

Communication présentée en séance plénière le 28 septembre 2023

**COMMUNICATION SUR LES REGLES APPLICABLES AU
REGARD DES TRANSFERTS DE DONNEES HORS UNION
EUROPEENNE**

Rapporteur : **M. François PELLEGRINI**

Avec le concours de :

A large rectangular area of the page is redacted with black ink, obscuring a list of names that would normally be attributed to the rapporteur as co-authors or contributors.

1 **Table des matières**

2	1. Rappel des principes généraux en matière de transferts de données hors de l'Union	2
3	européenne.....	
4	2. Les décisions d'adéquation	6
5	A. Focus sur l'adéquation des États-Unis.....	6
6	a) Rappel du contexte	6
7	b) Éléments clés du nouveau cadre.....	7
8	c) Conséquences pour les organismes souhaitant transférer des données vers les	
9	États-Unis	8
10	B. Application de l'article 48 du RGPD à des fournisseurs soumis à des lois extra-	
11	européennes autorisant les demandes d'accès par des autorités publiques de pays tiers... 9	
12	3. Les garanties appropriées.....	13
13	A. Présentation des garanties	13
14	B. Analyse d'impact sur les transferts	15
15	4. Les dérogations	16
16	5. Possibilités liées à l'article 9.4 du RGPD	17
17		
18		

19 1. Rappel des principes généraux en matière de transferts de données hors 20 de l'Union européenne

21 Le chapitre V du RGPD (articles 44 à 49) fixe les règles en matière de transfert de données
22 hors de l'Union européenne, de sorte que le niveau de protection des personnes physiques
23 garanti par le RGPD ne soit pas compromis lorsque des données à caractère personnel sont
24 transférées vers un pays tiers ou une organisation internationale. Les responsables de
25 traitement et les sous-traitants peuvent transférer des données hors de l'Union européenne
26 et de l'espace économique européen à condition d'assurer un niveau de protection des
27 données suffisant et approprié c'est-à-dire en transférant vers un pays considéré comme
28 assurant un niveau de protection adéquat (section 2.) ou si des garanties appropriées sont
29 mises en place (section 3.). À défaut, il existe également des dérogations permettant
30 d'effectuer des transferts dans certains cas particuliers (section 4.).
31

32 L'article 4 du RGPD ne contient pas de définition de **la notion de transfert**. Le CEPD a
33 adopté le 14 février 2023 des lignes directrices sur l'articulation entre le champ d'application
34 territorial du RGPD (article 3) et les dispositions relatives aux transferts énoncées au
35 chapitre V¹. Ces lignes directrices visent à aider les organismes à déterminer si une opération
36 de traitement constitue un transfert et à fournir une interprétation commune de cette notion.
37 Les trois **critères cumulatifs pour considérer qu'un traitement constitue un**
38 **transfert** sont :

- 39 1. le responsable de traitement ou le sous-traitant exportateur de données est soumis au
40 RGPD pour le traitement donné ;
41 2. l'exportateur transmet ou met les données à caractère personnel à la disposition de
42 l'importateur de données (une autre responsable du traitement, responsable conjoint
43 ou sous-traitant) et
44 3. l'importateur est dans un pays tiers ou est une organisation internationale, qu'il soit
45 soumis ou non au RGPD.

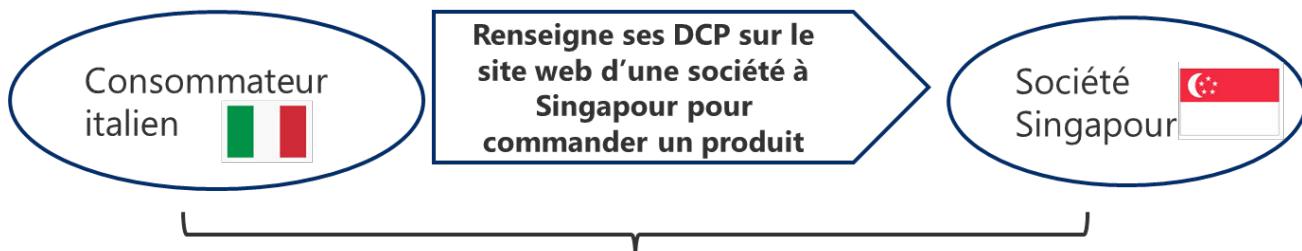
46 À titre d'exemple, la transmission de données par un organisme responsable de traitement
47 soumis au RGPD vers un sous-traitant fournisseur de services de *cloud* à des fins
48 d'hébergement sur des serveurs dans un pays tiers constitue un transfert de données hors
49 Union européenne. Si l'hébergement est réalisé sur des serveurs situés en Europe, il peut tout
50 de même y avoir des transferts vers des serveurs hors UE gérés par des entités situées dans
51 des pays tiers à des fins de réPLICATION ou de sauvegarde ou vers des équipes localisées dans
52 des pays tiers à des fins de support ou de maintenance.

53 En revanche, le recours par un responsable de traitement soumis au RGPD à un fournisseur
54 de services de *cloud* soumis à une législation d'un pays tiers qui héberge les données sur le
55 territoire de l'Union européenne ne constitue pas en tant que tel un transfert et le chapitre V
56 du RGPD n'est pas applicable. Toutefois, si le fournisseur communique des données à
57 caractère personnel en réponse à une demande d'accès des autorités du pays tiers en vertu de
58 la législation à laquelle il est soumis, une telle divulgation constitue un transfert en vertu du
59 chapitre V du RGPD.

60 ¹ https://edpb.europa.eu/system/files/2023-02/edpb_guidelines_05-2021_interplay_between_the_application_of_art3-chapter_v_of_the_gdpr_v2_en_o.pdf

64 Un autre cas ne constituant pas un transfert est celui d'un salarié qui, à l'occasion d'un
 65 déplacement professionnel temporaire hors de l'Union européenne, accède à distance à ses
 66 documents professionnels stockés dans le *cloud*. Le CEPD a considéré qu'il ne s'agissait pas
 67 ici d'un transfert dans la mesure où le salarié n'est pas une entité distincte de son employeur
 68 responsable de traitement.
 69

70 Les schémas ci-dessous présentent différentes situations permettant d'illustrer des situations
 71 de transfert ou d'absence de transfert.
 72

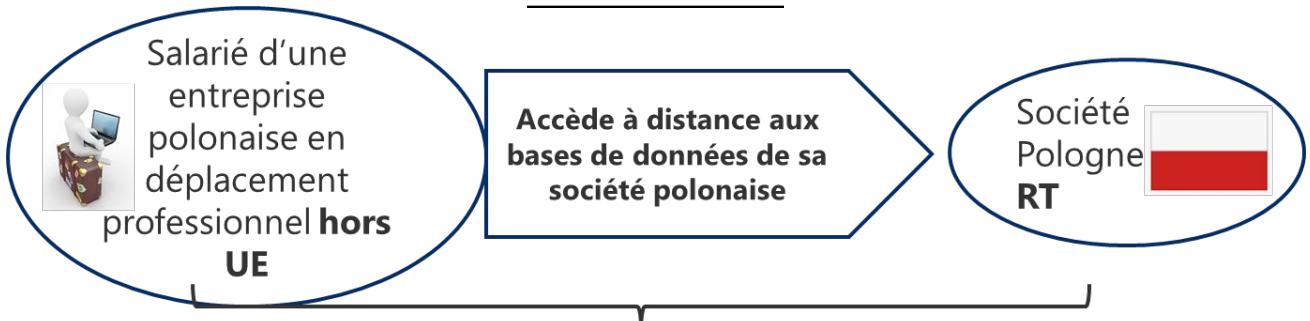


Ce n'est pas un transfert
 Pas de RT/ST exportateur (données divulguées directement et de sa propre initiative par la personne concernée).
 Attention, la société singapourienne peut être soumise au RGDP en vertu de l'art 3.2



C'est un transfert

73
 74



Ce n'est pas un transfert

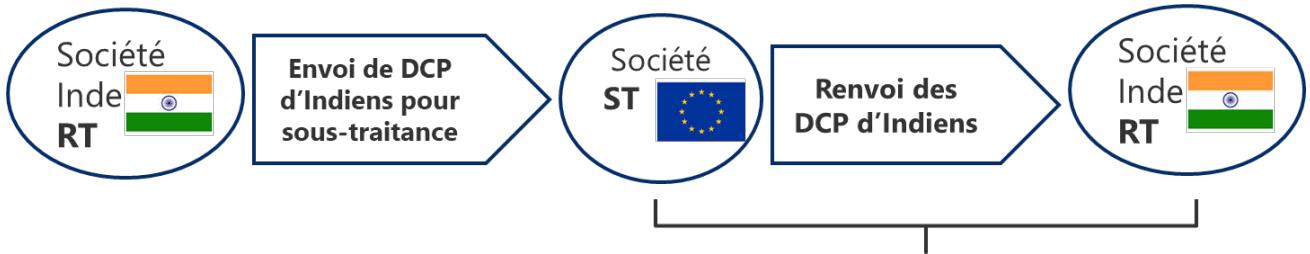
Le salarié n'est pas un RT/ST distinct, il « fait partie » de sa société RT

76
77



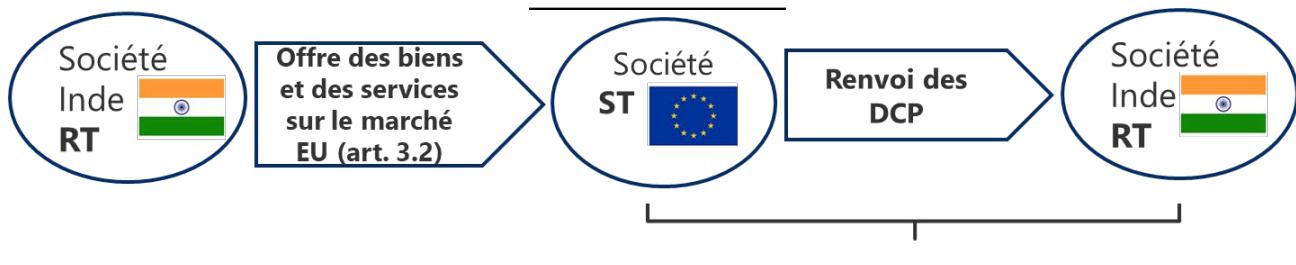
C'est un transfert

78
79



C'est un transfert

80
81



C'est un transfert

Les deux entités sont toutes deux soumises au RGPD, la société indienne en vertu de l'art. 3.2 et la société EU en vertu de l'art 3.1

84

2. Les décisions d'adéquation

85

86 Une décision d'adéquation est une décision adoptée par la Commission européenne fondée
87 sur l'article 45 du RGPD, qui établit qu'un pays tiers ou une organisation internationale
88 assure un niveau de protection adéquat des données à caractère personnel.

89

90 Le RGPD prévoit une liste non exhaustive d'éléments qui, cumulés, permettent à la
91 Commission d'évaluer le caractère adéquat du niveau de protection des données du pays tiers.
92 Ces éléments incluent notamment la législation interne du pays, l'existence d'une ou de
93 plusieurs autorités de contrôle indépendantes en matière de protection des données et les
94 engagements internationaux pris par le pays.

95

96 Une décision d'adéquation a pour effet de permettre le transfert, sans exigence
97 supplémentaire, de données à caractère personnel par des organismes soumis au RGPD vers
98 le pays tiers concerné. **À ce jour, 15 pays bénéficient d'une décision d'adéquation²** :
99 Andorre, Argentine, Canada (volet commercial)³, Îles Féroé, Guernesey, Israël, Île de Man,
100 Jersey, Nouvelle-Zélande, Suisse et Uruguay et, depuis l'entrée en application du RGPD,
101 Japon, République de Corée, Royaume-Uni et États-Unis (organismes auto-certifiés).

102

103 La Commission est actuellement en phase de **revue des 11 décisions d'adéquation**
104 **adoptées avant l'entrée en application du RGPD**. Cette revue prendra la forme d'un
105 rapport adressé au Parlement et au Conseil qui contiendra une synthèse des modifications
106 internes (réformes législatives, jurisprudence) depuis l'adoption de la décision d'adéquation.
107 Pour la première fois, les règles en matière d'accès aux données par les gouvernements seront
108 évaluées. Pour chaque pays, le rapport présentera et évaluera les modifications puis conclura
109 sur l'adéquation. Si la conclusion est positive, l'adéquation restera en place. Si elle est
110 négative, une procédure sera alors initiée pour modifier ou retirer la décision. Pour certains
111 pays (par exemple Israël), la Commission a indiqué que des préoccupations ont été identifiées
112 mais des solutions portant sur des garanties additionnelles ont été négociées.

113

A. Focus sur l'adéquation des États-Unis

114

a) Rappel du contexte

115

116 Le 16 juillet 2020, la CJUE dans son arrêt « Schrems II » a invalidé la précédente décision
117 d'adéquation de la Commission européenne à l'égard des États-Unis (le « Privacy Shield »).

118

119 La CJUE a analysé la législation étasunienne alors en vigueur en matière d'accès aux données
120 des fournisseurs de services web et entreprises de télécommunications par les services de
121 renseignement étasuniens (Section 702 FISA et Executive Order n°12333). Elle en a conclu
122 que les atteintes portées à la vie privée des personnes dont les données étaient traitées par les
123 entreprises et opérateurs étasuniens soumis à cette législation étaient disproportionnées au

² https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#adequacy-decisions-latest

³ Décision d'adéquation applicable uniquement aux traitements couverts par la loi PIPEDA (« Personal Information Protection and Electronic Documents ») régissant le traitement des informations personnelles par les organisations sur secteur privé à des fins commerciales.

124 regard des exigences de la Charte des Droits Fondamentaux européenne. En particulier, la
125 Cour a jugé que la collecte des données par les services de renseignement n'est pas
126 proportionnée et que les voies de recours, y compris juridictionnelles, dont disposent les
127 personnes à l'égard du traitement de leurs données étaient insuffisantes. La CJUE a dès lors
128 invalidé cette décision d'adéquation de la Commission européenne.
129

130 En réaction à cette invalidation, le président des États-Unis, Joe Biden, a adopté
131 le 7 octobre 2022, un décret présidentiel (Executive Order n°14086) pour renforcer les
132 garanties concernant la collecte et l'utilisation des données à caractère personnel par les
133 services de renseignement étasuniens.
134

135 Sur cette base, le Département du Commerce étasunien a adopté un nouveau cadre
136 transatlantique pour la protection des données à caractère personnel (le « EU-U.S. Data
137 Privacy Framework »).
138

139 Ce nouveau cadre transatlantique a été soumis à la Commission européenne afin qu'elle
140 évalue s'il permet d'assurer un niveau de protection adéquat des données des Européens.
141 Avant d'adopter définitivement sa décision reconnaissant le caractère adéquat de ce nouveau
142 dispositif, la Commission a soumis le 13 décembre 2022 un projet de décision pour avis au
143 CEPD.
144

145 Le 28 février 2023, le CEPD a adopté et publié son avis sur ce projet d'adéquation. Le CEPD
146 y relève les améliorations apportées par le gouvernement des États-Unis, tout en faisant part
147 de ses préoccupations sur un certain nombre de points dont il dresse la liste.
148

b) Éléments clés du nouveau cadre

149 Le cadre de protection des données UE-États-Unis est composé d'un nouvel ensemble de
150 règles et de garanties contraignantes pour limiter l'accès aux données à caractère personnel
151 par les autorités de renseignement étasuniennes à ce qui est nécessaire et proportionné pour
152 protéger la sécurité nationale.
153

154 Le système d'auto-certification des entités important des données

155 Comme dans le précédent cadre de protection des données UE-États-Unis (le « Privacy
156 Shield »), **157 un système d'auto-certification des entités étasuniennes** est mis en place.
158 Une fois inscrites sur la liste des organismes certifiés, ces dernières s'engagent annuellement
159 et publiquement à adhérer à ce cadre légal et à en respecter l'ensemble des principes. Des
160 garanties similaires à celles de l'UE sont prévues, telle que la limitation de la finalité, c'est-à-
161 dire l'obligation de supprimer les données qui ne seraient plus nécessaires à la finalité de
162 collecte. En cas de partage des données européennes à un tiers, la continuité de leur
163 protection devra également être assurée.
164

165 **166 Seuls les transferts vers les entités étasuniennes certifiées ne nécessitent pas
167 l'utilisation d'outils d'encadrement des transferts prévus par l'article 46 du
168 RGPD.** Pour les transferts de données vers d'autres entités que celles certifiées, des garanties
169 appropriées doivent être fournies et ces transferts ne sont possibles qu'à condition de garantir
170 des droits opposables aux personnes concernées ainsi que des voies de recours effectives.
171

171

172 **Le décret présidentiel n°14086**

173

174 **Un des éléments clés de ce cadre** est le décret présidentiel étasunien n°14086 qui a pour
175 objet de renforcer la protection des données à caractère personnel traitées par les services de
176 renseignement étasuniens, en :

177

- 178 • consacrant les principes de nécessité et de proportionnalité dans le cadre de l'accès des
179 autorités étasuniennes aux données ; et
- 180 • introduisant un nouveau mécanisme de recours indépendant et impartial auprès d'une
Cour de contrôle de la protection des données.

181

182 **c) Conséquences pour les organismes souhaitant transférer des données vers les États-Unis**

183

184 La Commission européenne ayant constaté que les États-Unis assurent un niveau de
185 protection substantiellement équivalent à celui de l'UE, les organismes soumis au RGPD
186 (qu'ils soient responsables de traitement ou sous-traitants) peuvent désormais transférer des
187 données à caractère personnel vers les organismes certifiés qui se sont engagés, annuellement
188 et publiquement, à adhérer à ce cadre légal. Ils n'ont pas l'obligation de mettre en place un
189 outil de transfert au titre de l'article 46 du RGPD ou de se prévaloir d'une dérogation au titre
190 de l'article 49 du RGPD.

191

192 Avant de procéder au transfert, les organismes doivent s'assurer que l'organisme destinataire
193 figure sur une liste mise à disposition sur le site du Département du Commerce des États-
194 Unis⁴.

195

196 Les organismes certifiés sur la base du Privacy Shield et qui avaient maintenu cette
197 certification même après l'invalidation de la décision d'adéquation ont été automatiquement
198 inscrits sur la nouvelle liste. Ils ont trois mois pour mettre à jour leur Politique de
199 Confidentialité (jusqu'au 10 octobre 2023)⁵. Néanmoins, les transferts vers ces organismes
200 peuvent bénéficier immédiatement de la décision d'adéquation, dans la mesure où les
201 principes de protection des données à caractère personnel sont restés les mêmes que
202 précédemment, combinés au cadre de protection renforcé offert par le décret présidentiel.

203

204 Les responsables du traitement et les sous-traitants réalisant des transferts vers des
205 organismes auto-certifiés au titre de la décision d'adéquation doivent par ailleurs se
206 conformer à d'autres obligations découlant du RGPD, notamment en ce qui concerne la
207 nécessité de mettre à jour leurs registres de traitement et l'information des personnes
208 concernées des transferts vers les États-Unis.

209

210 Les transferts vers des entités étasunies ne figurant pas sur la liste du Département du
211 Commerce ne peuvent pas être fondés sur la décision d'adéquation et nécessitent des
212 garanties appropriées prévues par l'article 46 du RGPD. Il est cependant important de
213 souligner que les garanties mises en place par le gouvernement étasunien via le décret
214 présidentiel dans le domaine de la sécurité nationale (y compris le mécanisme de recours)
215 s'appliquent à tous les transferts de données effectués par des entités publiques ou privées

⁴ <https://www.dataprivacyframework.gov/s/participant-search>

⁵ Annex I, Section III (Supplemental Principles), 6.e de la décision d'adéquation de la Commission européenne.

216 soumises au RGPD vers des entreprises situées aux États-Unis. Elles sont donc applicables
217 quel que soit l'outil de transfert utilisé (clauses contractuelles types ou règles d'entreprise
218 contraignantes, notamment).

219 **B. Application de l'article 48 du RGPD à des fournisseurs soumis à des lois**
220 **extra-européennes autorisant les demandes d'accès par des autorités**
221 **publiques de pays tiers**

222 Des lignes directrices sur l'article 48 sont actuellement en cours d'élaboration par le CEPD
223 [REDACTED]

225 [REDACTED] dont l'objectif est de clarifier son champ d'application dans le cadre de demandes
226 d'accès adressées à des destinataires dans l'UE à des fins répressives et de sécurité nationale.
227 [REDACTED]

228 Même en l'absence de transfert de données à caractère personnel hors UE, une société
229 soumise à la législation d'un pays tiers peut faire l'objet d'injonctions des autorités publiques
230 de ce pays l'obligeant à leur transférer des données stockées et traitées sur le territoire de
231 l'Union européenne.

232 Cette situation a été spécifiquement couverte par l'article 48 du RGPD qui prévoit que :
233 « *Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant*
234 *d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des*
235 *données à caractère personnel **ne peut être reconnue ou rendue exécutoire de***
236 ***quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord***
237 ***international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers***
238 ***demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert en***
239 ***vertu du présent chapitre*** ». Une demande d'un juge ou d'une autorité administrative d'un
240 pays tiers ne peut donc être exécutoire que s'il existe un cadre juridique spécifique en place
241 convenu entre les deux pays (comme un traité d'entraide judiciaire).

242 De telle demandes de transmission d'information peuvent ainsi être fondées sur :

- 243 - des traités d'entraide judiciaire, une juridiction étrangère demandant communication
244 d'information ou de document et pouvant être revêtue d'un exequatur en Europe ;
245 - des traités de coopération pénale ; on peut également signaler le deuxième protocole
246 additionnel à la convention du Conseil de l'Europe sur la cybercriminalité (Convention
247 de Budapest⁷) mais qui n'est pas encore applicable car en cours de ratification ;
248 - des traités de coopération fiscale qui prévoient la communication de renseignements
249 d'une administration fiscale à une autre : si la décision est « reconnue » par
250

6 [REDACTED]
7 Ce protocole a pour objectif d'améliorer l'accès transfrontière aux preuves électroniques à utiliser dans le cadre des procédures pénales. Il contribuera à la lutte contre la cybercriminalité et d'autres formes de criminalité au niveau mondial en facilitant la coopération entre les États membres et les pays tiers, tout en assurant un niveau élevé de protection des personnes et en veillant au respect des normes de l'UE en matière de protection des données. Le protocole prévoit des procédures visant à améliorer la coopération internationale entre autorités ainsi qu'à renforcer la coopération directe avec les fournisseurs de services et les entités situés dans d'autres pays. Il définit également des procédures relatives à la demande d'entraide judiciaire urgente.

254 l'administration européenne, dans le cadre du traité, elle communique les données
255 demandées.

256
257 De tels traités doivent d'ailleurs eux-mêmes être conformes aux exigences du RGPD et de la
258 jurisprudence de la CJUE.

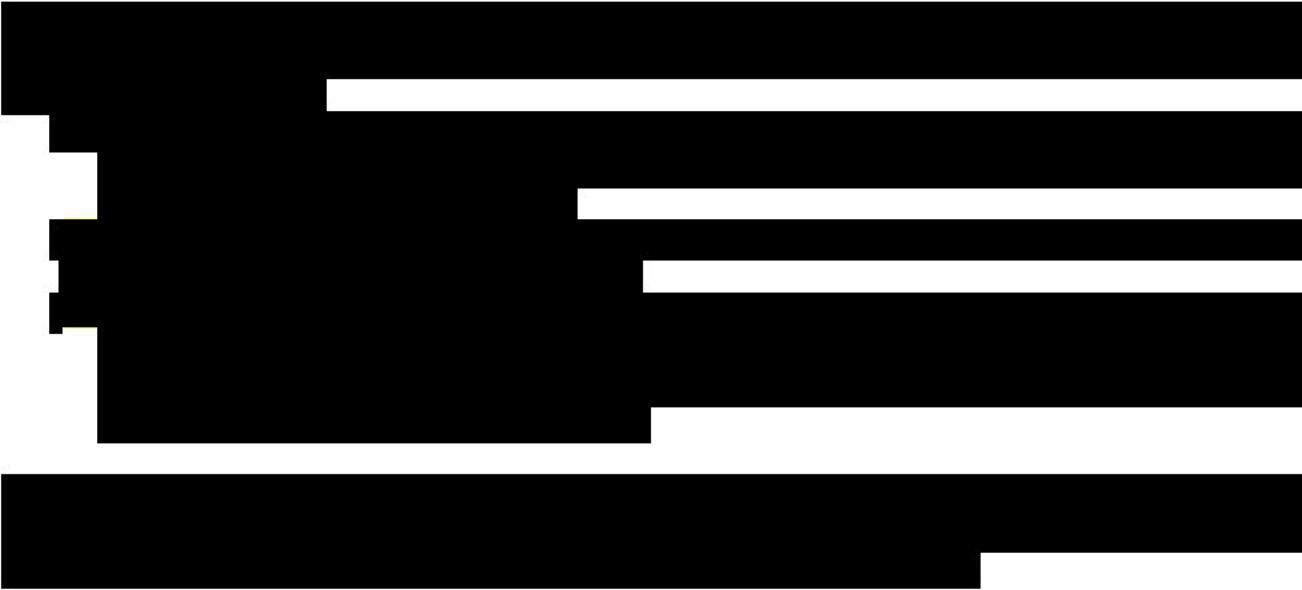
259
260 En revanche, en dehors d'actions de coopération entre États (telles que visées ci-dessus), il
261 n'existe évidemment pas de traités prévoyant que des services de renseignement d'États
262 étrangers puissent demander aux sociétés relevant de leurs lois nationales ayant des
263 établissements en Europe de leur communiquer des données personnelles d'Européens
264 (d'ailleurs généralement sans en informer les autorités européennes). Et il n'en existera
265 probablement jamais.

266
267 Ce risque de divulgation non autorisé par le droit de l'Union a d'ailleurs été confirmé par le
268 Conseil d'État dans son ordonnance du 13 octobre 2020 concernant le dossier HDH précisant
269 qu'«*(...) il résulte de l'instruction que les mesures techniques mises en œuvre par Microsoft*
270 *ou susceptibles de l'être à brève échéance n'écartent pas toute possibilité pour cette*
271 *entreprise d'accéder aux données traitées sous la responsabilité de la Plateforme des*
272 *données de santé, en dépit des précautions, limitant ce risque, qui entourent le chiffrement*
273 *dont elles font l'objet et le stockage des clés de chiffrement utilisées. Il ne peut ainsi être*
274 *totalellement exclu, sur le plan technique, que Microsoft soit amenée à faire droit*
275 *à une demande des autorités américaines fondée sur l'article 702 du FISA, ce*
276 *qui méconnaîtrait alors les articles 28 et 48 du règlement général sur la*
277 *protection des données (...)*».

278
279 La question se pose de savoir quelles sont les conséquences de la récente
280 adéquation des Etats-Unis sur l'application de cet article 48. Plus précisément,
281 les nouvelles garanties apportées par le droit étasunien permettent-elles de
282 conclure à la conformité des réponses aux demandes d'accès des autorités
283 étasuniennes aux données situées dans l'UE sur le fondement de l'article 48 ? Si
284 tel n'est pas le cas, comment appliquer l'article 48 sans toutefois empêcher tout
285 recours à des opérateurs non soumis à une législation d'un pays tiers ?

286

302



303

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

346

[REDACTED]

[REDACTED]

368

386

387

388

389 **3. Les garanties appropriées**

390 **A. Présentation des garanties**

391 L'article 46 prévoit différents outils pour encadrer les transferts de données vers des entités
392 situées dans des pays non adéquats.

393 **• Clauses contractuelles types (CCT) de la Commission européenne**

394 Les clauses contractuelles types sont des modèles de clauses encadrant le transfert de
395 données à caractère personnel et adoptés par la Commission européenne. Leur conclusion ne
396 nécessite pas d'autorisation d'une autorité de contrôle.

397 Les modèles de clauses contractuelles ont été mis à jour par la Commission européenne le
398 4 juin 2021. Elles combinent des clauses générales avec une approche « par modules » pour
399 répondre à divers scénarios de transfert.

- 400 - module 1 : transfert de responsable de traitement à responsable de traitement ;
401 - module 2 : transfert de responsable de traitement à sous-traitant ;
402 - module 3 : transfert de sous-traitant à sous-traitant ;
403 - module 4 : transfert de sous-traitant à responsable de traitement

404 Les clauses contractuelles types intègrent la jurisprudence « Schrems II » de la CJUE en
405 imposant à l'exportateur de tenir compte de la législation applicable à l'importateur pour
406 déterminer si les clauses contractuelles types pourront produire tous leurs effets.

407 Il convient de noter qu'elles ne peuvent pas être utilisées si l'importateur dans le pays tiers
408 est soumis au RGPD en vertu de l'article 3.2 du RGPD. La Commission a annoncé travailler à
409 l'élaboration de clauses « allégées » pour couvrir cette situation afin de tenir compte des
410 exigences qui s'appliquent déjà directement à ces organismes soumis au RGPD.

411 **• Règles internes d'entreprises (BCR)**

412 Il existe des BCR « responsable du traitement » et « sous-traitant ». Le nouveau référentiel
413 BCR « responsable du traitement » mis à jour a été approuvé par le CEPD le 20 juin 2023.
414 Les travaux de mise à jour du référentiel BCR « sous-traitant » ont démarré au sein du CEPD.
415 *Pour plus d'informations, il est renvoyé au le point d'actualité relatif aux dossiers BCR*
416 *présenté en séance plénière le 12 janvier 2023*

- 417 **• Clauses contractuelles types adoptées par une autorité de contrôle et**
418 **approuvées par la Commission européenne (pas de clauses adoptées à ce jour)**
- 419 **• Code de conduite** approuvé comportant l'engagement contraignant et exécutoire
420 pris par les destinataires hors UE (importateurs) d'appliquer les garanties appropriées

421 Le 22 février 2022, le CEPD a adopté des lignes directrices sur les codes de conduite en tant
422 qu'outils de transfert¹¹. Le principal objectif des lignes directrices est de clarifier l'application
423 de l'article 40, paragraphe 3, et de l'article 46, paragraphe 2, point e), du RGPD. Ces
424 dispositions prévoient qu'une fois approuvé par une autorité de contrôle compétente et après

11 <https://edpb.europa.eu/system/files/2022>

[10/edpb_guidelines_codes_conduct_transfers_after_public_consultation_fr.pdf](https://edpb.europa.eu/system/files/2022/10/edpb_guidelines_codes_conduct_transfers_after_public_consultation_fr.pdf)

433 s'être vu accorder une validité générale au sein de l'EEE par la Commission, un code de
434 conduite peut être adopté et utilisé par les responsables du traitement et les sous-traitants
435 qui ne sont pas soumis au RGPD afin de fournir des garanties appropriées pour les transferts
436 de données en dehors de l'UE.

437
438 À ce jour, aucun code de conduite en tant qu'outil de transfert n'a été approuvé¹².

439 Il convient de noter qu'un code de conduite en tant qu'outil de transfert est différent d'un
440 code de conduite « RGPD » au sens de l'article 40.2 du RGPD dont l'objectif est de démontrer
441 la conformité de ses adhérents au RGPD¹³. Même si le code de conduite « RGPD » contient
442 des éléments sur la conformité des transferts de données effectués par ses adhérents en tant
443 qu'exportateurs, il ne constitue pas pour autant un outil de transfert.

- 444
- 445 • **Mécanisme de certification approuvé** comportant l'engagement contraignant et
446 exécutoire pris par les importateurs hors UE d'appliquer les garanties appropriées

447 Le 14 février 2023, le CEPD a adopté des lignes directrices sur la certification en tant qu'outil
448 de transfert¹⁴. L'article 46, paragraphe 2, point f), du RGPD introduit des mécanismes de
449 certification approuvés en tant que nouvel outil permettant de transférer des données à
450 caractère personnel vers des pays tiers en l'absence d'accord d'adéquation. L'objectif
451 principal de ces lignes directrices est de fournir des précisions sur l'utilisation pratique de cet
452 outil de transfert.

453 À ce jour, aucune certification n'a été approuvée en tant qu'outil de transfert. Toutefois, un
454 organisme a soumis un projet à l'autorité luxembourgeoise.

455 De la même manière que pour les codes de conduite, les certifications outil de transfert sont
456 à distinguer des certifications « RGPD » au sens de l'article 42.1 du RGPD dont l'objectif est
457 de démontrer la conformité des organismes certifiés au RGPD, y compris pour les transferts
458 pour lesquels ils sont exportateurs¹⁵. En revanche, et conformément à l'article 42.2 du RGPD,
459 les certifications outil de transfert sont destinées aux **organismes qui ne sont pas soumis**
460 **au RGPD** et donc aux importateurs de données hors UE qui peuvent ainsi être certifiées
461 pour les données qu'ils reçoivent dans le cadre de transferts de leurs clients soumis au RGPD.

¹² À ce jour, un organisme a contacté la CNIL pour un projet de code de conduite comme outil de transfert mais les échanges sont à ce stade préliminaire et aucun projet n'a été adressé formellement à la CNIL.

¹³ En 2021, la CNIL a approuvé son premier code de conduite, le code européen porté par CISPE (Cloud Infrastructure Service Providers Europe) à destination des fournisseurs de services d'infrastructures informatiques en nuage (« *cloud* ») situés sur le territoire de l'Union européenne, de façon quasi simultanée avec l'approbation par l'autorité belge du Code européen « EU CLOUD CoC ». Au niveau européen, quatre codes nationaux et deux codes européens ont été approuvés à ce jour depuis l'entrée en vigueur du RGPD. Actuellement, les services de la CNIL accompagnent les porteurs de trois projets de codes de conduite européens et quatre projets nationaux dans différents secteurs d'activités.

¹⁴ https://edpb.europa.eu/system/files/2023-05/edpb_guidelines_07-2022_on_certification_as_a_tool_for_transfers_v2_fr_o.pdf

¹⁵ A ce jour, trois certifications « RGPD » ont été approuvées dont une seule s'applique en France car européenne (EuroPrivacy). Ces certifications sont toutes « généralistes », c'est-à-dire non spécifiques au secteur du *cloud* mais rien n'empêche un fournisseur de services de *cloud* d'y candidater. Huit projets de certifications sont en cours d'examen.

- 467 • **Arrangement administratif** entre les autorités ou les organismes publics qui
468 prévoit des droits opposables et effectifs pour les personnes concernées

469
470 Le 21 mars 2019, la CNIL a autorisé la mise en œuvre d'un arrangement administratif visant
471 à encadrer les transferts des données à caractère personnel entre l'autorité des marchés
472 financiers (AMF) et ses homologues en dehors de l'EEE.

473
474 Le 18 mars 2021, la CNIL a autorisé la mise en œuvre d'un arrangement administratif visant
475 à encadrer les transferts des données à caractère personnel entre le Haut Conseil du
476 Commissariat aux comptes (H3C) et son homologue étaisunien, le *Public Company
477 Accounting Oversight Board* (PCAOB).

478

491 **B. Analyse d'impact sur les transferts**

492

493 Dans son arrêt dit « Schrems II », la CJUE a souligné la responsabilité des exportateurs et
494 importateurs de garantir que le traitement des données à caractère personnel se fait, et
495 continue à se faire, dans le respect du niveau de protection fixé par la législation européenne.
496 Selon la Cour, les exportateurs ont également la responsabilité de suspendre le transfert,
497 et/ou de résilier le contrat si l'importateur n'est pas, ou n'est plus en mesure de respecter ses
498 engagements en matière de protection des données à caractère personnel. Ainsi, les
499 exportateurs s'appuyant sur les instruments de l'article 46 du RGPD pour leurs transferts de
500 données à caractère personnel ont l'obligation d'évaluer le niveau de protection dans les pays
501 tiers de destination. Une telle évaluation est communément appelée « *Transfer Impact
502 Assessment* » ou « *TIA* » (« analyse d'impact des transferts » en français).

503 *Pour plus d'éléments sur ce sujet, votre rapporteur renvoie au guide d'analyse d'impact sur
504 les transferts présenté en séance plénière le 14 septembre 2023.*

509 **4. Les dérogations**

510
511 Lorsqu'un pays tiers n'est pas reconnu comme offrant un niveau de protection adéquat et en
512 l'absence de garanties appropriées encadrant ce transfert, le transfert peut néanmoins, par
513 exception, être opéré dans les conditions prévues par l'article 49.1 du RGPD. Cet article
514 prévoit notamment le cas dans lequel la personne concernée a donné son consentement
515 explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait
516 comporter pour elle ou lorsque le transfert est nécessaire à la conclusion ou à l'exécution d'un
517 contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et
518 une autre personne physique ou morale. Ces dérogations sont soumises à des conditions
519 particulières, d'interprétation stricte, détaillées à l'article 49 du RGPD.

520
521 Le RGPD prévoit enfin, lorsqu'aucune de ces dérogations n'est applicable, la possibilité de
522 procéder au transfert s'il ne revêt pas de caractère répétitif, ne touche qu'un nombre limité
523 de personnes concernées, est nécessaire aux fins des intérêts légitimes impérieux poursuivis
524 par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et
525 libertés de la personne concernée, et si le responsable du traitement a évalué toutes les
526 circonstances entourant le transfert de données et a offert, sur la base de cette évaluation, des
527 garanties appropriées en ce qui concerne la protection des données à caractère personnel.
528 Le 25 mai 2018, le CEPD a adopté des lignes directrices sur l'interprétation de l'article 49 du
529 RGPD qui établissent sa doctrine sur ces dérogations réservées à des situations
530 particulières¹⁶.

531

536

537

¹⁶ https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_fr.pdf

538

5. Possibilités liées à l'article 9.4 du RGPD

539

Cet article permet aux États membres de maintenir ou d'introduire des conditions supplémentaires, y compris des limitations, en ce qui concerne le traitement des données génétiques, des données biométriques ou des données concernant la santé.

540

541

542

546

547