto, nous avons effectué un choix radical : nous n’avons recours qu’à des cookies indispensables au bon fonctionnement du site. Autrement dit, nous avons dit adieu à Google Analytics, au CRM et au retargeting. C’est un engagement éthique de notre part qui, il est vrai, réduit notre potentiel marketing. Mais, nous tenions à respecter à 100% la vie privée de nos visiteurs.

Pour nos besoins, nous avons adopté Plausible, un outil 100% européen et simple d’usage. En savoir plus.



Etape 2 : analyser les DPA et les engagements de vos sous-traitants

Qu’est-ce qu’un DPA ?

Un DPA (Data Processing Agreement ou Accord de Traitement des Données) est un contrat conclu entre le responsable de traitement et le sous-traitant précisant la façon dont ce dernier va utiliser les données qui lui ont été confiées dans le cadre de la mission qui lui a été assignée.

Ce document définit clairement l’objet, la durée, la nature et la finalité du traitement, les catégories de données à caractère personnel et de personnes concernées ainsi que les obligations et les droits du responsable du traitement. Il précise aussi les conditions dans lesquelles le sous-traitant peut recourir lui-même à un sous-traitant.

En pratique, chaque sous-traitant qui travaille sur le territoire de l’UE dispose d’un DPA. Il vous suffit de taper sur Google « Data Processing Agreement » ou « Accord de traitement des données » et le nom de votre prestataire.

La bonne nouvelle ?

Leto vous aide dans cette tâche fastidieuse. Nous collectons automatiquement les DPA.

Quels sont les points de vigilance pour vous ?

En fonction du service et des outils que vous utilisez, nous vous recommandons de procéder à certaines vérifications.

i) La vérification des données collectées par votre prestataire

Il vous appartient de veiller à 3 éléments :

- l’utilité réelle de la quantité et de la qualité des informations récoltées par votre sous-traitant ;
- les fonctionnalités proposées par votre prestataire en matière de consentement : lien de désinscription, demande du consentement, modèle d’information des personnes, purge des données des personnes, etc.
- la suppression, le renvoi des données au terme de la prestation de services, et même la destruction des copies existantes, à moins que le droit de l'Union ou de l’État destinataire n'exige la conservation des données à caractère personnel.

ii) La vérification des garanties des sous-traitants choisis par votre sous-traitant

Choisir un sous-traitant conformément aux exigences du RGPD n'est qu'une étape. En effet, que se passe-t-il si ce sous-traitant fait appel lui-même à un autre sous-traitant (qui soit d'ailleurs hors UE ou non) ?

La réglementation prévoit deux façons de procéder :

- soit il faut une autorisation écrite du responsable de traitement ;
- soit il existe une autorisation qui a une portée générale. Dans ce cas de figure, le sous-traitant doit vous informer de la liste de ses propres sous-traitants, à charge pour vous d'émettre des objections si ces derniers ne vous conviennent pas.

Vous l'avez deviné, en tant que responsable de traitement, vous avez pour mission de vous assurer du sort final et de la sécurité des données que vous confiez.

iii) La vérification du traitement d’exercice des droits (accès, rectification, effacement, limitation, portabilité)

Votre sous-traitant doit vous assister dans la mise en œuvre technique des suites apportées aux demandes d’exercice des droits.

Organisez les modalités de cette assistance. La solution fournie par le sous-traitant doit vous proposer des fonctionnalités vous permettant de répondre rapidement. En effet, suite aux demandes des personnes exerçant leurs droits, vous avez un délai d'un mois maximum à compter de la réception de la demande pour y répondre (3 mois pour une demande complexe, 8 jours pour des données de santé).

Leto le fait pour vous

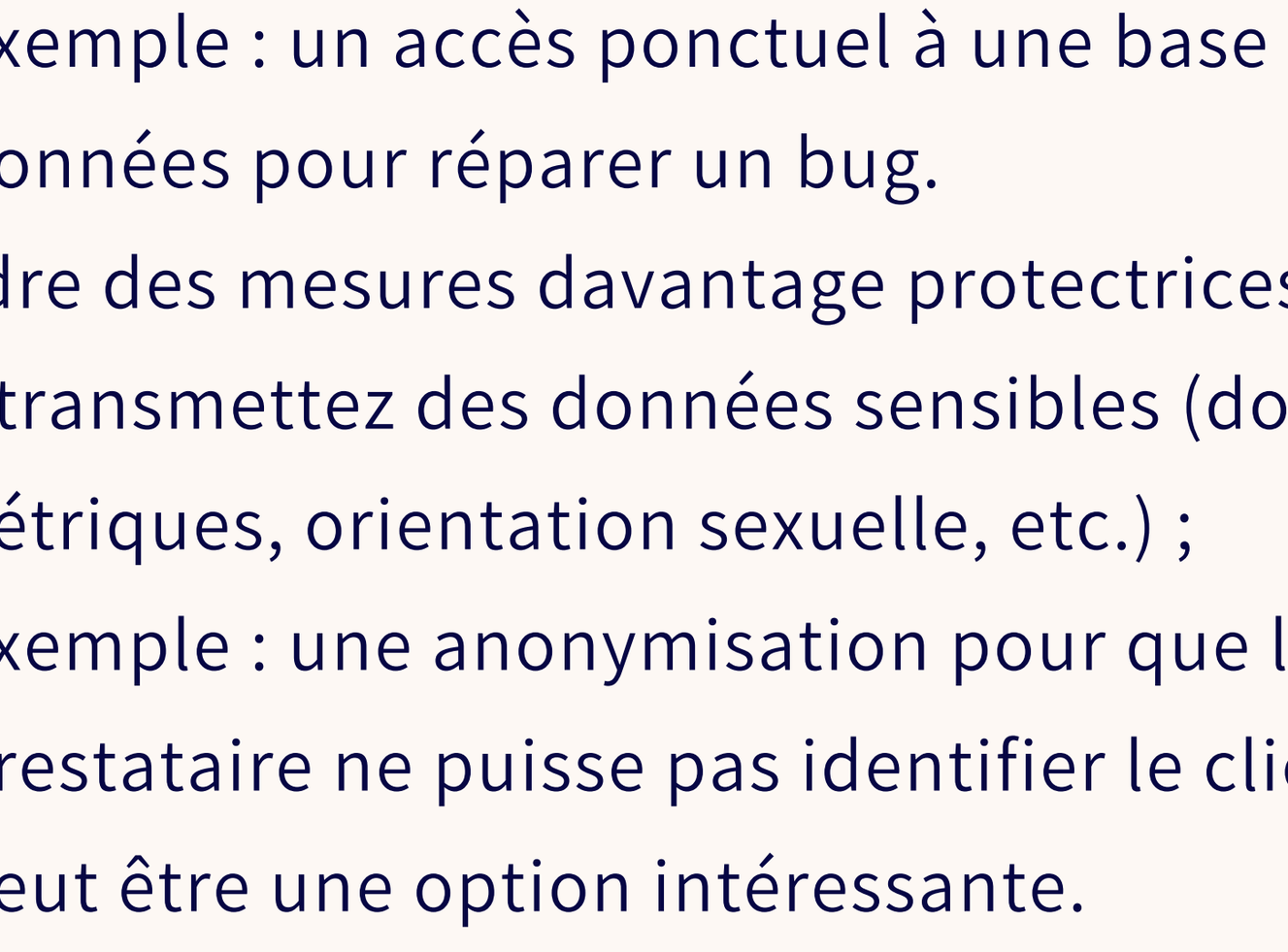
Avec son module d’exercice de droit, Leto vous permet de mettre en place le processus du traitement des demandes d’exercice de droit, que vous soyez responsable de traitement ou sous-traitant.

Étape 3 : limiter et sécuriser les transferts de données personnelles

Contrôler les transferts de données personnelles à votre sous-traitant

Nous vous invitons à :

1. transférer les données strictement nécessaires à la réalisation de la mission et diminuer ainsi le volume d'informations transmises à votre prestataire ;
    - Exemple : si une adresse mail est suffisante, inutile de communiquer le numéro de téléphone.
2. limiter la durée de conservation des données transférées. Le sous-traitant doit y avoir accès seulement le temps de sa mission ;
    - Exemple : un accès ponctuel à une base de données pour réparer un bug.
3. prendre des mesures davantage protectrices lorsque vous transmettez des données sensibles (données biométriques, orientation sexuelle, etc.) ;
    - Exemple : une anonymisation pour que le prestataire ne puisse pas identifier le client final peut être une option intéressante.



Signer les CCT

L’importance des CCT dans le transfert des données hors UE

Pour rappel, les clauses contractuelles types sont des modèles de contrats de transfert de données personnelles adoptés par la Commission Européenne.

Elles fonctionnent par module pour répondre à divers scénarios de transfert :

- module 1 : RT à RT ;
- module 2 : RT à ST ;
- module 3 : ST à ST ;
- module 4 : ST à RT.

Attention ! Désormais, les CCT sont imposées dans les relations avec les sous-traitants ultérieurs.

Exemple : vous êtes une entreprise française proposant en BtoC des souvenirs familiaux en motion design. Vous sous-traitez une partie de votre interface à une entreprise indienne A qui a besoin des adresses mail des clients finaux pour leur donner accès à la création. Cette même société indienne ayant beaucoup de succès mandate elle-même un prestataire indien B qui est donc un sous-traitant ultérieur.

Entreprise française à entreprise indienne A = module 2 + DPA

Entreprise indienne A à entreprise indienne B = module 3 + DPA

Ces documents sont contractuels. Pour les rendre juridiquement contraignants, les CCT et les DPA doivent être signés par les parties concernées. Leto vous permet d’ailleurs de tout centraliser au même endroit !

Le contenu des CCT

On y trouve bien évidemment les parties concernées mais aussi :

- la description du transfert : catégories de personnes concernées, catégories de données transférées, durée du transfert, fréquence, durée de conservation ou lorsque ce n’est pas possible, critères utilisés pour déterminer cette durée, etc.
- l'autorité de contrôle compétente ;
- les mesures techniques et organisationnelles pour chacun des transferts : pseudonymisation, chiffrement des données à caractère personnel, procédures visant à tester, à analyser et à évaluer régulièrement l’efficacité des mesures techniques et organisationnelles afin de garantir la sécurité du traitement, mesures d’identification et d’autorisation de l’utilisateur, mesures de protection des données pendant la transmission, mesures de protection des données pendant le stockage, etc.
- la liste des sous-traitants ultérieurs.

Retrouvez les CCT sur le site de la Commission Européenne.

Analyser les mesures de sécurité proposées

Lorsque vous choisissez un sous-traitant hors UE ou non, vous devez vérifier qu'il présente des garanties suffisantes en termes de sécurité.

La CNIL vous recommande :

- d'exiger la communication par le prestataire de sa politique de sécurité des systèmes d'information ;
- de documenter l'effectivité des garanties offertes par le sous-traitant en matière de protection des données.

Le RGPD précise d'ailleurs que le sous-traitant a pour obligation de vous mettre à disposition toutes les informations nécessaires pour démontrer le respect de ses obligations.

Les moyens à votre disposition : audit de sécurité, visite des installations, vérification des certifications de l'organisme, formation des équipes au RGPD, signature d'une clause de confidentialité pour les salariés du sous-traitant, etc.

d) Transformer les enjeux de transferts en un argumentaire commercial

Démontrer sa connaissance des sous-traitants

Alors que la CNIL met de plus en plus de pression sur les outils américains, concomitamment, 87% des Français se déclarent sensibles à l'enjeu de protection des données. La problématique juridique du RGPD devient éminemment politique et commerciale.

Afin de ne pas être pris en défaut sur ces questions, vous devez prouver :

- votre maîtrise sur les transferts hors UE : les prestataires, les pays concernés, les raisons des transferts, les données transférées ;
- votre implication dans le suivi sur le plan technique et juridique des flux hors UE dans le cadre de votre activité.

Pour mener cette mission à terme, mettez en place des outils de suivi :

- tableur spécifique recensant les outils numériques concernés, les contrats et prestataires, l'existence de flux de données hors UE, leur destination, ainsi que l'encadrement juridique de ces flux ;
- diagramme des flux de données maintenu à jour.

Leto peut vous aider ! Nous disposons d'une base de plus de 6000 outils référencés (Slack, Mailchimp, Alan, Payfit, etc) et nous cartographions les données personnelles présentes dans vos applications automatiquement.

Formaliser pour vendre plus efficacement

Les CCT sont la base légale incontournable pour permettre le transfert des données hors UE. Signées, elles sont contraignantes aussi bien pour le responsable de traitement que les sous-traitants et nous vous conseillons d’en transmettre une copie à vos prospects.

Prouver que vous êtes continuellement à jour sur la question du traitement des données est un avantage concurrentiel. Vos futurs clients seront de plus en plus pointilleux sur la question de la protection des données.

Ils le seront en fonction :

- du domaine dans lequel vous évoluez : santé, juridique, ressources humaines, SAAS, etc.
- de la politique de transparence de l’entreprise : la protection des données devient alors un élément marketing ;
- du risque qu’ils encourent en cas de violation du RGPD : à vous de le leur communiquer.

Leto peut vous aider ! L’un des enjeux est l’exercice des droits de la personne dont les données ont été traitées. Cette question est complexe lorsque la demande émane de votre client et que les données en question sont également chez votre sous-traitant. Chez Leto, vos clients disposent d'une interface dédiée pour exercer leurs droits en matière de protection des données. 100% no code.

Construire une feuille de route de rapatriement des données personnelles, notamment celles qui sont sensibles

Le désaveu de Google Analytics par la CNIL laisse présager que d'autres outils américains ou hors UE vont connaître un sort analogue. Nous vous invitons à mener une réflexion globale sur les outils que vous utilisez pour prévoir le passage progressif à un prestataire ou à une zone de stockage dans l'UE.

Pour ce faire, et dans la mesure où il serait utopique de vouloir rapatrier toutes vos données immédiatement, établissez un ordre de priorité dans un calendrier opérationnel :

- privilégier la relocation des données sensibles ;
- choisir un hébergement français ;
- sélectionner un outil d'analyse européen ;
- remplacer les messengers entreprises par une solution européenne, etc.

e) Quels outils utiliser ?

Les outils no code : ce que vous devez vérifier

De nouveaux outils made in USA séduisent de plus en plus les entreprises et les start-up européennes :

- Notion
- Bubble
- Airtable
- Webflow
- Adalo
- etc.

Mais, nous avons vu que l'invalidation du Privacy Shield le 16 juillet 2020, par la CJUE (Cour de justice de l'Union européenne) et l'arrêt Schrems II, exige de vous un encadrement strict pour transférer les données personnelles.

Pour rappel, voici les outils juridiques et techniques à votre disposition :

- les CCT
- les mesures supplémentaires (pseudonymisation, chiffrement, etc.)
- l'adoption d'un code de conduite
- la tenue d'un registre
- etc.

Les outils français : de plus en plus d’alternatives

Ils sont de plus en plus nombreux et la bonne nouvelle, c’est que les entreprises du numérique françaises sont très attentives au respect du traitement des données.

D’ailleurs, certaines d’entre elles en font un argument commercial.

Toutefois, en tant que responsable de traitement, pensez à vérifier :

- le DPA ;
- le lieu d’hébergement de l’outil.

Voici une liste non exhaustive d’outils made in France ou made in Europe pour développer votre business :

- Matomo : logiciel libre d'analyse d'audience qui protège vos données et la vie privée de vos clients
- Dropcontact : solution de cleaning de données de contacts 100% RGPD compliant
- Atolia : slack français qui est conforme à notre réglementation
- Eval&Go : outil français pour créer un questionnaire en ligne en quelques clics
- Tally : solution belge pour des formulaires conformes aux prescriptions réglementaires
- TarteAuCitron : gestionnaire de cookies qui respecte la vie privée de vos visiteurs
- Private Discuss : application cybersécurisée et RSE qui est une alternative à Teams
- pCloud : stockage en ligne le plus sécurisé d’Europe qui compte déjà 16 millions d’utilisateurs
- Sellsy : CRM avec un engagement fort sur l’environnement, le social et bien sûr le respect des données personnelles
- leto.legal : la solution conforme RGPD qui vous aide à mettre en place les outils RGPD !

4. CONCLUSION

Transfert des données hors UE : priorisez vos chantiers et privilégiez des solutions européennes !

CONCLUSION

La transparence et l’éthique sont des valeurs plébiscitées par les consommateurs qui sont désormais attentifs aux engagements des acteurs économiques.

Le transfert des données personnelles hors UE est donc une question cruciale pour le développement de votre entreprise. Par conséquent, il vous appartient de contrôler si vos actions à l’étranger fragilisent la sécurité et l’intégrité des données qui vous sont confiées.

Pour atteindre vos objectifs de conformité, vous devez :

- collecter toutes les données que vous transférez en dehors de l’UE ;
- auditer tous vos outils et vos partenaires choisis ;
- vérifier les DPA et les sous-traitants de vos propres sous-traitants ;
- analyser les risques de chaque transfert ;
- mettre en place des mesures techniques, contractuelles, organisationnelles ;
- former et sensibiliser vos collaborateurs,
- suivre avec attention la mise à jour des registres, etc.

Ces missions extrêmement chronophages sont pourtant essentielles pour maîtriser votre conformité et prouver votre implication en cas de contrôle de la CNIL.

Une telle complexité nécessite de plus en plus l'intervention des "Privacy Ops" dont le rôle est d'orchestrer la mise en place de mesures de protection des données et de jongler entre les différentes réglementations internationales.

Il doit aussi avoir cette faculté d'endosser un rôle transversal pour coopérer avec les équipes sur le terrain sans lesquelles il est impossible d'implémenter des solutions durables. L'automatisation sera la clé de voûte du succès de sa mission.

Adopter un outil collaboratif qui analyse les risques en temps réel, suit les requêtes et uniformise le traitement des données est donc un préalable pour les entreprises en quête de conformité.

À terme, la vraie victoire serait que les collaborateurs intègrent dans leur quotidien l'utilisation de l'outil choisi et prennent des décisions éclairées à la lumière des enjeux relatifs à la protection des données.

LETO.LEGAL

CONTACTEZ-NOUS

VOUS ÊTES À DEUX DOIGTS DE VOTRE CONFORMITÉ

E-MAIL :
contact@leto.legal

SITE WEB :
leto.legal