CHAMBRE DE COMMERCE ET D'INDUSTRIE

LES TRANSFERTS DE DONNÉES

À CARACTÈRE PERSONNEL

Sommaire

En France, la loi Informatique et Libertés du 6 janvier 1978 encadre strictement le traitement des données à caractère personnel dont elle donne la définition suivante : « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.[1]»
Celle loi prévoit notamment de déclarer à la CNIL (Commission Nationale de l'Informatique et des Libertés) tout fichier comportant des données à caractère personnel.

Transposant par la suite la directive européenne 95/45/CE parue en 1995, la législation française s'est étoffée afin d'encadrer également le transfert des données à caractère personnel en dehors de l'Union Européenne (UE).

L'article 68 de la loi Informatique et Libertés les interdit.

En revanche, sont autorisés les transferts dans les pays ou les entreprises étrangères garantissant un niveau suffisant de protection des données transférées. Il convient néanmoins de remplir quelques formalités afin d'obtenir la validation officielle de la CNIL.
Le non-respect de ces règles peut entrainer une condamnation par une juridiction européenne à une amende jusqu'à 300 000 euros pour une personne physique et 1,5 millions d'euros pour une personne morale, ainsi que 5 ans d'emprisonnement. La CNIL peut quant à elle infliger une sanction pécuniaire allant de 150 000€ pour le premier manquement à 300 000€ en cas de manquements réitérés ou 5% du chiffre d'affaires dans la limite de 300 000€ pour les entreprises.

Nul besoin d'être une multinationale pour avoir besoin de transférer des données à caractère personnel en dehors de l'UE : toute entreprise souhaitant, par exemple, sous-traiter son Service Après-Vente en dehors de l'UE - ou utilisant une CRM en mode SaaS dont les données sont stockées sur un serveur hébergé à l'étranger - doit se mettre en conformité avec la loi.

Cette notice traite de la règlementation en vigueur selon le pays destinataire des données transférées et des formalités à accomplir.

RÈGLES RELATIVES AUX DONNEES PERSONNELLES

Que ce soit sur le territoire européen ou à l'étranger, le transfert de données à caractère personnel est soumis aux mêmes obligations imposées par la loi Informatiques et Libertés :

COLLECTE DES DONNÉES

Dans un premier temps, il convient de recueillir le consentement de la personne concernée par ce transfert pour utiliser une information qui l'identifie. Les données traitées doivent être exactes, complètes et à jour.
Sauf dérogation, ces données ne doivent pas relever d'un caractère « sensible » : origines raciales ou ethniques, opinions politiques, philosophiques ou religieuses, appartenance syndicale, orientation sexuelle, informations médicales).

FINALITÉ DU TRAITEMENT

Un fichier doit avoir un objectif précis et les informations exploitées dans un fichier doivent être cohérentes par rapport à cet objectif.
Les informations ne peuvent pas être réutilisées de manière incompatible avec la finalité pour laquelle elles ont été collectées.

DURÉE DE CONSERVATION DES DONNÉES

Les données personnelles ont une date de péremption. Le responsable d'un fichier fixe une durée de conservation raisonnable en fonction de l'objectif du fichier.

SÉCURITÉ DES FICHIERS

Tout responsable de traitement informatique de données personnelles doit adopter des mesures de sécurité physique (liée à la sécurité des locaux) et logique (liées à la sécurité du système d'information) adaptées à la nature des données et aux risques présentés par le traitement.

CONFIDENTIALITÉ DES DONNÉES

Seules les personnes autorisées peuvent accéder aux données personnelles contenues dans un fichier. Il s'agit :

- → des destinataires explicitement désignés pour en obtenir régulièrement communication
- → des « tiers autorisés » ayant qualité pour les recevoir de façon ponctuelle et motivée (ex : la police, l'administration fiscale, etc.)

INFORMATION DES PERSONNES

Le responsable d'un fichier doit permettre aux personnes concernées d'exercer pleinement leurs droits.
Pour ce faire, il doit leur communiquer son identité, la finalité de son traitement, le caractère obligatoire ou facultatif des réponses, les destinataires des informations, l'existence des droits des personnes (accès, rectification et suppression des données), les transferts envisagés.

DÉCLARATION DES FICHIERS

Certains traitements informatiques de données personnelles qui présentent des risques particuliers d'atteinte aux droits et aux libertés doivent, avant leur mise en œuvre, être déclarés ou soumis à la CNIL.

RÈGLES RELATIVES AUX TRANSFERTS

La loi Informatique et Libertés distingue plusieurs cas de transferts selon le pays « importateur » de données.

TRANSFERTS VERS UN PAYS HOMOLOGUE PAR L'UE

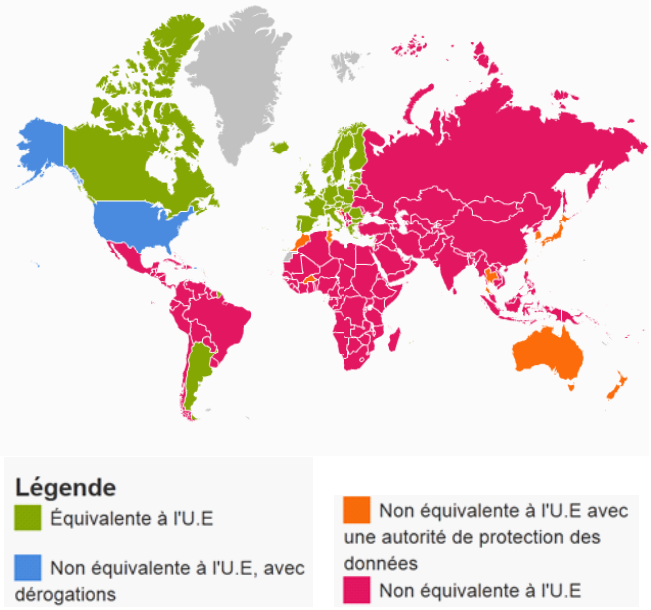
La Commission Européenne considère que certains pays possèdent une législation assurant un niveau de protection suffisant pour les données personnelles. Il s'agit des pays suivants :

- → Andorre, Argentine, Canada, Iles Féroé, l'Ile de Man, Guernesey, Jersey, Israël, Uruguay, Suisse. Cette liste pouvant évoluer dans le temps, la CNIL la tient à jour sur son site internet : http://bit.ly/d6wYTm

- → 3 pays de l'Espace Economique Européen non membres de l'Union Européenne ayant transposé la directive 95/46/CE dans leur législation : Norvège, Islande, Lichtenstein

Le transfert de données à caractère personnel vers ces pays n'implique aucune formalité supplémentaire (en vert sur la carte page suivante).

Législations nationales en matière de protection des données personnelles



TRANSFERTS VERS LES ETATS-UNIS

En 2001, la Commission Européenne a négocié avec le Département de Commerce des Etats-Unis un ensemble de principes de protection des données personnelles basés sur la directive 95/46/CE. Cet accord a donné lieu à la certification Safe Harbor, renouvelable tous les ans et à laquelle les entreprises américaines sont libres d'adhérer.

Seuls les transferts de données personnelles vers des entreprises adhérant au Safe Harbor sont autorisés par la CNIL.

Le Département de Commerce des Etats-Unis tient à jour la liste de ces entreprises en ligne : https://safe-harbor.export.gov/list.aspx.
La colonne « Certification Status » indique si la certification de l'entreprise a été renouvelée (current).

La consultation des fiches « entreprises » du site permet de s'assurer que l'adhésion de l'entreprise couvre bien le transfert envisagé.

TRANSFERTS ENTRE LES ENTITÉS D'UN GROUPE

Afin de faciliter les transferts de données entre ses différentes entités, une multinationale peut adopter un code de conduite interne définissant la politique du groupe en matière de protection des données personnelles. Ces Binding Corporate Rules (BCR) doivent être respectées par toutes les entités et salariés de la multinationale, quel que soit leur pays d'implantation.

Les transferts de données sur la base des BCR seront autorisés après validation de plusieurs autorités européennes de protection des données, équivalentes à la CNIL (schéma page suivante). L'entreprise doit au préalable saisir l'une de ces autorités, dite « chef de file » qui jouera un rôle d'interface au fil des étapes de validation des BCR.

Site répertoriant les entreprise adhérentes au Safe Harbor


Search by Organization Details Hide Details (...)

Organization Name:

Search Tip: Enter either (a) the exact Organization Name (e.g. The XYZ Corporation); or (b) the % symbol immediately before (i.e. no space) a word of consequence from the Organization Name (e.g. %XYZ)

Keyword:

Search Tip: Enter the Organization Contact name, Corporate Officer name, Independent Recourse Mechanism, Verification Method or Zip Code

Industry Sector:

State:

Search

Search by Organization Certification Status Hide Details (...)

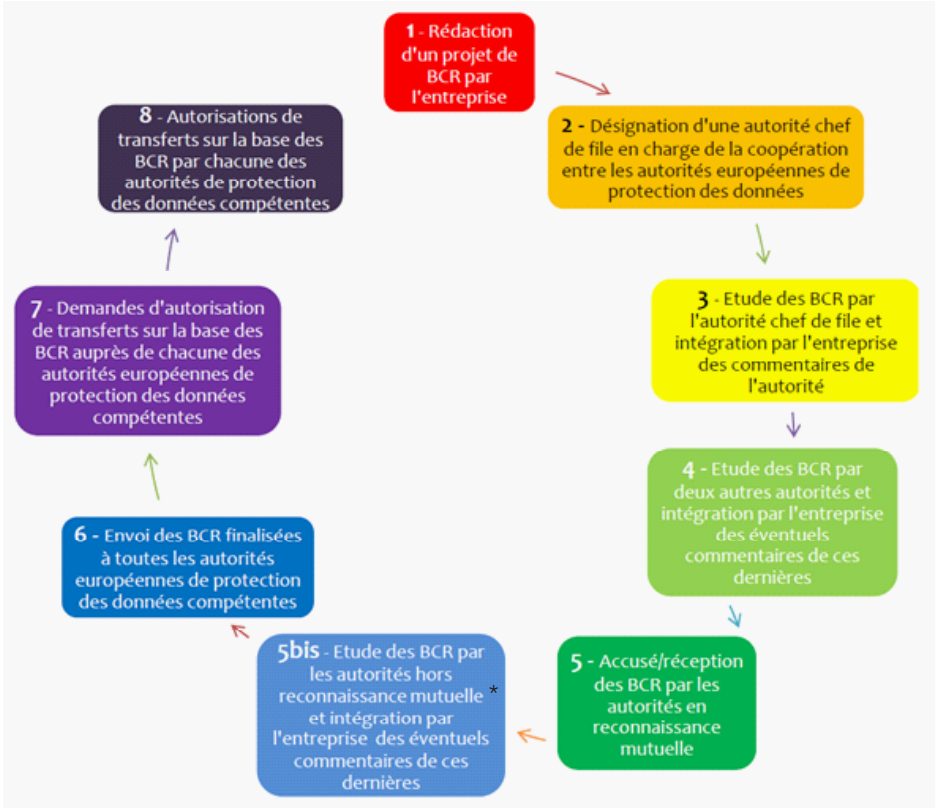
Certification Status:

Search Alphabetically for Organization Name Hide Details (...)

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z ALL

Organization	Certification Status	Personal Data
@ legal discovery LLC	Current	All personal data/On-line/On-line
1-800-HOSTING, Inc.	Current	off-line, on-line, manually processed data
100 Spears, LLC d/b/a eWork	Not Current	On-line, off-line, human resource data
101 Distribution	Not Current	on-line, off-line
1010data Global Telecom Solutions LLC	Not Current	All PII is denatured prior to being sent to 1010data. No such data is manually processed.

Processus de validation des BCR



* 21 Etats membres de l'Espace Economique Européen font partie de la reconnaissance mutuelle : Royaume-Uni, Royaume-Uni, Royaume-Uni, Bulgarie, Chypre, Royaume-Uni, Estonie, Royaume-Uni, Royaume-Uni, Islande, Royaume-Uni, Lettonie, Liechtenstein, Royaume-Uni, Malte, Norvège, Pays-Bas, République Tchèque, Royaume-Uni, Slovénie et Slovaquie.

Source : « Les transferts de données à caractère personnel hors Union Européenne » - CNIL / 2012
Téléchargeable sur le site de la CNIL : http://bit.ly/d7NCWA

La CNIL met à disposition une trame de BCR et une liste de critères à respecter pour obtenir la validation des BCR.[2]

TRANSFERT VERS TOUT AUTRE PAYS

Dans tout autre cas, les transferts de données personnelles hors de l'UE doivent être encadrés par des clauses contractuelles types. Ce document est conclu entre l'entreprise européenne et l'entreprise étrangère à qui elle souhaite transférer les données personnelles.
La Commission Européenne distingue deux types de clauses selon le statut de l'entreprise importatrice de données personnelles :

- → **Responsable de traitement** : ce statut signifie que l'entreprise est autonome dans le traitement des données transférées
- → **Sous-traitant** : dans ce cas l'entreprise agit pour le compte de l'entreprise exportatrice de données personnelles

[2] Téléchargeables à cette adresse : http://bit.ly/V6NPj5

La CNIL donne un exemple permettant de mieux comprendre cette distinction par le biais d'indices (tableau page suivante).
La distinction entre les deux statuts s'explique par des différences de responsabilités, de règlements de litige et de modalités de recours pour les personnes dont les données ont été transférées.
Une entreprise importatrice de données considérée comme « responsable de traitement » est sur un pied d'égalité avec l'entreprise exportatrice de données. En cas de manquements aux clauses contractuelles types, chaque partie est responsable des dommages causés envers l'autre partie et les personnes concernées par les données. Si ces dernières estiment, par exemple, que leurs droits ont été violés, elles pourront poursuivre l'exportateur et l'importateur en justice pour manquements respectifs.

Si, en revanche, l'entreprise importatrice de données est considérée comme « sous-traitant », l'exportateur est seul responsable et endossera toutes les responsabilités si les clauses contractuelles types ont été violées.

Indices	Le prestataire pourra être qualifié de sous-traitant	Le prestataire pourra être qualifié de responsable de traitement
Transparence : Le prestataire de service se présente-t-il sous son nom propre ou sous le nom de son client ?	L'employé du centre d'appel en Tunisie se présente sous le nom du client.	Le centre d'appel en Tunisie se présente sous son propre nom.
Niveau d'instruction : Le niveau d'instruction donné par le client indique le degré d'autonomie laissé au prestataire. Par conséquent, il permet d'apprécier s'il est plus qu'un simple sous-traitant.	Le contrat de prestation et les directives données au cours de son exécution sont très précis dans les instructions et le niveau de qualité demandé.	Le contrat de prestation et les directives données au cours de l'exécution sont très généraux en termes d'instruction et laissent expressément une grande autonomie au prestataire.
Niveau de contrôle : Le degré de contrôle du client sur les prestations et sur les données révèle également la liberté dont peut disposer le prestataire.	La société audite son prestataire et lui demande des comptes régulièrement.	La société ne s'intéresse pas à la façon dont le prestataire réalise ses prestations et le laisse libre d'utiliser les données comme bon lui semble.
Expertise : Un prestataire qui dispose d'une expertise peut ainsi décider des moyens à mettre en place dans le cadre de la réalisation des prestations.	Le prestataire utilise l'infrastructure technique du client pour réaliser sa prestation.	Le prestataire expert dans son domaine impose des outils au client qui n'a pas de pouvoir de négociation, ne peut les modifier parce qu'il n'a pas les compétences, ou parce que l'outil est un outil qui ne fait pas l'objet d'un développement spécifique.

Source : « Les transferts de données à caractère personnel hors Union Européenne » - CNIL / 2012
Téléchargeable sur le site de la CNIL : http://bit.ly/d7NCWA

Deux modèles de clauses contractuelles types sont donc à disposition des entreprises[3]. Une validation de la CNIL n'est pas nécessaire, mais le document liant les parties devra rester à sa disposition.

EXCEPTIONS

La loi Informatique et Libertés prévoie des exceptions à l'interdiction de transferts de données personnelles hors de l'UE dans deux cas, et uniquement si l'importateur de données est « responsable de traitement » :

→ Soit la personne a consenti expressément au transfert de ses données personnelles

→ Soit le transfert s'avère nécessaire à l'une des conditions suivantes :

- la sauvegarde de la vie de cette personne
- la sauvegarde de l'intérêt public
- le respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice
- la consultation, dans des conditions régulières, d'un registre public qui, en vertu de dispositions législatives ou réglementaires, est destiné à l'information du public et est ouvert à la consultation de celui-ci ou de toute personne justifiant d'un intérêt légitime
- l'exécution d'un contrat entre le responsable du traitement et l'intéressé, ou de mesures précontractuelles prises à la demande de celui-ci
- la conclusion ou l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers

Ce type de transfert doit cependant rester ponctuel. Les transferts massifs et répétés doivent être juridiquement encadrés par des BCR, le Safe Harbor ou des clauses contractuelles types.

FORMALITÉS

Tout fichier de données à caractère personnel doit être déclaré en ligne[4] ou en envoyant un formulaire par courrier à la CNIL. Certains fichiers comme les données relatives aux comités d'entreprise ou la paie sont néanmoins exemptés de déclaration.

DÉCLARATION DU FICHIER

Déclaration simplifiée

Un formulaire simplifié est à disposition des entreprises sur le site de la CNIL pour les déclarations les plus courantes telles que la gestion des fichiers de clients et prospects, le contrôle des accès aux lieux de travail, ou encore la prévention et la gestion des impayés par chèque bancaire.

[3] Téléchargeables à cette adresse : http://bit.ly/Wp6nK1

[4] Accessible à cette adresse : http://www.cnil.fr/vos-responsabilites/declarer-a-la-cnil/

■ Déclarations spécifiques

Une entreprise traitant des données sensibles devra s'orienter vers une procédure spécifique :

- → Demande d'autorisation : si elle traite des informations relatives à l'origine racial ou aux données biométriques, ou que le traitement poursuit des finalités spécifiques susceptibles d'exclure du bénéfice d'un droit, d'une prestation ou d'un contrat
- → Demande d'avis : si les données ont été collectées par le service public ou concerne la sureté, la défense ou la sécurité publique
- → Demande d'autorisation de recherche médicale : Demande d'autorisation d'évaluation des pratiques de soin

■ Déclaration normale

Tout autre cas fait l'objet d'une « déclaration normale ». Le déclarant est invité à renseigner :

- → Son identité et ses coordonnées
- → L'identité et les coordonnées du service chargé du traitement dans le cas où les données sont transférées à un prestataire ou sous-traitant
- → La finalité du traitement
- → La typologie des données (état civil, habitudes de vies, données de connexion, etc.), leur origine et leur durée de conservation
- → Les éventuels échanges de données avec des organismes tiers
- → Les moyens mis en œuvre pour sécuriser les données
- → La manière dont les personnes concernées par les données sont informées de leurs droits
- → Les transferts de données hors de l'UE

FORMALITES SPÉCIFIQUES AUX TRANSFERTS HORS DE L'UE

Les transferts de données hors de l'UE doivent faire l'objet d'une déclaration normale ou d'une déclaration spécifique si les données le justifient.

L'onglet relatif aux transferts devra être renseigné en fonction du cadre juridique choisi (clauses contractuelles types, Safe Harbor, BCR, exceptions) :

6) Si le transfert s'effectue vers un pays n'assurant pas un niveau de protection suffisant, sélectionnez les garanties mises en œuvre pour permettre le transfert (cf. liste à jour de ces pays sur la carte interactive du site internet) :

- ☐ *Contrat de responsable de traitement à responsable de traitement (clauses contractuelles types de la commission européenne)*
- ☐ *Contrat de responsable de traitement à sous-traitant (clauses contractuelles types de la commission européenne)*
- ☐ *Certification « safe harbour » (concerne uniquement les Etats-Unis)*
- ☐ *Règles internes (ou « BCR – Binding Corporate Rules »)*
- ☐ *Un des cas suivants, prévus par l'article 69 de la loi du 6 janvier 1978 modifiée :*
  - ☐ *La sauvegarde de la vie de la personne*
  - ☐ *La sauvegarde de l'intérêt public*
  - ☐ *Le respect d'obligations permettant d'assurer la constatation, l'exercice ou la défense d'un droit en justice*
  - ☐ *La consultation d'un registre public*
  - ☐ *L'exécution d'un contrat entre le responsable du traitement et l'intéressé*
  - ☐ *La conclusion ou l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et un tiers*
  - ☐ *Le consentement de la personne*

L'enregistrement de la déclaration est actif à la réception d'un récépissé de déclaration, indiquant le numéro sous lequel le traitement est enregistré par la CNIL. Ce numéro est nécessaire à toute modification ou suppression de la déclaration.

Les entreprises ayant déclaré un transfert dans le cadre de BCR ou de clauses contractuelles types reçoivent un récépissé pour le traitement principal en France mais doivent attendre une autorisation de transfert délivré par la CNIL pour transmettre leurs données hors de l'UE.

CONCLUSION

La législation actuelle sera susceptible d'évoluer en raison du développement du cloud computing : l'utilisation de serveurs distants éparpillés dans le monde complique en effet les démarches de déclarations de transferts.

Par ailleurs, la législation américaine pose un problème de confidentialité des données depuis le vote du Patriot Act en 2001 : celui-ci autorise les autorités américaines à accéder à toute donnée présente sur le territoire des Etats-Unis.

POUR ALLER PLUS LOIN

Guide édité par la CNIL en novembre 2012 : « Les transferts de données à caractère personnel hors Union Européenne ».

Téléchargeable sur le site de la CNIL : http://bit.ly/d7N-CWA