



Transferts de données

Cédric Burton

Partner

Global Co-Chair, Privacy and Cybersecurity

Agenda

1. La notion de transfert de données
2. Les mécanismes de transfert prévus par le RGPD
3. Les décisions d'adéquation
4. Le Safe Harbour et Schrems I
5. Le Privacy Shield et Schrems II
6. Les révisions du Privacy Shield

La notion de transfert de données

- Principe de libre circulation des données à caractère personnel dans l'Espace économique européen (EEE)
- Absence de définition de « transferts de données » dans le RGPD
- G29 : « un transfert vers un pays tiers consiste en la communication de données à un autre responsable du traitement ou sous-traitant dans un pays tiers »
- Tout transfert de ce type à partir de l'UE nécessite une base juridique
- Les données doivent avoir été collectées et traitées légalement avant le transfert

- Qu'est-ce qu'un transfert?



- Quelle est la règle de base?

**Libre circulation
des données au
sein de l'EEE.**

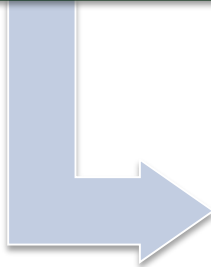
**Interdiction des
transferts en
dehors de l'EEE.**

Les mécanismes de transfert prévus par le RGPD

1. Décision d'adéquation adoptée par la Commission

- Privacy Shield.
- Pays tiers.
- Territoire.
- Secteur déterminé du pays tiers.
- Organisation internationale.

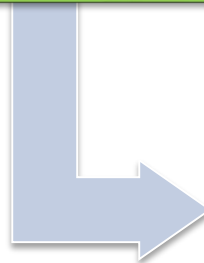
En l'absence d'une décision d'adéquation...



2. Garanties appropriées

- BCRs.
- Clauses contractuelles types (CCT).
- Codes de conduite approuvés et mécanismes de certification assortis d'engagements contraignants.
- Clauses contractuelles "ad hoc" autorisées par les autorités de contrôle.

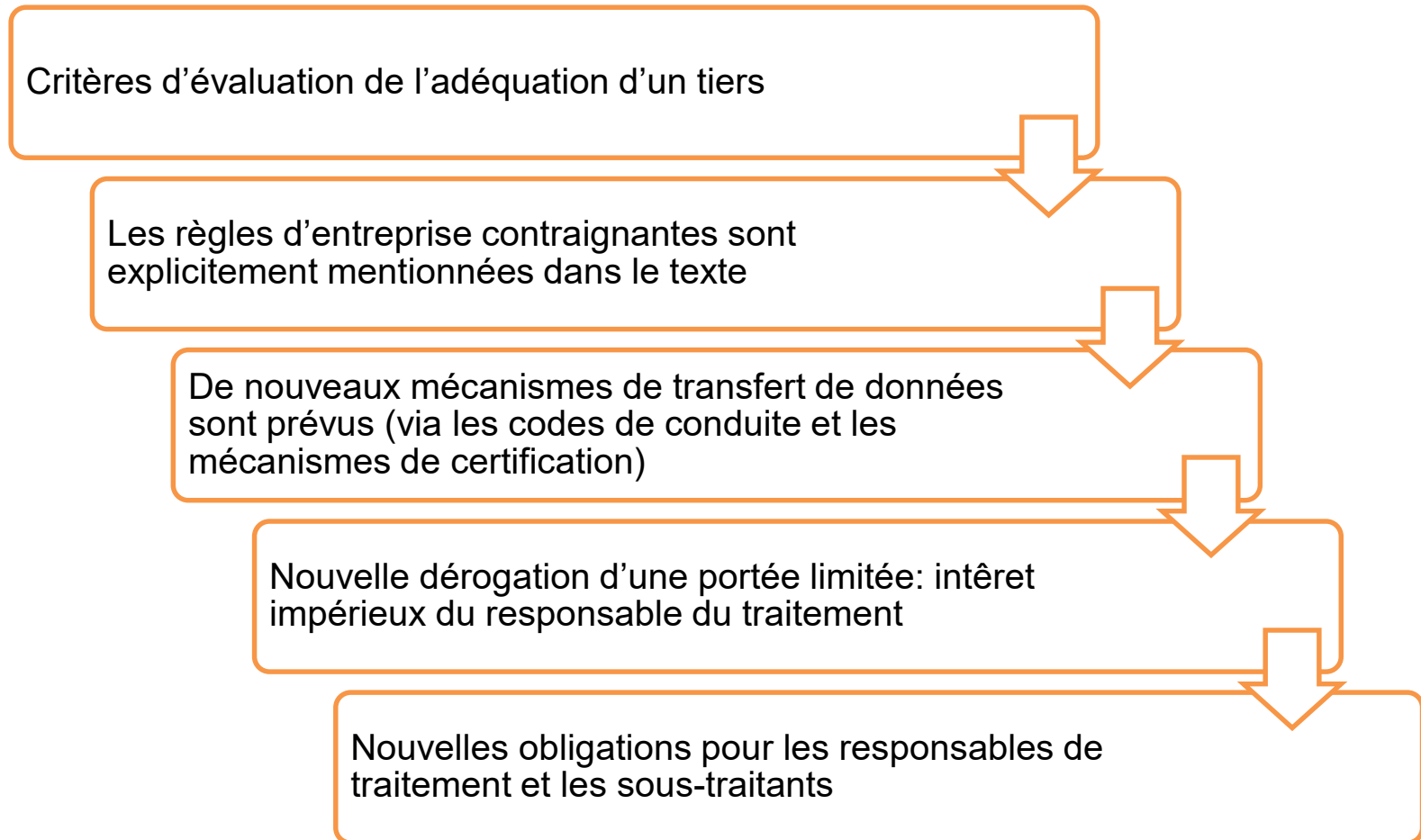
En l'absence d'une décision d'adéquation ou de garanties appropriées...



3. Dérogations

- Consentement.
- Intérêts légitimes impérieux du RT.
- Motifs importants d'intérêt public.

Les mécanismes de transfert prévus par le RGPD - Quelles nouveautés?



Les mécanismes de transfert prévus par le RGPD

	Scope	Legal certainty	Burden	
BCRs	<ul style="list-style-type: none"> Intra-group transfers Flexible Regulator approved 	High (GDPR Art. 47)	<ul style="list-style-type: none"> High upfront Low ongoing 	<hr/> <p style="text-align: center;">Data Protection Directive</p> <p style="text-align: center;">(Arts. 25, 26)</p>
Codes of Conduct/Seals	<ul style="list-style-type: none"> Sector/company specific New; mechanisms must be developed Seals valid for up to 3 years; option to renew 	Likely High (GDPR Arts. 40-43)	<ul style="list-style-type: none"> High upfront Low ongoing 	<ul style="list-style-type: none"> Transfers permissible only if third country ensures adequate level of protection <i>or</i> derogation applies Controllers responsible for compliance
Commission Adequacy	<ul style="list-style-type: none"> Limited to countries recognized as providing adequate protection 	High	<ul style="list-style-type: none"> Low 	
Derogations (e.g., explicit consent, contractual performance)	<ul style="list-style-type: none"> Limited in scope Narrowly interpreted 	Low to Medium	<ul style="list-style-type: none"> Medium Documentation required 	<hr/> <p style="text-align: center;">General Data Protection Regulation (GDPR)</p> <p style="text-align: center;">(Arts. 44-50)</p>
SCCs	<ul style="list-style-type: none"> Limited to contracting parties 	Invalidation Risk	<ul style="list-style-type: none"> Low Intensive maintenance 	<ul style="list-style-type: none"> Similar but more detailed transfer regime Controllers <i>and</i> processors responsible for compliance
Privacy Shield	<ul style="list-style-type: none"> Limited to certain business EU to U.S. transfers 	Invalidation Risk	<ul style="list-style-type: none"> High upfront Low ongoing 	



Décisions d'adéquation

Décisions d'adéquation de la Commission européenne

La Commission européenne peut décider qu'un pays tiers assure un niveau de protection adéquat (également possible pour un territoire, un secteur ou une organisation internationale)

Adéquation = niveau de protection "essentiellement équivalent"
(y compris les exigences issues de l'arrêt Schrems I)

Obligation de la Commission européenne de contrôler le fonctionnement des décisions d'adéquation

- Examen périodique au moins tous les quatre ans
- Si nécessaire elle peut abroger, modifier ou suspendre les décisions d'adéquation

Possibilité de limiter les transferts de données sensibles vers des pays tiers ou des organisations internationales "pour des raisons importantes d'intérêt public" :

- En l'absence d'une décision d'adéquation
- Les lois nationales mettant en œuvre cette restriction doivent être notifiées à la Commission européenne



Décisions d'adéquation de la Commission européenne

Andorre

Argentine

Canada (pour les organisations sous PIPEDA)

Îles Féroé

Guernesey

Israël

Île de Man

Japon

Jersey

Nouvelle-Zélande

Suisse

Uruguay

EU-US Privacy Shield

W&GR Qu'est ce que le Safe Harbor / Privacy Shield?



Privacy Shield
Framework

- Section 5 du FTC Act
- « *Say what you do, do what you say* »
- 7 Principes et 16 FAQs:
 - Information
 - Choix
 - Responsabilité pour transfert ultérieur
 - Sécurité
 - Intégrité des données et limitation de l'usage auquel elles sont destinées
 - Accès aux données
 - Recours, exécution et responsabilité

Safe Harbor

- Juin 2013: Révélations d'Edward Snowden.
- Juin 2013: Plainte de Max Schrems auprès de l'APD irlandaise.
- Novembre 2013:
 - 13 recommandations de la Commission européenne pour améliorer le Safe Harbor.
 - Début des négociations entre l'UE et les États-Unis.
- Septembre 2015: Opinion de l'Avocat Général.
- Octobre 2015: CJUE invalide la décision de la Commission européenne reconnaissant le Safe Harbor (*Schrems*, C-362/14).
 1. Une décision d'adéquation de la Commission européenne ne fait pas obstacle à ce qu'un DPA examine, à la demande d'une personne, si le transfert des données de cette personne vers un pays tiers respecte les exigences légales.
 2. Le Safe Harbor n'est plus une base légale valide.
 - ▶ Le Safe Harbor n'offre pas un niveau de protection équivalent.
 - ▶ Manque de protection juridictionnelle effective pour les Européens.
 - ▶ Peu de contrôle et de supervision.
 - ▶ Une exception de sécurité nationale disproportionnée.

Conséquences de l'arrêt *Schrems I*

- Les DPA peuvent enquêter et, le cas échéant, ordonner l'arrêt de transferts hors UE même s'il existe une décision d'adéquation de la Commission européenne (risque de fragmentation).
- Plus de 4000 sociétés sont sans base légale pour les transferts de données vers les Etats-Unis.
- Réactions des APD:
 - Échéance du 31 janvier 2016.
- Pression des APD pour la mise en œuvre d'une alternative au Safe Harbor.
- Incertitude juridique:
 - Quid des transferts vers d'autres pays que les États-Unis?
 - Quid de la validité des autres mécanismes de transfert (BCRs, SCC)?

Nouvel accord : *EU-U.S. Privacy Shield*

- 2 février 2016: Accord politique sur un « *EU-U.S. Privacy Shield* »:
 - Obligations strictes pour les entreprises qui traitent des données personnelles européennes, et un contrôle rigoureux du respect de ces obligations.
 - L'accès aux données par les autorités américaines est étroitement encadré et transparent.
 - Une protection effective des droits des citoyens de l'UE et plusieurs voies de recours (création d'un Ombudsman).
- Pas de texte; le G29 exige de recevoir le texte pour fin février.
- Mars 2016: analyse des garanties du nouvel accord par le G29.
- Opinion du G29 en avril 2016.
- 12 juillet 2016: Privacy Shield est adopté
- Exécutoire à compter du 1^{er} août 2016

EU – U.S. Privacy Shield

- Décision d'adéquation la plus importante
- Disponible pour les entreprises américaines depuis le 1er août 2016
- Mécanisme d'autocertification volontaire appuyé par les pouvoirs d'application de la FTC et du DoT des États-Unis
- Construit sur le squelette du Safe Harbor (Principes et FAQs) mais :
 - Nouveaux mécanismes de recours
 - Mécanisme pour les transferts ultérieurs renforcé
 - Renforcement des activités de supervision et d'application de la loi par la FTC et le DoC
- En septembre 2019, 5.001 entreprises sont enregistrées sur la liste Privacy Shield
- Contesté devant la CJUE
 - Une affaire a été jugée irrecevable, mais une autre est en cours
 - L'audience a eu lieu le 9 juillet 2019 devant la CJUE

Traitement des plaintes dans le cadre du Privacy Shield

- Système complexe de traitement des plaintes composé différents niveaux:
 1. Les particuliers sont encouragés à se plaindre d'abord directement auprès des entreprises, ou directement auprès des autorités de protection des données de l'UE, qui coopéreront avec le DoC et la FTC (les opinions des autorités de protection des données de l'UE sont contraignants dans le contexte des ressources humaines).
 2. Les particuliers ont accès à un organe de recours indépendant choisi par l'entreprise.
 3. Engagements appuyés par le DoC et la FTC
 - ▶ DoC : Examens d'office, personne de contact pour les APD de l'UE et processus de renvoi des plaintes par les APD de l'UE
 - ▶ FTC : Engagements d'accorder la priorité aux renvois de cas de non-conformité (de la part des organismes de règlement des différends, des organismes d'autoréglementation, du DoC, des APD de l'UE)
 4. Dans certaines situations et pour les réclamations résiduelles, demandez réparation auprès du Privacy Shield Panel:
 - ▶ Arbitrage exécutoire
 - ▶ Uniquement pour déterminer si la société certifiée Privacy Shield a violé ses obligations et si une telle violation n'a pas été corrigée en tout ou en partie
 - ▶ Possibilité d'imposer "une équité individuelle, non monétaire, fondée sur l'équité" (Ex: détection de données)
 - ▶ Possibilité de demander un contrôle judiciaire et l'exécution des décisions en vertu du Federal Arbitration Act des États-Unis
 5. En cas de non-conformité persistante : l'entreprise perdra les avantages du Privacy Shield, et sera retirée de la liste Privacy Shield
- Possibilité de recours dans le domaine du renseignement national pour les Européens par le biais d'un Ombudsman

Les affaires Schrems I & II

2013: Schrems → APD irlandaise
→ Haute Cour irlandaise

2014: Haute Cour irlandaise → CJUE:
La décision Safe Harbor empêche-t-elle
les APD de traiter la plainte d'une
personne au sujet de transferts de
données réalisés en vertu de cette
décision ?

2015: CJUE déclare Safe Harbor
invalide

2017: Le Privacy Shield remplace Safe
Harbor

**Quadrature du Net → CJUE
sur le Privacy Shield
Audience le 9 octobre**

2015: CJUE → Haute Cour irlandaise
→ APD irlandaise enquête sur la
plainte de Schrems

La plainte est reformulée pour tenir
compte de l'utilisation par Facebook
des clauses contractuelles types

2018: Haute Court irlandaise → pose
11 questions à la CJUE, notamment
sur les clauses contractuelles types
et le Privacy Shield

2018: Facebook fait appel de la décision de
renvoi. La Cour suprême irlandaise rejette
le pourvoi: les questions sont pendantes
devant la CJUE.

**Les audiences ont eu lieu le 9 juillet ;
Avis de l'AG prévu pour le 12 décembre**

Les révisions du Privacy Shield

Révision de 2017

- Les entreprises ne doivent **pas** faire référence publiquement à la certification Privacy Shield **avant** de l'avoir complètement obtenu
- Le ministère du Commerce (DoC) effectuera des recherches régulières pour déceler les fausses allégations et surveillera en permanence la conformité
- Le DoC et les APD **sensibilisent le public**
- Améliorer la **coopération** entre les autorités de contrôle (DoC et APD - DoC et FTC)
- Nommer un **Ombudsman**
- Des rapports complets doivent être présentés en temps opportun à la Commission par les autorités américaines

Révision de 2018

- Renforcement des procédures de certification - progrès constatés (Ex: contrôles aléatoires)

Toutefois, des préoccupations subsistent sur :

- L'efficacité des mécanismes et outils mis en place par le DoC
- Nomination d'un **Ombudsman** pour la protection de la vie privée et l'efficacité du traitement et du règlement des plaintes
- Élaboration de directives par la FTC et le DoC

Révision de 2019 (en cours)

- Des hauts fonctionnaires se sont réunis les 12 et 13 septembre à Washington D.C. La Commission a annoncé qu'un rapport relatif à la révision sera publié



Merci pour votre attention! Questions?

Consultez notre blog pour rester à jour sur toutes les actualités relatives à la protection des données

THE WSGR DATA ADVISOR
Unique Insights on Privacy and Data Protection Worldwide
<https://www.wsgrdataadvisor.com/>
Enter your email address to subscribe to regular updates.

WSGR Wilson Sonsini Goodrich & Rosati
PROFESSIONAL CORPORATION

The banner features a decorative top border with green and blue circular patterns. The text is centered on a light beige background.

Cédric Burton
Partner
Co-Chair Privacy and Cybersecurity
cburton@wsgr.com