n°30 Octobre 2021
#30 October 2021

Lexing Insights

Le réseau Lexing® vous informe – The Lexing® network informs you

LES TRANSFERTS INTERNATIONAUX DE DONNEES
INTERNATIONAL DATA TRANSFERS

QUELS OUTILS POUR ENCADRER LES TRANSFERTS INTERNATIONAUX DE DONNEES ?

- L'Internet et la numérisation ont facilité la circulation des données dans le monde et aujourd'hui les échanges commerciaux reposent de plus en plus sur des flux de données personnelles. La confidentialité et la sécurité de ces données sont devenues des facteurs centraux de la confiance.
- Dans l'Union européenne, le RGPD autorise le transfert des données vers un État tiers à condition d'assurer un niveau adéquat de protection des données grâce à différents instruments (décisions d'adéquation, clauses contractuelles types, BCR, dérogations etc.). En Chine, la loi sur la protection des informations personnelles (PIPL), qui entre en vigueur le 1 novembre 2021, pose, elle aussi, des règles strictes pour les transferts de données en dehors du territoire national.
- Quels instruments de transfert sont possibles en vertu du RGPD ? Comment effectuer des transferts vers les USA depuis l'invalidité du Privacy Shield par l'arrêt Schrems II de la CJUE ? Qu'en est-il des transferts vers le Royaume-Uni depuis le Brexit ? Quelles sont les sanctions en cas de transferts illégaux ? Quelles sont les règles en dehors de l'UE, comme en Chine, au Canada ou en Afrique du Sud ?

Les membres du réseau Lexing® dressent un tableau de la situation actuelle à travers le monde. Les pays suivants ont contribué à ce numéro : Afrique du Sud, Belgique, Canada, Chine, Espagne, France, Luxembourg.

WHAT ARE THE RULES ON INTERNATIONAL DATA TRANSFERS?

- *The Internet and digitization have made it easier to transfer data around the world and today commercial exchanges rely increasingly on personal data flows. The privacy and security of such data have become central factors of trust.*
- *In the European Union, the GDPR authorizes transfers of data to third countries provided that they ensure an adequate level of data protection using various tools (such as adequacy decisions, standard contractual clauses, BCRs, derogations). In China, the Personal Information Protection Law (PIPL), which will take effect on 1st November 2021, also sets strict rules for data transfers outside the country.*
- *What transfer tools are available under the GDPR? How to transfer data to the USA after the Privacy Shield was declared invalid by the CJEU's Schrems II ruling? How to transfer data to the UK after the Brexit? What are the penalties for unlawful transfers? What are the rules outside the EU, such as in China, Canada, or South Africa?*

The Lexing® network members provide a snapshot of the current state of play worldwide. The following countries have contributed to this issue: Belgium, Canada, China, France, Luxembourg, South Africa, Spain.

Lexing®

Lexing® est le premier réseau international d'avocats en droit du numérique et des technologies avancées. Créé sur une initiative d'Alain Bensoussan, Lexing® permet aux entreprises internationales de bénéficier de l'assistance d'avocats alliant la connaissance des technologies, des métiers et du droit qui leur sont applicables dans leurs pays respectifs.

Lexing® is the first international lawyers' network for digital and emerging law. Created on an initiative of Alain Bensoussan, Lexing® allows multinationals to benefit from the assistance of seasoned lawyers worldwide who each combines unique expertise in technology and industry with a thorough knowledge of law in their respective country.

https://lexing.network

CELINE AVIGNON
Directeur du département Publicité et Marketing Electronique du cabinet Lexing Alain Bensoussan-Avocats

Head of the Advertising & E-Marketing department of Lexing Alain Bensoussan-Avocats

Les transferts transfrontaliers depuis et vers l'Afrique du Sud

▪ La plupart des pays imposent dans leurs lois sur la protection des données des conditions pour le transfert de données personnelles depuis leur territoire vers un autre pays. En effet, si les Etats sont souverains sur leur territoire et dictent les lois qui s'appliquent à l'intérieur de leurs frontières pour protéger les données personnelles de leurs citoyens, ils souhaitent également s'assurer que ces données soient protégées conformément à leurs propres normes de protection lorsqu'elles sont transférées en dehors de leur territoire.

▪ Tel est le cas de l'Afrique du Sud, où de la loi sur la protection des informations personnelles (POPIA) fixe des conditions pour le transfert des données personnelles hors des frontières nationales. Ainsi, selon l'article 72 de la POPIA, un responsable du traitement ne peut transférer des données personnelles à un tiers qui se trouve dans un pays étranger que si : (1)

(1) Protection of Personal Information Act 4 of 2013, Section 72(1)(a) - (e)

- ce tiers est soumis à une loi, à des règles d'entreprise contraignantes ou à un accord contraignant qui assurent un niveau de protection adéquat ;
- la personne concernée consent au transfert ;
- le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement, ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée ;
- 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 un tiers ; ou
- le transfert est réalisé dans l'intérêt de la personne concernée et il n'est pas raisonnablement possible d'obtenir son consentement au transfert, ou si cela était possible, elle y consentirait probablement.

▪ En revanche, peu de lois nationales sur la protection des données fournissent des indications en cas de transfert de données personnelles dans le sens inverse, c'est-à-dire depuis un pays tiers vers leur pays. De fait, la loi POPIA ne précise pas les conditions à respecter pour transférer des données personnelles sur le territoire de l'Afrique du Sud. Le présent article examine les facteurs à prendre en compte, d'un point de vue sud-africain, pour transférer des données personnelles vers un autre pays en toute légalité.

1- Loi sur la protection des données en vigueur

▪ Le premier facteur à prendre en compte est de savoir si le pays vers lequel vous vous souhaitez transférer des données :

- dispose d'une loi sur la protection des données, et
- prévoit les modalités d'application de cette loi.

▪ **Loi sur la protection des données.** Les pays qui n'ont pas de loi sur la protection des données, ou dont les projets de lois sont en cours, sont naturellement problématiques pour le transfert de données. Par exemple, l'Afrique du Sud est bien dotée d'une loi, la POPIA, mais celle-ci n'est entrée pleinement en vigueur que le 1er juillet 2021, et avant cette date les transferts de données personnelles

vers ce pays pouvaient donc être source d'inquiétudes pour les organisations. Une fois la loi identifiée, il faut ensuite examiner dans quelle mesure son champ d'application affecte le transfert envisagé.

▪ **Champ d'application de la loi sur la protection des données.** La POPIA ayant été promulguée en 2013, c'est-à-dire avant l'entrée en vigueur du RGPD **(2)** en 2016, ses modalités d'application diffèrent de celles du RGPD ainsi que de la plupart des lois sur la protection des données adoptées postérieurement au RGPD et modelées sur celui-ci. Notamment, le RGPD a une application extraterritoriale : il s'applique indépendamment du fait que le traitement de données ait lieu ou non dans l'Espace économique européen (EEE). Concrètement, cela signifie que le RPGD est susceptible de s'appliquer aux organisations sud-africaines dès lors qu'elles offrent des produits ou des services aux personnes concernées dans l'UE ou suivent le comportement de ces personnes **(3)**. L'application du RGPD est axée sur la localisation de la personne concernée, ce qui veut dire, par exemple, que si vous transférez les données personnelles d'un citoyen de l'UE en Afrique du Sud, le RGPD s'appliquera. En revanche, la POPIA **(4)** se focalise, quant à elle, sur la localisation du traitement **(5)**. Or, puisque selon la POPIA, transférer des données personnelles, c'est traiter des données personnelles **(6)**, il est fort probable qu'en transférant les données personnelles de l'UE vers l'Afrique du Sud, le transfert sera soumis non seulement au RGPD, mais également à la POPIA.

(2) Règlement (EU) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (« RGDP »)

(3) Article 3.2 du RGPD.

(4) Section 3 de la POPIA.

(5) Accessible à l'adresse : https://www.michalsons.com/blog/must-i-comply-with-the-popi-act/41827

(6) Définition de « traitement » établie à la section 1 de la POPIA

2- Respect des principes relatifs à la protection des données

▪ Le deuxième facteur à prendre en compte est d'identifier si les lois du pays vers lequel vous transférez vos données édictent des principes relatifs à la protection des données. Nombre de lois sur la protection des données font référence au même ensemble de principes, à savoir **(7)** :

- Licéité, loyauté et transparence ;
- Limitation des finalités ;
- Minimisation des données,
- Exactitude ;
- Limitation de la conservation ; et
- Intégrité et confidentialité (sécurité).

(7) Article 5 du RGPD.

▪ La loi POPIA intègre également ce types principes, qu'elles désignent comme des « conditions » de licéité d'un traitement **(8)**. Ces conditions sont en grande partie similaires aux principes de la protection des données visés ci-dessus. Elles constituent les bases fondamentales d'un traitement licite en Afrique du Sud.

(8) Chapitre 3, section 4 de la POPIA.

3- Un niveau de protection adéquat

▪ Le niveau de protection offert aux données transférées est le troisième facteur à prendre en compte. Il est, en droit sud-africain, étroitement lié au deuxième facteur. Les notions de niveau de caractère adéquat ou d'adéquation sont parfois être vagues et peuvent être mal interprétés. À l'heure actuelle, ni le Régulateur de l'information **(9)** ni les tribunaux sud-africains ne se sont prononcés sur ce que constitue un « niveau de protection adéquat ». La POPIA précise toutefois qu'une loi, des règles d'entreprise contraignantes (BCR) ou un accord contraignant offrent une protection adéquate **(10)** dès lors qu'ils :

(9) Information Regulator of South Africa. Site web accessible à l'adresse : https://www.justice.gov.za/inforeg/

(10) Section 72(1)(a)(i) et (ii).

- établissent effectivement des principes de traitement raisonnables substantiellement similaires aux conditions établies pour un traitement licite des informations personnelles de la personne concernée ; (11) et
- incluent des dispositions, relatives au transfert ultérieur d'informations personnelles depuis le destinataire vers des tiers dans un autre pays, substantiellement similaires aux dispositions relatives aux transferts transfrontaliers prévues par la POPIA.

(11) Dans la POPIA, « personne concernée » peut designer une personne physique ou une personne morale

▪ Ces dispositions de la POPIA sont très proches de celles du RGPD, dont le principe général applicable aux transferts en dehors de l'UE est que le niveau de protection des personnes physiques garanti par le RGPD ne doit pas être compromis par le transfert (12). Prises ensemble, les exigences du RGPD et de la POPIA en termes d'adéquation signifient qu'une loi, des règles d'entreprise contraignantes ou un accord contraignant doivent :

(12) Article 44 du RGPD

- respecter ou être substantiellement similaires aux principes ou conditions de traitement licite prévus par le RGPD ou la POPIA, (13) et
- contenir des dispositions relatives aux transferts transfrontaliers qui sont substantiellement similaires à celles prévues par le RGPD ou la POPIA.

(13) Article 5 du RGPD

▪ Même si l'approche du RGPD est plus complexe, il existe donc de nombreuses similitudes entre les dispositions de la POPIA et du RGPD en matière de transferts transfrontaliers. Il pourrait être possible de considérer que loi POPIA respecte les grands principes posés par le RPGD et offre une protection adéquate des données personnelles en vertu du texte européen. À l'heure actuelle, l'Afrique du Sud n'a toutefois pas obtenu de décision d'adéquation de la part de la Commission européenne et il n'est pas certain que le Régulateur de l'information dépose une demande en vue d'en bénéficier, mais une telle décision d'adéquation serait la bienvenue.

4- Mesures de protection

▪ Enfin, le quatrième et dernier facteur à prendre en considération comprend les mesures que vous pouvez mettre en place afin de respecter les principes de protection des données et de protéger les données personnelles des personnes concernées de manière équivalente à la protection offerte par la loi du pays d'origine. Différents types de mesures peuvent être adoptées.

▪ Mesures techniques. Les mesures techniques visent à contrôler et protéger les ressources technologiques d'une organisation, telles que ses systèmes, ses dispositifs, ses réseaux et son matériel. Le chiffrement, les pare-feu et la protection par mot de passe sont des exemples typiques de mesures techniques. Les organisations qui transfèrent des données personnelles en Afrique du Sud voudront ainsi s'assurer que les destinataires disposent de mesures techniques appropriées pour protéger les données contre les accès non autorisés et tous autres incidents.

▪ Mesures organisationnelles. Les mesures organisationnelles sont des mesures destinées à protéger les données personnelles lors des opérations courantes d'une organisation. Ces mesures sont essentielles pour garantir l'existence d'une norme de protection des données à caractère personnel au sein une organisation.

Constituent de telles mesures, par exemple : les actions de sensibilisation menées auprès des employés, l'adoption de politiques et procédures internes propres à faire respecter les mesures de protection, l'établissement et la mise en œuvre de normes pour la protection des données, ou la réalisation d'évaluations et d'audits de conformité.

▪ **Mesures contractuelles.** Des mesures contractuelles sont mises en place pour lier juridiquement les parties à des normes spécifiques de protection des données et s'assurer de leur conformité. Ainsi, en Afrique du Sud, la POPIA impose au responsable du traitement la conclusion d'un contrat écrit avec son sous-traitant afin de s'assurer que ce dernier établisse et maintienne les mesures de sécurité requises par la POPIA **(14)**.

(14) Section 21(1) de la POPIA.

▪ Dans la pratique, les organisations s'acquittent de cette obligation en intégrant des dispositions relatives à la protection des données dans les accords existants avec leurs sous-traitants, ou en concluant des avenants à ces accords à cet effet, ou bien encore en signant des accords de traitement des données distincts. Les responsables du traitement peuvent également signer des contrats entre eux. Par conséquent, les organisations qui souhaitent transférer des données personnelles en Afrique du Sud peuvent demander à leurs partenaires sud-africains de conclure des accords de traitement de données ou d'inclure des clauses de protection des données dans leurs accords avec les entités sud-africaines qui seront destinataires des données. De cette façon, ils s'assurent que les données personnelles qu'ils transfèrent en Afrique du Sud seront protégées à un niveau équivalent à celui de la législation de leur pays d'origine et selon une norme conforme à leurs principes de la protection des données.

Conclusion

▪ Il est conseillé de bien prendre en compte les facteurs décrits ci-dessus lors du transfert de données personnelles vers un autre pays en général, et vers l'Afrique du Sud en particulier. Ces facteurs doivent être évalués au cas par cas. Dans l'idéal, tous ces facteurs devraient être remplis avant de transférer des données personnelles vers un autre pays. Toutefois, si après avoir effectué cette évaluation, vous constatez que le pays vers lequel vous souhaitez transférer vos données à caractère personnel ne répond pas à ces exigences, et si vous désirez toujours procéder au transfert malgré tout, vous devrez alors mettre en œuvre des mesures supplémentaires afin de remédier à ces lacunes.

LISA EMMA – IWUOHA

south-africa@
lexing.network

Crossborder transfers in and out of South Africa

▪ *Most data protection laws impose requirements for transferring personal data out of the country and to another country. Since nations are sovereign and can dictate the laws that apply within their borders, and to their citizen's data, they want to ensure that their country's personal data is protected according to their standards regardless of where the data goes.*

▪ *South Africa is no different in this regard. Section 72 of the Protection of Personal Information Act 4 of 2013 (POPIA) sets out the conditions for the transfer of personal data. A responsible party may only transfer personal data to a third party who is in a foreign country if:* ***(1)***

(1) Section 72(1)(a) - (e) of POPIA

- *the third party is subject to a law, binding corporate rules or binding agreement which provide an adequate level of protection;*
- *the data subject consents to the transfer;*
- *the transfer is necessary for the performance of a contract between the data subject and the responsible party, or for the implementation of pre-contractual measures in response to the data subject's request;*
- *the transfer is necessary to conclude or perform a contract concluded in the interest of the data subject between the responsible party and a third party; or*
- *the transfer is for the benefit of the data subject, and it was either not reasonably practicable to get the data's subject consent for the transfer, or if it were, the data subject would likely consent.*

▪ *In contrast, most data protection laws do not provide guidance for transferring third party personal data to their countries. For example, POPIA does not state the requirements for transferring personal data to South Africa. Therefore we need to examine the factors to consider to determine whether you can transfer personal to another country.*

1 - Enacted data protection law

▪ *The first factor to consider is if the country you are transferring to:*

- *has data protection law, and*
- *how that law applies.*

▪ ***Data protection law.*** *Countries that do not have comprehensive data protection laws, or simply have draft laws are concerning from a transfer perspective. South Africa has POPIA, which came into full force and effect on 1 July 2021. Before that, organisations may have been concerned about transferring personal data to South Africa. Next, you need to understand how POPIA applies and if the application affects the transfer.*

▪ ***Application of the data protection law.*** *POPIA was enacted in 2013, before the commencement of the GDPR* ***(2)*** *in 2016, so there are some inconsistencies with the laws. Since POPIA was enacted earlier and could not consider the GDPR, the*

(2) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Referenced as 'the GDPR'

rules for applying POPIA are different to most post-GDPR data protection laws. Like the GDPR, these laws have an extra-territorial application, so they apply regardless of whether the processing happens in the European Economic Area (EEA). In practice, laws like the GDPR could apply to South African organisations if they offer goods or services to data subjects in the EU or monitor their behaviour ***(3)****. Therefore, the application of the GDPR focuses on the location of the data subject. For example, if you transfer EU citizen's personal data to South Africa, the GPDR will apply. However, the application of POPIA* ***(4)*** *focuses on the location of the processing* ***(5)****. Transferring personal data is processing personal data,* ***(6)*** *therefore, it is very likely that by transferring the EU personal data to South Africa, POPIA will now apply to that personal data, in addition to the GDPR.*

(3) Article 3.2 of the GDPR.

(4) Section 3 of POPIA.

(5) Available at: https://www.michalsons.com/blog/must-i-comply-with-the-popi-act/41827

(6) The definition of 'processing' in section 1 of POPIA

2 - Adherence to the data protection principles

▪ *The next factor to consider is whether the country you are transferring to has laws that align with the data protection principles. Most data protection laws follow the same set of principles, namely* ***(7)****:*

- *Lawfulness, fairness and transparency,*
- *Purpose limitation*
- *Data minimisation,*
- *Accuracy,*
- *Storage limitation, and*
- *Integrity and confidentiality (security).*

(7) Article 5 of the GDPR.

▪ *In comparison, POPIA follows these principles but describes them as the conditions for lawful processing* ***(8)****. The conditions align substantially to the data protection principles. They are the fundamental bases for lawful processing in South Africa.*

(8) Chapter 3 Part 4 of POPIA.

3 - An adequate level of protection

▪ *Closely related to the second factor for consideration is the level of protection for data subjects in South African law. The concepts of adequate levels of protection or adequacy can sometimes be vague and misconstrued. At present, neither the Information Regulator of South Africa* ***(9)*** *nor the South Africa courts have not ruled on what amounts to an 'adequate level of protection'. POPIA does provide some guidance for factors to consider when determining if a law, binding corporate rules (BCRs) or binding agreement provides adequate protection* ***(10)****. Factors such as whether the law, binding corporate rules or binding agreement:*

(9) Available at: https://www.justice.gov.za/inforeg/

(10) Section 72(1)(a)(i) and (ii).

- *effectively upholds principles for reasonable processing of the information substantially similar to the conditions for the lawful processing of the data subject's personal information;* ***(11)*** *and*
- *includes provisions substantially similar to the crossborder transfer provisions in POPIA, where they relate to the further transfer of personal information from the recipient to third parties in another country.*

(11) In POPIA, data subjects include both natural and juristic persons

▪ *This is very similar to the GDPR, where the general principles for transfer state that the level of protection for natural persons guaranteed in the GDPR should be not undermined* ***(12)****. Considering the adequacy requirements in the GDPR and*

(12) Article 44 of the GDPR

POPIA collectively, they essentially mean that a law, BCRs or binding agreement has:

- *to uphold or substantially similar to the principles or conditions for lawful processing, **(13)** and*
- *crossborder provisions that are substantially similar and align to those in data protection laws.*

(13) Article 5 of the GDPR

▪ *There is a lot of similarity between the crossborder provisions in POPIA and the GDPR. The GDPR 's crossborder approach is more complex and but one could argue that POPIA covers those broad principles, and could be found to have adequate protection for EU personal data. Currently, South Africa does not have an adequacy finding from the European Commission, and it is not clear if the Information Regulator will pursue one, but it is highly recommended.*

4 - Protective measures.

▪ *The fourth factor to consider is whether you can put measures in place to uphold the data protection principles and protect the personal data of data subjects equivalent to the protection by the country of origin's law. Various measures can be put in place to achieve this.*

▪ *Technical measures. Technical measures are controls to protect any technological element within an organisation like their systems, devices, networks and hardware. Typical examples include encryption, firewalls, and password protection. Organisations transferring personal data to South Africa would want to ensure the recipients have suitable technical measures to protect the data from unauthorised access and other incidents.*

▪ *Organisational measures. Organisational measures are measures in place to protect personal data during day-to-day operations. These measures are crucial to ensure that an established standard for protecting personal data exists in an organisation. Typical examples include awareness training for employees, policies and procedures to comply with safeguards, establishing and implementing standards for data protection, assessments and audits on compliance.*

▪ *Contractual measures. Contractual measures are put in place to bind parties legally to specific data protection standards and ensure contractual compliance. From a South African perspective, POPIA requires a responsible party (the equivalent of a controller in the GDPR) to have a written contract with their operator (the equivalent of a processor in the GDPR) to ensure that the operator establishes and maintains the security measures required by POPIA **(14)**.*

(14) Section 21(1) of POPIA.

▪ *In practice, organisations have included data protection provisions or addendums in their existing agreements with their operators. They may also have followed the global approach and signed data processing agreements. These kinds of measures have also extended to contracts between controllers. Therefore, organisations that wish to transfer personal data to South Africa may consider concluding data processing agreements or including data protection clauses in their agreements with South African entities that receive personal data from them as an added measure. This ensures that when you transfer personal data to South*

Africa, it is protected to an equivalent level as the country of origin's law, and to a standard that aligns with the principles of data protection.

Parting thoughts

- *Organisations should carefully consider these factors when transferring personal data in general, and specifically to South Africa. Organisations should do this assessment on a case by case basis. Ideally, all of these factors should be present before you transfer personal data to another country. However, if a country or organisation you want to transfer your personal data to does not meet these requirements after conducting an assessment, if you still insist on the transfer, you must implement supplementary measures to bridge the gap.*

LISA EMMA – IWUOHA

south-africa@
lexing.network

REFERENCES

▪ Le cadre juridique applicable aux transferts de données en dehors de l'Union européenne a été précisé par l'arrêt Schrems II de la Cour de justice de l'Union européenne **(1)** et par les recommandations du CEPD **(2)** formulées dans la foulée. Il en ressort qu'après avoir procédé à une évaluation de la loi du pays de destination, s'il apparaît que cette loi ne présente pas un niveau de protection adéquat des données à caractère personnel (ce qui est le cas par exemple aux Etats-Unis), des mesures supplémentaires doivent être adoptées.

▪ Contre toute attente, en Belgique, le Conseil d'Etat a été le premier à se prononcer sur le sujet. Dans cette affaire, la région flamande avait attribué un marché public à une société, filiale d'une entité américaine, pour la mise en place d'une nouvelle plateforme visant à faciliter la mobilité des personnes handicapées. Cette plateforme devant traiter des données à caractère personnel (dont certaines sensibles), le cahier des charges prévoyait des obligations renforcées en matière de conformité au RGPD. Compte tenu de l'arrêt Schrems II, afin de vérifier la capacité des soumissionnaires à respecter les dispositions du RGPD, le pouvoir adjudicateur avait exigé de remplir un questionnaire relatif aux transferts de données et de le joindre à l'offre.

▪ Les concurrents de la société à qui le marché public a été attribué ont fait appel de la décision d'attribution devant le Conseil d'État belge, en mettant en avant le fait que des données étaient susceptibles d'être transférées aux Etats-Unis et qu'aucune mesure supplémentaire ne pouvait être prise pour remédier au niveau inadéquat de protection des données dans ce pays.

▪ Dans une première décision **(3)**, le Conseil d'État belge a décidé de suspendre l'attribution du marché en cause, au motif que la décision prise par le pouvoir adjudicateur ne permettait pas un réel examen de la conformité de l'offre aux dispositions du RGPD et du cahier des charges.

▪ Le pouvoir adjudicateur a alors retiré la décision d'attribution initiale et pris une nouvelle décision d'attribution en faveur ... du même soumissionnaire. Un nouveau recours a été introduit, invoquant une violation des articles 28, 44 et 45 à 50 du RGPD puisque le soumissionnaire retenu mentionnait dans son offre la possibilité de transférer les données aux États-Unis.

▪ Lors de ce nouvel examen de la légalité des offres présentées **(4)**, le Conseil d'État belge a relevé cette fois le soin particulier qui avait été apporté à la vérification du respect de la réglementation en matière de protection des données. En effet, le pouvoir adjudicateur avait demandé au délégué à la protection des données du service de la mobilité et des travaux publics d'examiner attentivement les offres. Ce dernier a confirmé que l'offre était bien conforme aux exigences des documents contractuels, et ce bien qu'un si un transfert de données vers les Etats-Unis soit possible.

▪ De fait, le Conseil d'Etat a rappelé que, même après l'arrêt Schrems II, un transfert de données vers les Etats-Unis pouvait encore être autorisé, à condition

(1) CJUE, 16 juillet2020 (Data Protection Commissioner c. Facebook Ireland Ltd, Maximillian Schrems), C-311/18, ECLI:EU:C:2020:559, accessible à l'adresse : https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=FR&mode=lst&dir=&occ=first&part=1&cid=12312155

(2) 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, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en.)

(3) Conseil d'Etat, 12 mai 2021, n°250.599.

(4) Conseil d'Etat, 19 août 2021, n°251.378

que des mesures supplémentaires soient adoptées. Malheureusement, le Conseil n'a pas repris dans sa décision les mesures spécifiques adoptées à cet effet par le titulaire du marché. Il laisse toutefois entrevoir que les mesures demandées par la recommandation 01/2020 du CEPD étaient bien mises en œuvre :

- « L'affirmation des requérants selon laquelle aucune mesure supplémentaire n'est envisageable pour remédier au niveau insuffisant de protection des données aux États-Unis, même au moyen du chiffrement ou de la pseudonymisation, semble méconnaître, de manière générale, la manière dont de telles mesures pourraient être mises en œuvre. Il ressort du dossier que ni la VTC [pour « Vlaamse toezichtcommissie voor de verwerking van persoonsgegevens », c'est-à-dire la Commission de contrôle flamande du traitement des données à caractère personnel] ni le Comité européen de la protection des données ne s'opposent à un chiffrement complet des données avant leur remise au prestataire de services, les clés de chiffrement étant conservées entièrement sous le contrôle de l'instance flamande. Il ressort du dossier que le soumissionnaire sélectionné offre un ensemble complet de garanties. » (5)

(5) Paragraphe 16 de l'arrêt du Conseil d'État du 19 août 2021 précité (traduction libre).

▪ Par cette décision, le Conseil d'Etat belge a donc confirmé la jurisprudence Schrems II en Belgique et a appliqué la recommandation du CEPD. Il est toutefois regrettable que le Conseil n'ait pas plus détaillé sur les mesures exactes mises en œuvre par l'adjudicataire. Dès lors, il est difficile de savoir si le Conseil a procédé à un examen concret des garanties.

ELÉONORE COLSON

belgium@
lexing.network

REFERENCES

▪ *Following the Schrems II ruling of the European Court of Justice **(1)** and the resulting recommendations of the EDPB **(2)**, the legal framework applicable to data transfers outside the European Union has been clarified. After conducting an assessment of the law of the country of destination, if it appears that this law does not present an adequate level of protection of personal data (e.g. the United States), additional measures must be adopted.*

▪ *Contrary to all expectations, in Belgium, the Council of State was the first to have to decide on the subject. The Flemish Region of Belgium had awarded a public contract to a company, a subsidiary of a U.S. entity, for the implementation of a new platform aimed at facilitating the mobility of disabled people. As this platform was to process a certain amount of personal data (some of which was sensitive), the contract specifications provided for certain reinforced obligations in terms of compliance with the GDPR. In view of the Schrems II ruling, in order to verify the tenderers' ability to comply with the provisions of the GDPR, the contracting authority also required to fulfill a questionnaire relating to the data transfers and to attach it to the tender.*

▪ *The award decision was appealed to the Council of State. The competitors of the selected company argued that no additional measures could be taken to remedy the inadequate level of data protection in the United States. In this case, however, a data transfer was still possible.*

▪ *In a first decision **(3)**, the Council of State decided to suspend the award of the contract in question, on the grounds that the decision taken by the contracting authority did not allow for a real examination of the compliance of the tender with the provisions of the GDPR and the contract documents.*

▪ *The contracting authority then withdrew the initial award decision and took a new award decision ... to the same tenderer. A new appeal was lodged, alleging a violation of Articles 28, 44 and 45 to 50 of the GDPR since the successful tenderer mentioned in its tender the possibility of transferring the data to the United States.*

▪ *During this new examination of the legality of the tenders submitted **(4)**, the Council of State noted this time the particular care that had been taken to verify the respect of data protection regulation. To this end, the contracting authority had asked the data protection officer of the Mobility and Public Works Department to examine the tenders carefully. The latter confirmed that the tender complied with the requirements of the contract documents, although a transfer of data to the United States was still possible.*

▪ *The State Council recalled that a transfer of data to the United States was still permitted, even after the Schrems II ruling, provided that additional measures were adopted. Unfortunately, the Council did not include in its decision the specific measures adopted by the successful tenderer. However, it suggests that the measures called for by EDPB recommendation 01/2020 are implemented:*

(1) CJEU, July 16, 2020 (Data Protection Commissioner v. Facebook Ireland Ltd, Maximillian Schrems), C-311/18, ECLI:EU:C:2020:559, available at: https://curia.europa.eu/juris/document/document.jsf?docid=228677&text=&dir=&doclang=EN&part=1&occ=first&mode=DOC&pageIndex=0&cid=4488618

(2) EDPB, Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer_en

(3) Council of State, May 12, 2021, n°250.599.

(4) Council of State, August 19, 2021, n°251.378

- *"Petitioners' assertion that no additional measures are conceivable that would remedy the inadequate level of data protection in the United States, even through encryption or pseudonymization, appears to misunderstand, in a general way, how such measures could be implemented. From the file, it appears that neither the VTC [for "Vlaamse toezichtcommissie voor de verwerking van persoonsgegevens", i.e. "Flemish Commission for the Supervision of the Processing of Personal Data"] nor the European Data Protection Board object to full encryption of the data before it is handed over to the service provider, with the encryption keys being kept entirely under the control of the Flemish appeal body. The file shows that the selected tenderer offers a complete set of guarantees."* ***(5)***

▪ *With this decision, the Belgian Council of State has therefore confirmed the Schrems II case law at the Belgian level and has applied the content of the EDPB's recommendation. It is regrettable, however, that the Council did not elaborate on the exact measures implemented by the successful tenderer. It is difficult to know whether the Council carried out a concrete examination of the guarantees.*

(5) Paragraph 16 of the aforementioned Council of State decision of August 19, 2021 (Free translation).

ELEONORE COLSON

belgium@
lexing.network

Cadre juridique applicable à la communication de renseignements personnels à l'extérieur du Québec

▪ Le 21 septembre 2021, l'Assemblée nationale du Québec a adopté la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels **(1)**.

▪ Cette loi vient modifier mais aussi ajouter plusieurs dispositions applicables à la protection des renseignements personnels dans diverses lois, dont la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels **(2)** et la Loi sur la protection des renseignements personnels dans le secteur privé **(3)**.

▪ Ces deux lois ont pour objet d'encadrer respectivement les exigences que les organismes publics et les entreprises doivent respecter quant au cycle de vie des renseignements personnels qu'ils recueillent, détiennent, utilisent ou communiquent. Elles précisent également les droits des personnes concernées et les pouvoirs de la Commission d'accès à l'information.

▪ Relativement à la communication des renseignements personnels à l'extérieur du Québec, la nouvelle loi modifie le régime applicable tant à l'égard des organismes publics (article 70.1) que des entreprises (article 17). Il est à noter que ce nouveau régime entrera en vigueur deux ans après la sanction de la loi, laquelle est intervenue le 22 septembre 2021.

▪ Ainsi à partir de cette date, les organismes publics et les entreprises devront procéder à une évaluation des facteurs relatifs à la vie privée (« EFVP »).

▪ Il est prévu que pareille évaluation devra se faire lorsqu'un organisme public ou une entreprise confie à une personne ou à un organisme à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour son compte des renseignements personnels.

▪ Cette évaluation devra notamment tenir compte des éléments suivants :

- de la sensibilité des renseignements personnels ;
- de la finalité de leurs utilisations ;
- des mesures de protection, y compris celles qui sont contractuelles, dont les renseignements bénéficieront. Précisons que la référence aux mesures contractuelles a été ajoutée lors de l'étude article par article du PL64 ;
- du régime juridique applicable dans l'État où ces renseignements seront communiqués, notamment les principes de protection des renseignements personnels qui y sont applicables.

▪ La communication ne pourra se faire que si l'évaluation démontre que les renseignements personnels bénéficieront d'une protection adéquate, notamment

REFERENCES

(1) Pour un aperçu du cheminement du projet de loi n°64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (« PL64 ») ayant conduit à l'adoption de la loi : http://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html

(2) RLRQ, c. A-2.1. https://www.canlii.org/fr/qc/legis/lois/rlrq-c-a-2.1/derniere/rlrq-c-a-2.1.html

(3) RLRQ, c. P-39.1, https://www.canlii.org/fr/qc/legis/lois/rlrq-c-p-39.1/derniere/rlrq-c-p-39.1.html

au regard des principes de protection des renseignements personnels généralement reconnus.

- Il convient de préciser que lors du dépôt du PL64, il était fait référence au « degré d'équivalence » et à une « protection équivalant à celle prévue à la présente loi ». Cette référence à l'équivalence des lois a été retiré lors de l'étude article par article du PL64. Elle a été remplacée par la notion de « protection adéquate ».

- Dès lors, la disposition prévoyant que « le ministre publie une liste d'États dont le régime juridique encadrant les renseignements personnels équivaut aux principes de protection des renseignements personnels applicables au Québec » a été supprimée.

- Par ailleurs, les organismes publics et les entreprises devront conclure une entente écrite. Cette entente devra tenir compte notamment des résultats de l'évaluation et, le cas échéant, des modalités convenues dans le but d'atténuer les risques identifiés dans le cadre de cette évaluation.

- Des exceptions sont prévues à cette obligation de réaliser une EFVP et de conclure une entente écrite. Il en va ainsi, tant à l'égard des organismes publics que des entreprises, lorsque la communication doit être faite en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée. Il en est de même pour les organismes publics lorsque la communication est manifestement au bénéfice de la personne concernée ou encore lorsqu'elle s'effectue dans le cadre d'un engagement international, d'une entente visant un programme de coopération ou si cela s'inscrit dans le cadre d'une entente prises en matière de santé publique.

- Enfin advenant la communication de renseignements personnels en contravention aux nouvelles exigences, les organismes publics et les entreprises s'exposent à des amendes, éventuellement à des sanctions administratives pécuniaires dans le cas des entreprises, dont les montants ont été substantiellement augmentés.

CYNTHIA CHASSIGNEUX

canada@
lexing.network

REFERENCES

Legal framework applicable to the transfer of personal information outside Quebec

▪ *On 21 September 2021, the National Assembly of Quebec adopted the Act to modernize legislative provisions as regards the protection of personal information* ***(1)****.*

▪ *This Act amends and adds several provisions applicable to the protection of personal information in various laws, including the Act respecting Access to documents held by public bodies and the Protection of personal information* ***(2)*** *and the Act respecting the protection of personal information in the private sector* ***(3)****.*

▪ *The purpose of these two Acts is to provide a framework for the requirements that public bodies and enterprises must respect regarding the life cycle of the personal information they collect, hold, use or communicate. They also specify the rights of the persons concerned and the powers of the Commission d'accès à l'information.*

▪ *With respect to the transfer of personal information outside Quebec, the new Act modifies the rules applicable to both public bodies (section 70.1) and enterprises (section 17). These new rules will come into force two years after the Act's date of assent (22 September 2021).*

▪ *As of that date, public bodies and enterprises will have to carry out an assessment of privacy-related factors (privacy impact assessment or PIA).*

▪ *Such an assessment will have to be carried out when a public body or an enterprise entrusts a person or a body outside Quebec with the task of collecting, using, releasing or keeping personal information on its behalf.*

▪ *This assessment must, in particular, take into account:*

- *the sensitivity of the personal information;*
- *the purposes for which it is to be used;*
- *the protection measures, including contractual measures, that would apply to the information (Note that the reference to contractual measures was added during the clause-by-clause consideration of Bill 64);*
- *the legal framework applicable in the State in which the information would be released, including the personal information protection principles applicable there.*

▪ *The information may be released only if the assessment establishes that the personal information receives adequate protection, including with respect to the generally accepted principles for the protection of personal information.*

▪ *It should be noted that when Bill 64 was tabled, reference was initially made to the "degree of equivalency" and to "protection equivalent to that afforded under this Act". The reference to equivalency of laws was removed during the clause-by-*

(1) Pour un aperçu du cheminement du projet de loi n°64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (« PL64 ») ayant conduit à l'adoption de la loi : http://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html

(2) RLRQ, c. A-2.1. https://www.canlii.org/fr/qc/legis/lois/rlrq-c-a-2.1/derniere/rlrq-c-a-2.1.html

(3) RLRQ, c. P-39.1, https://www.canlii.org/fr/qc/legis/lois/rlrq-c-p-39.1/derniere/rlrq-c-p-39.1.html

clause consideration of Bill 64 and replaced by the concept of "adequate protection".

- *Consequently, the provision that previously provided or that "The Minister shall publish (…) a list of States whose legal framework governing personal information is equivalent to the personal information protection principles applicable in Quebec" was deleted.*

- *In addition to the PIA, public bodies and enterprises will also have to enter into a written agreement. This agreement will have to take into account the results of the assessment and, if applicable, the terms agreed on to mitigate the risks identified in the assessment.*

- *There are exceptions to the obligation to conduct a PIA and to conclude a written agreement. This is the case for both public bodies and enterprises when the release must be made because of the urgency of a situation that threatens the life, health or safety of the person concerned. The same applies to public bodies when the release is clearly for the benefit of the person to whom it relates or when it is within the scope of an international commitment, an agreement concerning a cooperation program or an agreement taken in the area of public health.*

- *Finally, if personal information is disclosed in contravention of the new requirements, public bodies and enterprises may be subject to fines, and possibly monetary administrative penalties in the case of enterprises, the amounts of which have been substantially increased.*

CYNTHIA CHASSIGNEUX

canada@
lexing.network

JADE & FOUNTAIN PRC LAWYERS

Les transferts internationaux d'informations personnelles en droit chinois

Les transferts en vertu de la loi sur la cybersécurité : principe et exception

▪ Entrée en vigueur le 1er juin 2017, la loi sur la cybersécurité (*Cyber-security Law*, CSL) de la République populaire de Chine (RPC) prévoit que, par principe, les informations personnelles **(1)** et les données importantes **(2)** collectées et générées dans le cadre de l'exploitation d'une infrastructure d'information critique (IIC**) (3)** par un opérateur sur le territoire chinois doivent impérativement être stockées en Chine.

▪ Par exception à ce principe, sauf disposition contraire de la loi et des règlements, le transfert vers un ou plusieurs territoires étrangers peut avoir lieu à condition d'être justifié par une raison commerciale et de faire l'objet d'une évaluation de la sécurité en application des règles qui seront élaborées par le Bureau d'État de l'information sur internet (*State Internet Information Office*, SIIO) en consultation avec d'autres départements ministériels (NB : Les termes « territoire chinois » ou « Chine font référence à la « Chine continentale » uniquement et, par conséquent, le terme « territoire étranger » comprend également les régions administratives spéciales de Hong Kong et de Macao ainsi que Taiwan qui font constitutionnellement partie du territoire chinois mais qui sont considérés comme des territoires distincts de la Chine continentale aux fins de la CSL).

Les règles encadrant l'évaluation de la sécurité en cas transfert en dehors de Chine

▪ A ce jour, les règles encadrant l'évaluation de la sécurité n'ont pas encore été officiellement publiées, bien qu'un projet de « Règles sur l'évaluation de la sécurité des transferts d'informations personnelles vers l'étranger » ait été dévoilé en juin 2019 par le SIIO et soumis à consultation pour commentaires.

▪ Ce projet prévoit la procédure à suivre pour passer une évaluation de la sécurité ainsi que les pièces justificatives à produire :

- L'opérateur concerné (équivalent du responsable du traitement au sens du RGPD) dépose une demande pour faire l'objet d'une évaluation de la sécurité auprès du département du SIIO au niveau provincial, qui rend ses conclusions sous 15 jours ouvrables, ce délai pouvant être prolongé si la complexité du dossier le justifie. L'opérateur a le droit de contester le résultat de l'évaluation et de demander un réexamen de son dossier ;
- Le dossier de demande soumis par l'opérateur est composé a) du formulaire de demande, b) du contrat conclu entre l'opérateur et le destinataire étranger et c) du rapport d'analyse des risques présentés par le transfert et des mesures à prendre pour faire face à ces risques ;
- Lors de l'évaluation de la sécurité, les agents du SIIO vérifient principalement a) le respect total de la législation et de la réglementation applicables, b) l'applicabilité du contrat conclu entre l'opérateur et le destinataire (notamment pour vérifier si les intérêts légitimes de la personne concernée seront suffisamment protégés en vertu des termes

REFERENCES

(1) Dans la CSL, « informations personnelles » désigne les « informations enregistrées par des moyens électroniques ou non qui permettent d'identifier un individu, seules ou conjointement avec d'autres informations, telles que le nom, la date de naissance, le numéro de la pièce d'identité, les données biométriques, l'adresse du domicile, le numéro de téléphone ».

(2) Les « données importantes » sont des données étroitement associées à la sécurité nationale, au développement économique et aux intérêts publics (y compris les données brutes et les données dérivées).

(3) Les « infrastructures d'information critiques » désignent les infrastructures d'information qui, en cas de destruction, de dysfonctionnement ou de fuite de leurs données, sont susceptibles de mettre gravement en danger la sécurité nationale, l'économie et les intérêts publics. La CSL énumère de manière non exhaustive les IIC dans les secteurs suivants : services de télécommunication et d'information, énergie, transport, irrigation, finances, service public, administration électronique.

du contrat) ; c) si les informations personnelles ont bien été collectées en toute légalité ; d) les incidents, infractions ou crimes antérieurs concernant la sécurité des données impliquant l'opérateur et le destinataire.

▪ Le projet dispose également que les informations suivantes doivent impérativement figurer dans le contrat conclu entre l'opérateur et le destinataire des données :

- La finalité du transfert ainsi que la catégorie des informations personnelles concernées et leur durée de conservation ;
- Le fait que la personne concernée sera bénéficiaire de la clause spécifique relative aux droits de la personne concernée ;
- L'existence du droit pour la personne concernée de tenir l'opérateur et le destinataire responsables individuellement ou conjointement des dommages qu'elle a subis, sauf preuve contraire de l'opérateur ou du destinataire ;
- Le fait que le contrat sera immédiatement résilié ou qu'une nouvelle évaluation de la sécurité sera requise en cas d'évolution de la législation dans le pays du destinataire de nature à rendre impossible l'exécution du contrat ;
- En cas de résiliation du contrat, le fait que l'opérateur ou le destinataire ne sera pas exempté de ses obligations en vertu de la clause relative aux droits de la personne concernée, à moins qu'il n'ait correctement détruit ou anonymisé les informations personnelles de la personne concernée.

▪ Etonnement, contrairement à ce qui est prévu par la CSL, l'évaluation de la sécurité prévue par ledit projet semble concerner tous les opérateurs souhaitant transférer des informations personnelles vers l'étranger, qu'ils soient ou non des opérateurs d'IIC.

Les transferts en vertu de la loi sur la protection des informations personnelles

▪ De manière générale, la Chine est très prudente en matière de transfert d'informations personnelles à l'étranger, comme en témoigne la proposition faite par le SIIO, en juillet 2021, de demander à ce que tous les opérateurs enregistrant plus d'un million d'utilisateurs individuels et projetant d'être cotés sur une bourse étrangère soient soumis à une évaluation de la cybersécurité **(4)**.

▪ La très attendue loi sur la protection des informations personnelles (*Personal Information Protection Law*, PIPL) de la RPC, adoptée le 20 août 2021, entrera en vigueur le 1er novembre 2021. Cette loi précise davantage les étapes à suivre pour le transfert de données vers l'étranger, tout en illustrant une fois de plus la prudence de l'approche chinoise en la matière.

▪ Ainsi, en vertu de la PIPL, si cela est justifié par des raisons commerciales, un responsable du traitement **(5)** peut procéder au transfert vers l'étranger d'informations personnelles dans la mesure où une des conditions suivantes est remplie :

- (a) passer avec succès l'évaluation de sécurité réalisée par les autorités compétentes ;

(4) Le régulateur aurait été alerté par la cotation à la Bourse de New York de Didi, l'un des principaux opérateurs de services de taxi et de VTC du pays. En règle générale, une entreprise technologique cotée sur une bourse étrangère s'engage à respecter les exigences en matière de divulgation d'informations dans le pays concerné. Or, une telle divulgation d'informations est susceptible d'être en contradiction avec les impératifs de sécurité des données prévus par les lois chinoises.

(5) Il n'y a pas de distinction entre le « responsable du traitement » et le « sous-traitant de données » dans la PIPL, mais le « data processor » dans le PIPL peut correspondre au « responsable du traitement » au sens du RGPD.

- (b) obtenir une certification en matière de protection des informations personnelles délivrée par un organisme spécialisé ;
- (c) conclure avec le destinataire un contrat, établi sur le modèle de contrat élaboré par les autorités compétentes, afin de stipuler clairement les droits et obligations de chaque partie ;
- (d) respecter toutes autres conditions spécifiées par la loi, la réglementation ou les autorités compétentes.

▪ Le responsable du traitement s'engage également à prendre les mesures nécessaires pour s'assurer que le traitement des données par le destinataire établi dans un pays étranger bénéficie d'une protection au moins aussi favorable que celle garantie par la PIPL.

▪ Par ailleurs, outre les mesures susmentionnées, le responsable du traitement doit obtenir le consentement distinct de la personne concernée au transfert et lui fournir les informations suivantes :

- a) l'identité et les coordonnées du destinataire ;
- b) la finalité et les modalités du traitement ;
- c) les catégories d'informations personnelles qui feront l'objet d'un traitement ;
- d) les modalités et la procédure par lesquelles la personne concernée peut exercer les droits qui lui sont conférés par la PIPL auprès du destinataire situé à l'étranger.

▪ Les opérateurs d'IIC et les autres responsables de données qui traitent un grand nombre d'informations personnelles (seuils fixés par la réglementation applicable) doivent obligatoirement stocker en Chine les informations personnelles collectées et générées en Chine. En cas de nécessité de transférer des informations à l'étranger, ils doivent d'abord se soumettre à une évaluation de la sécurité effectuée par les autorités compétentes.

▪ Enfin, il est interdit à un responsable du traitement de fournir des informations personnelles stockées sur le territoire chinois à une autorité judiciaire ou à un organisme répressif étranger sans avoir obtenu l'autorisation préalable des autorités chinoises compétentes.

JUN YANG

china@
lexing.network

International transfer of personal information under Chinese law

The principle and exception under Cyber-Security Law

▪ *The PRC Cyber-security Law ("CSL") effective on June 1st, 2017 provides that the personal information* ***(1)*** *and important data* ***(2)*** *collected and generated in course of operation by a critical information infrastructure* ***("CII") (3)*** *operator within Chinese territory shall be imperatively stored in China.*

▪ *As an exception to this principle, if the outbound transfer to overseas jurisdiction(s) is justified by a business reason, the security assessment shall be required in application of the rules to be elaborated by the State Internet Information Office("SIIO") in consultation with other ministerial departments save otherwise provided by law and regulation (NB: The above term "Chinese territory" or "China" refer to the "mainland China" only and accordingly the term "overseas jurisdiction" above covers Hong Kong SAR, Macau SAR and Taiwan region which are constitutionally part of Chinese territory but remain as separate jurisdictions from the mainland China for purpose of CSL.).*

The rules governing the security assessment for outbound transfer of personal information

▪ *The rules governing the security assessment have not yet been officially released though the bill of "Rules on security assessment on outbound transfer of personal information" was unveiled in June, 2019 by SIIO for comments.*

▪ *The said bill provides the applicable procedure, documentary requirements as well as criteria for the security assessment which are summarized as follows:*

- *The operator concerned (equivalent to Data Controller in GDPR) shall file application for security assessment with SIIO department at provincial level and the latter shall render its conclusion of security assessment within 15 working days or a longer period if justified by complexity of the dossier. The operator shall be entitled to apply for review of the conclusion should it contest such conclusion;*
- *The application dossier submitted by the operator shall be comprised of (a) application form; (b) the contract concluded between the operator and the overseas recipient; (c) the analytical report on the risks and measures to be taken;*
- *The key criteria retained by the SIIO officers when conducting the security assessment include essentially the following: (a) full compliance with applicable law and regulation; (b) enforceability of the contract concluded between the operator and the recipient (in particular, to ascertain whether the legitimate interests of the data subject will be sufficiently protected under the terms and conditions of the contract); (c) the personal information are collected in full legality; (d) any data incident,*

REFERENCES

(1) The "personal information" in CSL refers to the "information recorded by electronic or other means which may identify an individual by such information alone or in conjunction of other information, including but not limited to name, date of birth, ID document number, biometrics, residential address, phone number."

(2) The "important data" refers to the data closely associated with national security, economic development and public interests (including raw data and derivative data)

(3) The ''CII'' refers to the information infrastructure which, if destroyed, dysfunctional or leaked, is likely to seriously endanger the national security, economy and public interests. CSL enumerates in non-exhaustive manner the CII in the following sectors: telecommunication and information service, energy, transportation, irrigation, finance, public service, e-government.

offence/crime concerning data security ever involving the operator and recipient.

▪ *The said bill also provides that the following terms and conditions shall be imperatively included in the contract concluded between the operator and the recipient:*

- *The purpose of the outbound transfer and the category and retention period of personal information concerned;*
- *The data subject concerned shall be the beneficiary of the specific clause substantiating the rights for data subject;*
- *The data subject shall be entitled to hold the operator and recipient liable individually or jointly for his/her damages save otherwise proved by operator/recipient;*
- *The contract shall be immediately terminated or a fresh security assessment is required in case where the legislative evolution in the country of the recipient renders the contract unlikely to be performed;*
- *The operator/recipient shall not be exempted for their corresponding obligations under the clause reserved for the rights of the data subject in case of termination of the contract unless they have properly disposed of or de-identified the personal information of the data subject concerned.*

▪ *One curious "deviation" from the CSL is that the security assessment under the said bill appears to concern all operators applying for outbound transfer of personal information regardless whether they are CII operator.*

The outbound transfer of personal information under Personal Information Protection Law

▪ *Over all, China is very cautious on the issues with respect to the outbound transfer of personal information to overseas jurisdictions. This position is well illustrated by SIIO's proposal in July, 2021 to request that all operators registering more than 1 million individual users be subject to a cyber-security review should they intend to be listed in an overseas stock exchange* ***(4)****.*

▪ *The long-awaited "PRC Personal Information Protection Law" ("PIPL") was finally unveiled on August 20, 2021 and will take effect on November 1, 2021. PIPL came to shed more light on the roadmap for outbound transfer of data whilst it once again highlights the cautious approach of Chinese approach in this regard.*

▪ *A data processor* ***(5)****, if justified by a business reason, may proceed with outbound transfer of personal information if one of the following conditions is fulfilled:*

- *(a) pass successfully the security assessment by competent authorities;*
- *(b) receive personal information protection certification by professional agency;*
- *(c) A contract based on the template elaborated by competent authorities entered into with the recipient of personal information based in overseas jurisdictions to clearly stipulate the rights and obligations of each party.*
- *(d) other conditions specified by law, regulation or the competent authorities.*

(4) The regulator was reportedly alerted by listing on NYSE of Didi, a leading cab-hailing platform operator in the country. Typically, a tech company listed in an overseas stock exchange shall commit to meet information disclosure requirement in the jurisdiction concerned. Such information disclosure is however likely in contradiction with the data security imperatives under the above Chinese laws

(5) There is no distinction between ''data controller'' and ''data processor'' under PIPL, but ''data processor" under PIPL may cover the "data controller" in the sense of GDPR

▪ *The processor shall take necessary measures to ensure that the processing of the recipient of the personal information in overseas jurisdiction be under the protection no less favorable than PIPL.*

▪ *In addition to the above measures, the processor shall inform the data subject of the following information and secure the separate consent from the data subject:*

- *(a) the identity and contact details of the recipient;*
- *(b) purpose and modality of processing;*
- *(c) the categories of personal information to be processed;*
- *(d) the modality and procedure whereby the data subject may exercise his/her rights under PIPL vis-a-vis the recipient in overseas jurisdiction.*

▪ *CII Operator and other data processor whose processing breaching the quantitative threshold set by applicable regulation shall store in China the personal information collected and generated in China. They have to pass successfully the security assessment by competent authorities if outbound transfer of personal information is justified.*

▪ *Last but not the least, a data processor shall be prohibited from providing personal information stored in Chinese territory to any foreign judiciary or law enforcement department unless duly approved by Chinese competent authorities.*

JUN YANG

china@
lexing.network

REFERENCES

Les transferts internationaux de données personnelles en droit espagnol

▪ En Espagne, les transferts internationaux de données à caractère personnel sont régis par les dispositions du RGPD. La Loi organique 3/2018, du 5 décembre, relative à la protection des données personnelles (LOPD), complète ou précise très brièvement certains aspects du RGPD en ce qui concerne le régime des transferts internationaux de données.

▪ Ainsi, par exemple, l'article 42 de la LOPD établit les cas soumis à l'autorisation préalable des autorités de protection des données (AEPD et autorités régionales en Catalogne et Madrid), qui sont ceux qui impliquent des transferts internationaux de données vers des pays ou des organisations internationales qui ne disposent pas d'une décision d'adéquation approuvée par la Commission européenne ou qui ne sont couverts par aucune des garanties prévues à l'article 41 de la LOPD. Dans ce cas, l'AEPD ou les autorités régionales de protection des données peuvent autoriser les transferts internationaux de données :

- qui reposent sur l'apport de garanties adéquates fondées sur des clauses contractuelles correspondant aux clauses types prévues à l'article 46 du RGPD, et
- lorsqu'ils sont effectués par des autorités ou des entités publiques sur la base de dispositions incorporées dans des accords internationaux qui incorporent des droits effectifs et exécutoires pour les personnes concernées.

▪ En revanche, depuis l'entrée en vigueur du RGPD, l'AEPD n'a pas publié ses propres critères ou lignes directrices pour aider les responsables de traitement et les sous-traitants à se conformer aux règles régissant les transferts internationaux de données, renvoyant dans ses communiqués de presse aux travaux et communications publiés par le CEPD (Comité européen de la protection des données).

▪ Un résumé de la réglementation applicable aux transferts internationaux de données, les questions fréquemment posées et les résolutions autorisant certains transferts internationaux de données peuvent être consultés sur le site de l'AEPD (1).

(1) Transferencias internacionales | AEPD (uniquement en espagnol)

MARC GALLARDO

spain
@lexing.network

REFERENCES

International transfers of personal data under Spanish law

▪ *In Spain, international data transfers are governed by the provisions of the GDPR. Organic Law 3/2018, of 5 December, on the Protection of Personal Data (LOPD), complements or specifies very briefly some aspects of the GDPR and of the international data transfer regime.*

▪ *Thus, for example, Article 42 of the LOPD establishes the cases subject to prior authorisation by the data protection authorities (Spanish AEPD and the regional ones in Catalonia and Madrid), which are those involving international transfers of data to countries or international organisations that do not have an adequacy decision approved by the European Commission or that are not covered by any of the guarantees provided for in Article 41 of the LOPD. In such cases, the AEPD or regional data protection authorities may authorise those international data transfers:*

- *i) that are based on the provision of adequate guarantees based on contractual clauses that correspond to the standard clauses provided for in Article 46 of the GDPR and*
- *ii) when they are carried out by public authorities or entities on the basis of provisions incorporated in international agreements that incorporate effective and enforceable rights for data subjects.*

▪ *On the other hand, since the entry into force of the GDPR, the AEPD has not published its own criteria or guidelines to assist data controllers and data processors in complying with the rules governing international data transfers, referring in its press releases to the work and communications issued by the EDPB (European Data Protection Board).*

▪ *A summary of the regulations applicable to international data transfers, frequently asked questions and the resolutions authorising certain international data transfers can be consulted on the AEPD website* ***(1)****.*

(1) Transferencias internacionales | AEPD (only in Spanish)

MARC GALLARDO

spain
@lexing.network

Les transferts internationaux de données personnelles en droit français

▪ En France, les transferts internationaux de données à caractère personnel sont régis par la loi Informatique et libertés **(1)**.

(1) Loi Informatique et libertés, art. 123

▪ Un responsable de traitement ne peut transférer des données à caractère personnel vers un Etat n'appartenant pas à l'Union européenne que si cet Etat assure un niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement dont ces données font l'objet ou peuvent faire l'objet.

▪ Ce sera le cas si le pays de l'importateur bénéficie d'une décision d'adéquation.

▪ Pour les pays ne bénéficiant pas d'une décision d'adéquation, il est possible de recourir à différents outils juridiques tels que notamment les clauses contractuelles types (CCT) ou les règles internes d'entreprises (BCR).

▪ S'agissant des CCT, les modèles de clauses mises à jour par la Commission européenne le 4 juin 2021 **(2)** sont composés d'articles généraux applicables à l'ensemble des situations et d'articles spécifiques selon le rôle des parties au traitement (caractère modulaire des clauses).

(2) Annexe de la décision d'exécution de la Commission relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil, 4-6-2021

▪ L'adoption de ces CCT implique de les accepter sans modification de contenu. Seules des modifications de forme ou de choix des modules peuvent être faites.

▪ Avant d'utiliser les CCT, il convient de mener une analyse de la règlementation locale du pays tiers.

▪ Les CCT imposent en effet à l'exportateur de données de tenir compte de la législation applicable à l'importateur des données pour déterminer si les clauses contractuelles types pourront produire tous leurs effets et offrir une protection suffisante.

▪ L'analyse doit permettre de déterminer si la législation du pays de destination permet l'accès aux données par les autorités publiques dans des conditions permettant d'offrir une protection équivalente à celle pratiquée en Europe. Selon le CEPD **(3)**, si les autorités publiques ont accès aux données, la protection n'est pas substantiellement équivalente lorsque :

(3) Recommandations 02/2020 sur les garanties essentielles européennes pour les mesures de surveillance, 10-11-2020

- les règles d'accès ne sont pas claires, précises et accessibles ;
- l'accès n'est pas strictement nécessaire et limité aux objectifs légitimes poursuivis en lien avec la sécurité nationale ;
- il n'existe pas de mécanisme de supervision indépendant ;
- il n'existe pas de recours efficaces à la disposition des personnes concernées.

▪ Cette analyse doit être effectuée au cas par cas, en tenant compte du nombre d'acteurs, des canaux, des transferts ultérieurs, des types de destinataires, des finalités, de la nature des données, du secteur économique, du lieu de stockage des données etc.

▪ A défaut, l'exportateur doit mettre en place, en plus des clauses, des garanties supplémentaires avec contrôle effectif de ces mesures, notamment par des audits.

▪ Les mesures peuvent être techniques et/ou contractuelles.

▪ La difficulté provient du fait que peu de mesures ou garanties supplémentaires sont reconnues, notamment par le CEPD, comme des garanties efficaces.

▪ Il a considéré que dans certains cas, des mesures supplémentaires n'étaient pas à date identifiées. C'est le cas par exemple, des solutions cloud nécessitant un accès en clair aux données **(4)**.

▪ A cet égard, en France, la position de la Cnil, autorité de contrôle en matière de protection des données, est alignée avec celle du CEPD. Elle n'a pas encore rendu de décision publique sur ce sujet.

▪ Toutefois, il convient de relever qu'elle a pu indiquer, pour les outils américains utilisés pour l'enseignement supérieur et la recherche, qu'une période transitoire devait exister en attente de recherche alternative de solutions à ces outils **(5)**.

▪ Les plus grands (AWS, Google, Microsoft, etc.) ont d'ores et déjà annoncé avoir pris des mesures et garanties supplémentaires et ont modifié leur DPA (Data Protection Agreement) en les explicitant.

▪ Il reste à voir si la Cnil, à l'occasion d'une procédure, estimera que ces mesures applicables à des flux vers les Etats-Unis sont suffisantes et permettent d'utiliser les clauses contractuelles types ou les BCR (*Binding Corporate Rules*).

(4) 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, version 2.0, 18-6-2021

(5) La CNIL appelle à des évolutions dans l'utilisation des outils collaboratifs états-uniens pour l'enseignement supérieur et la recherche, 27-5-2021

CELINE AVIGNON

france
@lexing.network

International transfers of personal data under French law

▪ *In France, international transfers of personal data are governed by the Data Protection Act* ***(1)****.*

▪ *A controller may only transfer personal data to a country outside the European Union if that country ensures a sufficient level of protection of the privacy and fundamental rights and freedoms of individuals with regard to the processing their data are or may be subject to.*

▪ *There is a sufficient level of protection if the data importer's country has been granted an adequacy decision.*

▪ *For countries that do not benefit from an adequacy decision, other legal tools may be used such as standard contractual clauses (SCC) or binding corporate rules (BCRs).*

▪ *With regard to SCCs, the model clauses updated by the European Commission on 4 June 2021* ***(2)*** *are composed of (i) general clauses applicable to all situations and (ii) specific clauses to be chosen depending on the role of the parties to the processing operation (modular approach).*

▪ *Adopting SCCs implies accepting them without making any change to their content, except for editorial changes or changes caused by the choice of the available modules.*

▪ *Before using the SCCs, an assessment of the local regulations of the third country should be carried out.*

▪ *The SCCs require the data exporter to take into account the law applicable to the data importer in order to determine whether the SCCs will be able to have full effect and to offer sufficient protection.*

▪ *The assessment must determine whether the legislation of the country of destination allows access to the data by public authorities under conditions that offer protection equivalent to that in the EU. According to the EDPB* ***(3)****, if public authorities have access to the data, the protection will not be essentially equivalent when:*

- *access rules are not clear, precise and accessible;*
- *access is not strictly necessary and not limited with regard to the legitimate national security objectives pursued;*
- *there is no independent oversight mechanism;*
- *there are no effective remedies available to data subjects.*

▪ *The assessment must be carried out on a case-by-case basis, taking into account various things such as the number of stakeholders, channels, onward transfers, types of recipients, purposes, nature of the data, economic sector, location of data storage.*

(1) Data Protection Act, art. 123

(2) Annex to the Commission implementing decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679, 4-6-2021

(3) Recommendations 02/2020 on the European Essential Guarantees for surveillance measures, 10-11-2020

- *If the assessment reveals that the level of protection is not essentially equivalent, the data exporter must implement, in addition to the SCCs, supplementary measures, with effective control of these measures (in particular through audits).*
- *Such measures may include technical and/or contractual measures.*
- *The difficulty is that few additional measures or safeguards have been recognised as effective, in particular by the EDPB.*
- *In some cases, the EDPB has even considered that no effective supplementary measures could be identified yet. This is the case, for example, for cloud solutions which require access to data in the clear* ***(4)****.*
- *In France, the position of the national supervisory authority, the CNIL, is aligned with that of the EDPB: it has not yet issued a public decision on this issue.*
- *However, it should be noted that regarding American tools used for higher education and research, the CNIL pointed out that a transitional period should exist while alternative solutions to these tools are sought* ***(5)****.*
- *The biggest companies (including AWS, Google, Microsoft) have already announced that they have taken supplementary measures and safeguards and modified their DPA (Data Protection Agreement) by making them more explicit.*
- *It remains to be seen whether, following an investigation or a complaint, the CNIL will consider that these measures are sufficient for data flows to the United States and allow the use of SCCs or BCRs.*

(4) Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, version 2.0, 18-6-2021

(5) La CNIL appelle à des évolutions dans l'utilisation des outils collaboratifs états-uniens pour l'enseignement supérieur et la recherche, 27-5-2021

CÉLINE AVIGNON

france
@lexing.network

Emmanuelle Ragot

Les transferts internationaux de données

Après le Brexit

▪ Le 28 juin 2021, la Commission européenne a adopté deux décisions d'adéquation **(1)** par lesquelles elle constate que le Royaume-Uni assure un niveau de protection adéquat des données à caractère personnel, d'une part, pour les transferts au titre du règlement général sur la protection des données (RGPD) et, d'autre part, pour les transferts dans le domaine répressif au titre de la directive « Police-Justice ».

▪ Ainsi, le régime de protection des données personnelles du Royaume-Uni est considéré offrir des garanties « substantiellement équivalentes » à celles offertes par l'Union européenne. Autrement dit, les transferts de données à caractère personnel depuis l'UE vers le Royaume-Uni peuvent donc être effectués comme s'il s'agissait d'un transfert vers un pays de l'Espace économique européen (EEE).

(1) Décision d'exécution de la Commission du 28.6.2021 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le Royaume-Uni
Décision d'exécution de la Commission du 28.6.2021 constatant, conformément à la directive (UE) 2016/680 du Parlement européen et du Conseil, le caractère adéquat du niveau de protection des données à caractère personnel assuré par le Royaume-Uni

Après l'arrêt de la Cour de justice de l'Union européenne (CJUE) du 16 juillet 2020 (Schrems II) – Feuille de route pour les exportateurs de données

▪ Dans son arrêt Schrems II, la CJUE a invalidé la décision 2016/1250 relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis (« Privacy Shield »), faute d'offrir un niveau de protection substantiellement équivalent à celui garanti par le RGPD et la Charte des droits fondamentaux de l'UE **(2)**.

(2) Affaire C-311/18 Data Protection Commissioner c. Facebook Ireland Limited et Maximillian Schrems

▪ Par conséquent, les entreprises de l'Union européenne ne peuvent désormais plus transférer légalement des données vers les États-Unis sur le fondement du Privacy Shield, devenu invalide. A défaut, elles risquent une amende pouvant s'élever jusqu'à de 20 millions d'euros ou 4 % de leur chiffre d'affaires mondial.

▪ Dans ce même arrêt Schrems II, la CJUE a également déclaré que les transferts reposant sur les clauses contractuelles types (CCT) restaient, en principe, valables sous réserve que l'exportateur et l'importateur de données vérifient, avant tout transfert, le niveau de protection assuré par le pays tiers, compte tenu de toutes les circonstances de ce transfert.

▪ En cas d'incapacité de se conformer aux obligations lui incombant au titre des CCT et, le cas échéant, à toute mesure supplémentaire à celles offertes par ces clauses, l'importateur de données est tenu d'en informer l'exportateur de données, à charge alors pour ce dernier de suspendre le transfert de données et/ou de résilier le contrat avec l'importateur de données.

▪ Le 10 novembre 2020, le Comité européen de la protection des données (CEPD) a publié des 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. Ces recommandations présentent aux exportateurs de données une série d'étapes à suivre, des sources d'information

potentielles et quelques exemples de mesures supplémentaires qui pourraient être mises en place. Le CEPD recommande ainsi aux exportateurs de prendre les actions suivantes :

- cartographier tous les transferts de données personnelles vers des pays tiers ;
- vérifier que le transfert est adéquat, pertinent et proportionné ;
- vérifier les instruments de transfert sur lesquels le transfert s'appuie (art. 45 /46 du RGPD), étant précisé que l'article 49 du RGPD ne peut être utilisé que dans certains cas de transferts occasionnels et non répétitifs ;
- évaluer si le droit ou la pratique du pays tiers sont susceptibles de porter atteinte à l'efficacité des garanties appropriées qu'offrent les instruments de transfert auxquels il est fait recours dans le cadre du transfert particulier ;
- identifier et adopter les mesures supplémentaires nécessaires pour que le niveau de protection des données transférées soit porté au niveau de la norme européenne d'équivalence essentielle ;
- prendre toutes les mesures procédurales formelles que l'adoption d'une mesure supplémentaire pourrait exiger, en fonction de l'instrument de transfert visé à l'article 46 du RGPD auquel il est fait recours ;
- réévaluer à intervalles appropriés le niveau de protection dont bénéficient les données transférées vers des pays tiers et vérifier s'il y a eu ou s'il y aura des développements susceptibles de l'affecter.

▪ Reste à savoir si l'autorité de contrôle du Luxembourg, la Commission Nationale pour la Protection des Données (« CNPD ») **(3)**, pourrait imposer une amende élevée à une entreprise en cas de violation des dispositions du RGPD sur les transferts internationaux de données. Alors qu'avant 2021, la CNPD était l'une des rares autorités à n'avoir infligé aucune amende pour violation du RGPD, sa décision **(4)** (frappée d'un appel) d'imposer à Amazon une amende de 746 millions d'euros pour violation du RGPD marque de toute évidence une nouvelle ère.

(3) Commission Nationale de la Protection des Données

(4) Décision de la CNPD du 16 juillet 2021

EMMANUELLE RAGOT

luxembourg@lexing.network

Emmanuelle Ragot

International data transfers

Post Brexit

▪ *Recently on 28 June 2021, the European Commission adopted two adequacy decisions **(1)** and found that the United Kingdom ensures an adequate level of protection for transfers of personal data, in accordance with the General Data Protection Regulation and the Law Enforcement Directive and with regards to national security.*

▪ *It means that the UK's personal data protection regime provides with safeguards that are "substantially equivalent" to those of the European Union and that transfers of personal data to the UK can be made as if it was a transfer with the European Economic Area (EEA).*

Post the Judgment from the European Court of Justice of European Union (CJEU) of July 16, 2020 (Schrems II) – Steps to follow by the Exporters

▪ *The CJEU has invalidated Decision 2016/1250 on the adequacy of the protection provided by the EU-US Privacy Shield for not ensuring a level of protection essentially equivalent to that guaranteed by the GDPR and the EU Charter of Fundamental rights **(2)**.*

▪ *The implications for commercial data transfers are that EU companies can no longer legally transfer data to the US based on the Privacy Shield framework, should they carry on to transfers data based on an invalid mechanism the companies risk a penalty of EUR 20 million or 4% of their global turnover.*

▪ *It has also ruled that the Standard Contractual Clauses (SCCs) transfer mechanisms remains, in principle, valid. However, the SCCs lay down an obligation on a data exporter and on the data importer to verify, prior any transfer and considering the circumstances of the transfer, whether that level of protection is respected in the third country.*

▪ *The data importer has also to inform the data exporter of any inability to comply with the CSSs, and where necessary with any supplementary measures to those offered by those clauses, the data exporter then being, in turn, obliged to suspend the transfer of data and / or to terminate the contract with the data importer.*

▪ *The European Data Protection Board on 10 November 2020 has issued a recommendation 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data. In a nutshell, the exporters have a series of steps to follow, potential sources of information and examples of supplementary measures that could be implemented:*

- *Mapping all transfers of personal data to third countries.*
- *Verifying that the transfer is adequate, relevant and proportionate.*

(1) Commission implementing decision of 28.06.2021 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom
Commission implementing decision of 28.06.2021 pursuant to Directive (EU) 2016/680 of the European Parliament and of the Council on the adequate protection of personal data by the United Kingdom

(2) Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited & Maximillian Schrems

- *Verifying the transfer tools the transfer is relying on (Art. 45 /46 GDPR). Art.49 GDPR may only be used in some cases of occasional and non-repetitive transfers.*
- *Assessing if there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of the specific transfer.*
- *Identify and adopt supplementary measures that are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence.*
- *Taking any formal procedural steps, the adoption of supplementary measure may require, depending on the Art. 46 GDPR transfer tool you are relying on;*
- *Re-evaluating at appropriate intervals the level of protection afforded to the data transferred to third countries and monitoring them to check whether there have been or there will be any developments that may affect.*

▪ *The question whether the National Commission for the Data Protection ("CNPD") **(3)** will impose or not a serious fine to a company in breach with GDPR's provisions on the international data transfers is not debatable anymore. If prior to 2021, the CNPD was one of the few authorities which had not imposed any fines relating to breaches of GDPR, the decision **(4)** (still under appeal) to hit Amazon with a EUR 746 million fine for GDPR violations is clear sign of a new era.*

(3) Commission Nationale de la Protection des Données

(4) Decision of 16 July 2021 CNPD

EMMANUELLE RAGOT

luxembourg@lexing.network

PAYS / COUNTRY	CABINET / FIRM	CONTACT	TELEPHONE	EMAIL
Afrique du Sud *South Africa*	Michalsons	John Giles	+27 (0) 21 300 1070	south-africa@lexing.network
Allemagne *Germany*	Beiten Burkhardt	Andreas Lober	+49 69 756095-0	germany@lexing.network
Australie *Australia*	Gadens	Dudley Kneller	+61 438 363 443	australia@lexing.network
Belgique *Belgium*	Lexing Belgium	Jean-François Henrotte	+32 4 229 20 10	belgium@lexing.network
Brésil	Montgomery & Associados	Neil Montgomery	+55 11 4096-4000	brazil@lexing.network
Canada *Canada*	Langlois avocats, S.E.N.C.R.L.	Pascal Archambault	+1 (418) 650 7000	canada@lexing.network
Chine *China*	Jade & Fountain PRC Lawyers	Jun Yang	+86 21 6235 1488	china@lexing.network
Côte d'Ivoire *Ivory Coast*	Imboua Kouao Tella & Associés	Annick Imboua-Niava	+ 225 22 44 74 00	ic@lexing.network
Espagne *Spain*	Lexing Spain	Marc Gallardo	+ 34 93 476 40 48	spain@lexing.network
États-Unis *USA*	Mulligan, Banham & Findley	Janice F. Mulligan	+1 619.238.8700	usa@lexing.network
France *France*	Alain Bensoussan-Avocats Lexing	Alain Bensoussan	+33 1 82 73 05 05	france@lexing.network
Grèce *Greece*	Ballas, Pelecanos & Associates L.P.C.	George A. Ballas	+ 30 210 36 25 943	greece@lexing.network
Guinée *Guinea*	BAO & Fils	Mody Oumar Barry	+ 224 623 68 78 79	guinea@lexing.network
Hongrie *Hungary*	OPL - Orbán & Perlaki	Miklos Orban	+36 1 244 8377	hungary@lexing.network
Inde *India*	Poovayya & Co	Siddhartha George	+91 80 4115 6777	india@lexing.network
Italie *Italy*	Studio Legale Zallone	Raffaele Zallone	+ 39 (0) 229 01 35 83	italy@lexing.network
Japon *Japan*	Hayabusa Asuka Law Office	Koki Tada	+81 3 3595 7070	japan@lexing.network
Liban *Lebanon*	Kouatly & Associates	Rayan Kouatly	+ 961 175 17 77	lebanon@lexing.network
Luxembourg *Luxembourg*	Emmanuelle Ragot Lawyers & Associates	Emmanuelle Ragot	+ 352 661 84 4250	luxembourg@lexing.network
Maroc *Morocco*	Elkhatib Lawfirm	Hatim Elkhatib	+212 5 39 94 05 25	morocco@lexing.network
Mexique *Mexico*	Carpio, Ochoa & Martínez Abogados	Enrique Ochoa De Gonzälez Argüelles	+ 52 55 25 91 1070	mexico@lexing.network
Norvège *Norway*	Advokatfirmaet Føyen Torkildsen AS	Øyvind Eidissen Ransedokken	+47 21 93 10 00	norway@lexing.network
Nouvelle-Calédonie *New Caledonia*	Cabinet Franck Royanez	Franck Royanez	+ 687 24 24 48	nc@lexing.network
République tchèque *Czech Republic*	Rowan Legal	Josef Donát Michal Nulíček	+420 224 216 212	czechrepublic@lexing.network
Royaume-Uni *United Kingdom*	Preiskel & Co LLP	Danny Preiskel	+ 44 (0) 20 7332 5640	uk@lexing.network
Sénégal *Senegal*	SCP Faye & Diallo	Mamadou Seye	:(+221) 33 823 60 60	senegal@lexing.network
Slovaquie *Slovakia*	Rowan Legal	Josef Donát Michal Nulíček	+420 224 216 212	slovakia@lexing.network
Suisse *Switzerland*	Sébastien Fanti	Sébastien Fanti	+ 41 (0) 27 322 15 15	switzerland@lexing.network

La JTIT est éditée par Alain Bensoussan Selas, société d'exercice libéral par actions simplifiée, 58 boulevard Gouvion-Saint-Cyr, 75017 Paris, président : Alain Bensoussan. Directeur de la publication : Alain Bensoussan – Responsable de la rédaction : Isabelle Pottier Diffusée uniquement par voie électronique – gratuit– ISSN 1634-0701
Abonnement à partir du site : https://www.alain-bensoussan.com/outils/abonnement-petit-dejeuner-debat/