CLUSIF

INVALIDATION DU PRIVACY SHIELD : QUELLES CONSÉQUENCES ?

SEPTEMBRE 2021

SOMMAIRE

1. Rappel sur l'encadrement des transferts de données en dehors de l'UE

2. Conséquences de l'invalidation du *Privacy Shield* sur les transferts en dehors de l'UE

CLUSIF

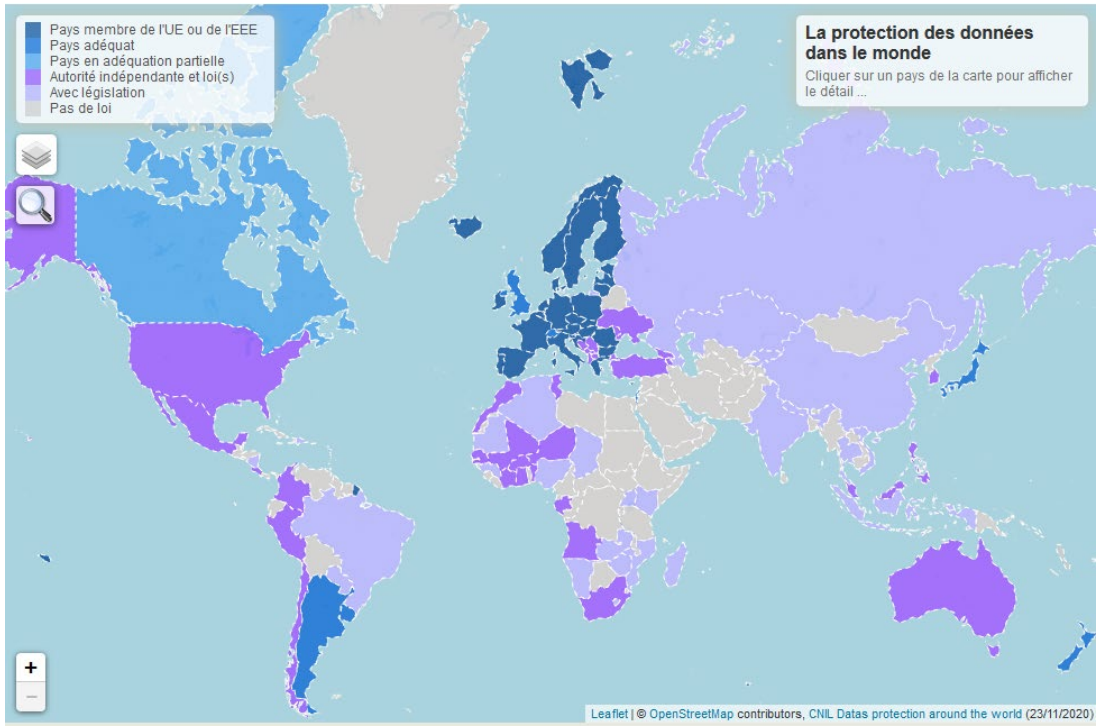
1. RAPPEL SUR L'ENCADREMENT DES TRANSFERTS DE DONNÉES EN DEHORS DE L'UE

Les transferts de données hors Union européenne, c'est-à-dire « *toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'UE* », **ne sont pas interdits.**

Toutefois, ils doivent être **encadrés par un mécanisme** prévu par le Règlement général sur la protection des données (RGPD, art. 44).

Cf. CNIL : Glossaire
Cf. FAQ sur le transfert de données à caractère personnel

CNIL – Carte de la protection des données dans le monde



1. RAPPEL SUR L'ENCADREMENT DES TRANSFERTS DE DONNÉES EN DEHORS DE L'UE

Outils de transferts de données	
Décisions d'adéquation de la Commission européenne (art. 45 du RGPD)	
Garanties appropriées (art. 46 du RGPD)	Instruments juridiquement contraignants ou exécutoires entre autorités/ organismes publics
	Règles d'entreprise contraignantes
	Clauses contractuelles types (CCT) adoptées par la Commission européenne
	Clauses contractuelles adoptées par une autorité de contrôle et approuvées par la Commission européenne
	Code de conduite
	Mécanisme de certification
	Clauses contractuelles ad hoc
	Dispositions intégrées dans les arrangements administratifs entre autorités/ organismes publics
Règles d'entreprises contraignantes (BCR : Binding Corporate Rules) (art. 47 du RGPD)	
Dérogations pour situations particulières (art. 49 du RGPD)	

CLUSIF

1. RAPPEL SUR L'ENCADREMENT DES TRANSFERTS DE DONNÉES EN DEHORS DE L'UE

Focus : Brexit et transferts de données vers le Royaume-U

Le Royaume-Uni a quitté l'Union européenne en vertu d'un accord de retrait du 31 janvier 2020

Une période transitoire, pendant laquelle le droit de l'UE restait applicable dans le Royaume-Uni, s'est achevée 1er janvier 2021

En vertu d'un accord de commerce et de coopération du 24 décembre 2020 **le RGPD est resté applicable de manière transitoire jusqu'à 1er juillet 2021**

Deux décisions d'adéquation ont été adoptées par la Commission européenne le 28 juin 2021

CLUSIF

2. LES CONSÉQUENCES DE L'INVALIDATION DU *PRIVACY SHIELD* PAR LA CJUE

Remise en contexte : l'invalidation du *Safe Harbor (1/2)*

Safe Harbor **= sphère de sécurité** reprenant les principes de protection des données à caractère personnel auxquels les entreprises établies aux Etats-Unis pouvaient adhérer afin de pouvoir traiter des données personnelles provenant d'entreprises et d'administrations situées sur le territoire européen.

- Décision d'adéquation de la Commission européenne du **26 juillet 2000** conformément à la directive 95/46/CE

Arrêt de la Cour de justice de l'Union européenne (CJUE) du 6 octobre 2015, dit « Schrems I » :

Les faits :

- M. Schrems, utilisateur autrichien du réseau social Facebook, a saisi le Commissaire à la protection des données irlandais d'une plainte considérant que la législation outre-Atlantique n'offrait pas une protection suffisante des données personnelles des citoyens européens stockées aux Etats-Unis ;
- Cette plainte avait été rejetée, le Commissaire à la protection des données la considérant comme infondée. Il avait également estimé ne pas avoir à l'instruire compte tenu de la décision 2000/520 du 26 juillet 2000 (décision d'adéquation).

Question préjudicielle (posée par la Haute Cour de justice irlandaise) :

- Une autorité nationale de protection des données personnelles peut-elle enquêter sur une plainte alléguant qu'un pays tiers n'assure pas un niveau de protection adéquat, et, le cas échéant, suspendre le transfert de données contesté, si une décision d'adéquation a été rendue antérieurement par la Commission ?

2. LES CONSÉQUENCES DE L'INVALIDATION DU *PRIVACY SHIELD* PAR LA CJUE

Remise en contexte : l'invalidation du *Safe Harbor (2/2)*

Arrêt de la Cour de justice de l'Union européenne (CJUE) du 6 octobre 2015, dit « Schrems I » :

- La CJUE a **invalidé** la décision par laquelle la Commission européenne avait constaté que les Etats-Unis assurent un niveau de protection suffisant des données.

- La CJUE souligne la **disproportion** du large accès aux données personnelles des citoyens européens dont bénéficient les services de renseignement américains dans la mesure où la surveillance n'est pas ciblée.

- La CJUE reconnait que le niveau de protection assuré par un pays tiers peut évoluer : il incombe à la Commission de **vérifier de manière périodique** si le constat du niveau de protection adéquat est toujours justifié.

Conséquence : le Safe Harbor ne peut plus servir de cadre juridique aux transferts de données aux États-Unis depuis le 6 octobre 2015.

Quelles solutions ?

Recours aux outils alternatifs (clauses contractuelles types, règles d'entreprise contraignantes)…

…avant l'adoption d'un nouveau cadre, le ***Privacy Shield***

CLUSIF

2. LES CONSÉQUENCES DE L'INVALIDATION DU *PRIVACY SHIELD* PAR LA CJUE

***Privacy Shield* du 8 juillet 2016 = décision d'adéquation de la Commission européenne du 8 juillet 2016** permettant le transfert de données entre l'Union européenne et les Etats-Unis.

Arrêt de la Cour de justice de l'Union européenne (CJUE) du 16 juillet 2020, dit « Schrems II »

✓ Questions posées à la CJUE :

- Interprétation et validité du ***Privacy Shield*** (Décision de la Commission européenne du 12 juillet 2016) ;
- Interprétation et validité des **clauses contractuelles types** pour les transferts de données par un responsable du traitement à un sous-traitant (Décision de la Commission européenne du 5 février 2010).

2. LES CONSÉQUENCES DE L'INVALIDATION DU *PRIVACY SHIELD* PAR LA CJUE

Arrêt de la Cour de justice de l'Union européenne (CJUE) du 16 juillet 2020, dit « Schrems II »

✓ **Invalidation du *Privacy Shield***

- La CJUE a estimé que le droit américain n'accorde pas une protection équivalente à celle du droit européen en matière de la protection des données personnelles.

- Pourquoi ? Il existe une surveillance excessive exercée par les services de renseignements américains sur les données des citoyens et résidents européens, insuffisamment encadrée et sans réelle possibilité de recours.

    - Sont visés notamment la collecte et l'accès aux données personnelles à des fins de sécurité nationale en vertu de l'article 702 de la loi américaine FISA et du décret (« Executive Order ») 12 333.

2. LES CONSÉQUENCES DE L'INVALIDATION DU *PRIVACY SHIELD* PAR LA CJUE

Arrêt de la Cour de justice de l'Union européenne (CJUE) du 16 juillet 2020, dit « Schrems II »

✓ **Affirmation de la validité des clauses contractuelles types (sous réserve d'adaptation au cas par cas)**

- Avant tout transfert, le responsable du traitement ou le sous-traitant doit **vérifier au cas par cas** si le droit du pays du destinataire assure une protection appropriée.

- Si besoin, ils doivent mettre en place, en collaboration avec le destinataire de données, des **garanties supplémentaires** à celles offertes par les clauses contractuelles types (CCT).

CLUSIF

2. LES CONSÉQUENCES DE L'INVALIDATION DU *PRIVACY SHIELD* PAR LA CJUE

Quels sont les impacts de l'arrêt Schrems II ?

Transferts vers les Etats-Unis

Impossibilité de fonder les transferts de données sur le *Privacy Shield*

↓

Recours aux autres outils de transferts (CCT, BCR, etc.)

Transferts vers les autres pays tiers

Hypothèse où les transferts vers le pays tiers ne bénéficient pas d'une décision d'adéquation

↓

Recours aux autres outils de transferts (CCT, BCR, etc.)

L'exportateur (*entité qui transfère les données*) et l'importateur (*entité qui reçoit les données de la part de l'exportateur en vue de leur traitement*) des données personnelles doivent **évaluer si la législation concernée respecte le niveau de protection requis par l'UE.**

CLUSIF

2. LES CONSÉQUENCES DE L'INVALIDATION DU *PRIVACY SHIELD* PAR LA CJUE

Comment évaluer la législation du pays tiers ?

Le Comité européen de la protection des données (CEPD) a publié des recommandations sur les **garanties essentielles qui doivent être trouvées dans le cadre juridique d'un pays tiers** dans le cadre de la surveillance mise en œuvre par les autorités publiques de ce pays.

Quelles sont les garanties essentielles européennes ?

- ✓ L'ingérence dans la vie privée doit :
  - ✓ reposer sur des **règles claires, précises et accessibles** ;
  - ✓ être **nécessaire et proportionnée** au regard des objectifs légitimes poursuivies ;
- ✓ Un **mécanisme de contrôle indépendant** doit être mis en place ;
- ✓ Les personnes doivent bénéficier de **voies de recours effectives**.

Source : CEPD, Recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance, 10 novembre 2020

CLUSIF

2. LES CONSÉQUENCES DE L'INVALIDATION DU *PRIVACY SHIELD* PAR LA CJUE

Quelles sont les actions à mettre en œuvre avant de mettre en œuvre un transfert hors UE ?

Dans ses recommandations du 10 novembre 2020, le CEPD préconise la mise en place des étapes suivantes :

1. **Cartographier** les transferts vers des pays hors UE ;
2. **Vérifier les outils de transfert utilisés** pour encadrer ces transferts ;
3. **Evaluer le niveau de protection** offert par le pays vers lequel les données sont transférées (en l'absence d'une décision d'adéquation et hors l'hypothèse d'une dérogation particulière) ;
4. **En l'absence d'un niveau de protection adéquate, identifier les garanties supplémentaires** à intégrer dans les outils de transfert.

Source : CEPD, Recommandations 01/2020 sur les mesures qui complètent les instruments de transfert destinés à garantir le respect du niveau de protection des données à caractère personnel de l'UE, 10 novembre 2020

CLUSIF

2. LES CONSÉQUENCES DE L'INVALIDATION DU *PRIVACY SHIELD* PAR LA CJUE

Bons réflexes pour les transferts aux États-Unis …

L'ensemble des entités états-uniennes ne sont pas soumises aux programmes de surveillance du FISA et de l'EO12333 !

La CNIL distingue deux situations en fonction du destinataire des données :

Le destinataire des données est directement soumis aux programmes de surveillance
(ex.: prestataires de services de cloud, fournisseur d'accès, entreprises de télécommunications)

La mise en place de mesures additionnelles est délicate.

CNIL, Mémoire en observations devant le Conseil d'Etat (Affaire Health Data Hub), 8 octobre 2020

Le destinataire des données n'est pas directement soumis aux programmes de surveillance
(ex.: société produisant des biens industriels, société du secteur médical ou pharmaceutique)

Les données sont généralement dans le champ de ces programmes lors de leur transit vers le destinataire **mais** les mesures additionnelles (dont le chiffrement) peuvent assurer une protection suffisante sous certaines conditions

CLUSIF

2. LES CONSÉQUENCES DE L'INVALIDATION DU *PRIVACY SHIELD* PAR LA CJUE

Que faut-il entendre par « garanties supplémentaires » ?

Dans ses recommandations du 10 novembre 2020, le CEPD donne des précisions sur la notion de garanties supplémentaires :

Garanties techniques

Au cas par cas, en fonction des circonstances de traitements mis en œuvre

Garanties contractuelles

- Obligation de mettre en œuvre des mesures techniques spécifiques,
- Obligation de transparence,
- Obligation de renforcer l'exercice des droits des personnes concernées, etc.

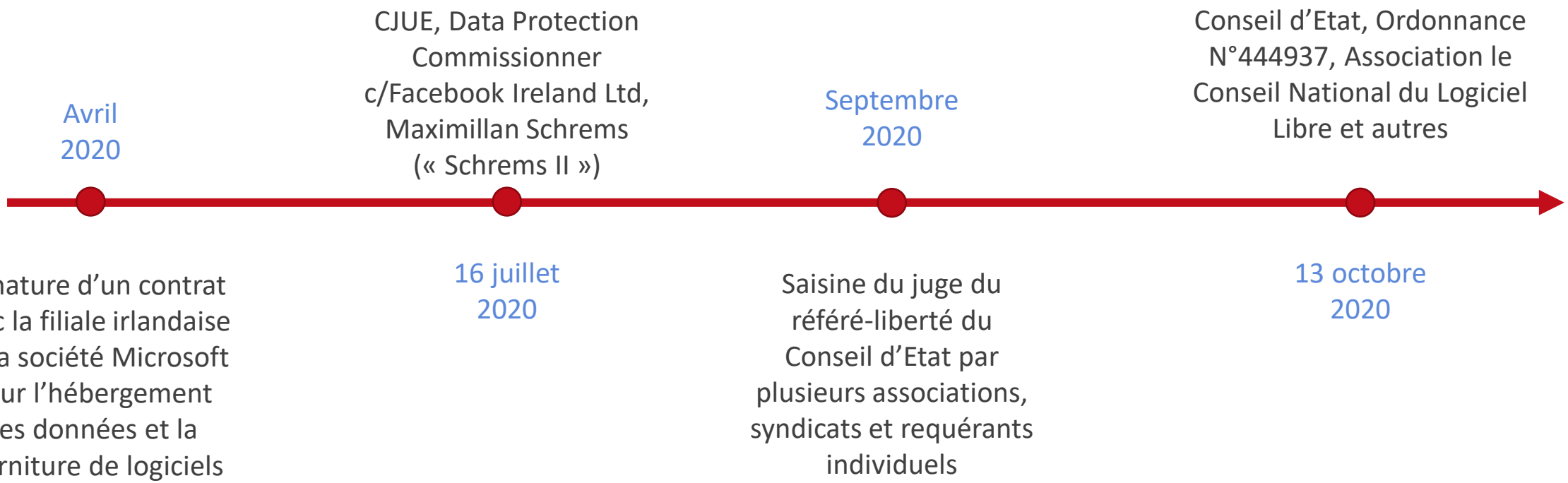
Garanties organisationnelles

- Politiques internes sur les transferts notamment au sein des groupes,
- Publication de rapports de transparence,
- Minimisation de données,
- Audits internes, etc.

CLUSIF

2. LES CONSÉQUENCES DE L'INVALIDATION DU *PRIVACY SHIELD* PAR LA CJUE

Focus : l'affaire Health Data Hub (www.health-data-hub.fr)



2. LES CONSÉQUENCES DE L'INVALIDATION DU *PRIVACY SHIELD* PAR LA CJUE

Focus : l'affaire Health Data Hub

La **Plateforme des données de santé** (PDS) / Health Data Hub (HDH) – une infrastructure mise en œuvre de façon anticipée (en raison de la COVID-19) en avril 2020 afin de **faciliter le partage des données de santé** issues de sources diverses pour les besoins de la recherche.

La PDS a recouru au **service américain de cloud AZURE (Microsoft)**. Compte tenu de la sensibilité et du volume des données, la CNIL a fait part de son souhait que l'hébergement et les services liés à sa gestion puissent être réservés à des entités relevant exclusivement des juridictions de l'UE.

Source : Cnil.fr
Rapport d'activité 2020

2. LES CONSÉQUENCES DE L'INVALIDATION DU *PRIVACY SHIELD* PAR LA CJUE

Focus : l'affaire Health Data Hub

Synthèse de l'ordonnance du Conseil d'Etat :

- ✓ Existence d'un **risque d'accès par les services de renseignements américains** aux données de santé hébergées dans la plateforme Health Data Hub.
- ✓ **Poursuite du fonctionnement de la plateforme** en raison des besoins de l'épidémie de Covid-19 et des moyens techniques de la plateforme pour lesquels il n'existe pas d'alternative satisfaisante.
- ✓ Injonction au Health Data Hub de continuer à travailler avec Microsoft pour **renforcer la protection des droits des personnes concernées** sur leurs données et ce sous le contrôle de la CNIL.

2. LES CONSÉQUENCES DE L'INVALIDATION DU *PRIVACY SHIELD* PAR LA CJUE

Focus : les nouveaux modèles de CCT de la Commission européenne

Rappel

Avant le 4 juin 2021 – deux types de CCT

- ✓ Clauses encadrant les transferts de données personnelles **entre deux responsables de traitement (CCT « responsables de traitement »)**
- ✓ Clauses Contractuelles Types encadrant les transferts de données personnelles **entre un responsable de traitement et un sous-traitant (CCT « sous-traitant »)**

→ **Avant les nouvelles CCT, il n'existait pas de clauses contractuelles types entre sous-traitants !**

Cf. CNIL : « *Transfert de données : les clauses contractuelles types (CCT) de la Commission européenne* », 15 juin 2021

CLUSIF

2. LES CONSÉQUENCES DE L'INVALIDATION DU *PRIVACY SHIELD* PAR LA CJUE

Focus : les nouveaux modèles de CCT de la Commission européenne

Depuis le 4 juin 2021 – quatre modules de clauses contractuelles types :

Les nouvelles CCT combinent des **clauses générales** avec les **clauses spéciales** encadrant chaque type de transfert. Les responsables de traitement et les sous-traitants doivent choisir le module applicable à leur situation.

4 modules prévus :

- ✓ **entre un responsable de traitement UE et un responsable de traitement non UE**
- ✓ **entre un responsable de traitement UE et un sous-traitant non UE**
- ✓ **entre un sous-traitant UE et un sous-traitant non UE**
- ✓ **entre un sous-traitant UE et un responsable de traitement non UE**

Période transitoire de 18 mois :

Les responsables de traitement et les sous-traitants ont 18 mois pour se conformer aux nouvelles clauses → **jusqu'au 27 décembre 2022**.

Les anciennes CCT peuvent être utilisées pendant cette période.

Au-delà de cette période les contrats doivent être mis à jour avec nouvelles CCT.

2. LES CONSÉQUENCES DE L'INVALIDATION DU *PRIVACY SHIELD* PAR LA CJUE

Focus : les nouveaux modèles de CCT de la Commission européenne

✓ **Quels impacts de l'affaire Schrems II ?**

Obligations relatives à l'évaluation du niveau de protection offert par le pays tiers

- Obligation d'évaluer si les CCT permettent de garantir un niveau de protection adéquate en tenant compte de la législation du pays tiers, des circonstances du transfert, des garanties supplémentaires ;
- Obligation de documenter cette évaluation.

Obligations spécifiques pour l'importateur en cas de demande d'autorités publiques du pays tiers d'accéder aux données

- Obligation d'informer l'exportateur d'une telle demande ;
- Obligation d'évaluer la légalité de la demande au regard du droit local et, le cas échéant, de la contester ;
- etc.

CLUSIF

2. LES CONSÉQUENCES DE L'INVALIDATION DU *PRIVACY SHIELD* PAR LA CJUE

Focus : les nouveaux modèles de CCT de la Commission européenne

✓ L'avis conjoint 2/2021 du Comité européen de la protection des données et du Contrôleur européen de la protection des données

✓ Les principaux constats :

- Les nouveaux modèles de CCT reflètent les changements induits par l'entrée en application du RGPD.
- Ils prennent en compte **les recommandations du CEPD** sur les mesures qui complètent les instruments de transfert.
- Si l'utilisation des modèles de CCT permet de renforcer le niveau de protection offerte aux personnes, la mise en place d'autres mesures (notamment techniques et organisationnelles) peut s'avérer nécessaire.

CLUSIF

11 rue de Mogador
75009 Paris
Tél. : +33 1 53 25 08 80
Email : clusif@clusif.fr
Site Web : https://clusif.fr