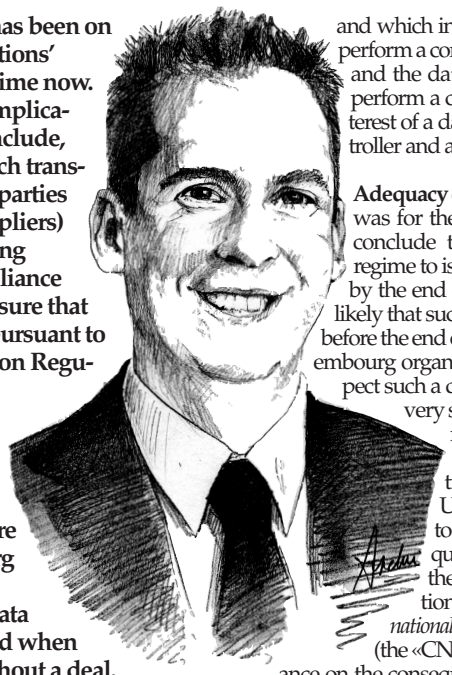
Personal data transfers to the UK:

Last weeks to prepare for an increasing likely «no-deal» Brexit



A «no-deal» Brexit has been on most EU organisations' agenda for some time now. The wide ranging legal implications of such a scenario include, for EU organisations which transfer personal data to third parties (e.g. group entities or suppliers) located in the UK, assessing whether additional compliance steps must be taken to ensure that such transfers are made pursuant to the General Data Protection Regulation (679/2016/UE) (the «GDPR»). As the end of the transition period is less than two months away and as negotiations for a future partnership are still ongoing, Luxembourg organisations should be ready to adopt the right data protection measures if and when the UK leaves the EU without a deal.

Up until now, organisations based in Luxembourg and in the UK could count on the free movement of personal data within the European Economic Area (the «EEA») to transfer personal data between them without having to comply with rules other than the general principles set out in the GDPR (such as ensuring that the transfer had a legal basis under Article 6 and that the data subjects were informed of the transfer or, as the case may be, consented to the transfer).

However, the transition period agreed upon between the UK and the EU, during which the GDPR continues to apply in the UK, is planned to end on 31 December 2020. Unless there is a breakthrough in the negotiations on a future partnership or a last-minute solution that is found between the UK and the EU before the end of the year, the UK will become a «third country» under the GDPR (i.e. a non-EEA country) as of 1st January 2021. In such a case, any EU-based organisation that sends personal data to third parties (entities, public bodies or associations, etc.) located in the UK (or allows personal data to be accessed by these third parties in the UK), will have to make sure that these data transfers comply with Chapter V of the GDPR. The latter in effect creates a number of so-called «transfer tools» by which personal data can be transferred to organisations located in non-EEA countries.

1. Which transfer tools are available for Luxembourg organisations that transfer personal data to the UK?

The most relevant transfer tools in the context of Brexit are:
- transfers made on the basis of an «adequacy decision» under Article 45 of the GDPR, whereby the European Commission, following an in-depth assessment of the country's legal system, adopts a formal decision that an adequate level of protection for personal data exists allowing personal data to flow freely to this country or, depending on the adequacy decision, to certain of its territories or sectors (e.g. Canada where the adequacy decision covers commercial organisations only);
- transfers that are subject to the «appropriate safeguards» listed in Article 46 of the GDPR and which include binding corporate rules (so-called «BCRs») and standard contractual clauses as adopted by the European Commission (so-called «SCCs»); and
- transfers that are subject to one of the «derogations for specific situations» listed in Article 49 of the GDPR and which include transfers necessary to perform a contract between the controller and the data subject or to conclude or perform a contract concluded in the interest of a data subject between the controller and a third party.

Adequacy decisions. Although the aim was for the European Commission to conclude the assessment of the UK regime to issue an «adequacy decision» by the end of 2020, it seems highly unlikely that such a decision will be adopted before the end of the transition period. Luxembourg organisations should thus not expect such a decision to be adopted in the very short term, which is unfortunate as this transfer tool would be the ideal choice to transfer personal data to the UK. Given the uncertainty as to whether and when the adequacy decision will be adopted, the Luxembourg data protection authority (the *commission nationale pour la protection des données*) (the «CNPD») makes clear in its guidance on the consequences of Brexit for international data transfers (available on the CNPD's website[1]) that concerned organisations should determine whether alternative transfer tools can be used.

Appropriate safeguards. Given the fact that concerned Luxembourg organisations need to find a swift transfer tool in case of a no-deal Brexit (thereby making BCRs less attractive), SCCs will be the preferred appropriate safeguards in most cases. In practice, these are template clauses to be concluded between the EU entity transferring the personal data and the «third country» entity (in this case the UK entity) receiving the personal data. These clauses need to be slightly adapted and their annexes completed to fit the contemplated transfer. SCCs can be incorporated into broader agreements between the parties (e.g. IT agreements).

Using SCCs requires a prior assessment as to the role of the entity transferring the data and the entity receiving the data under the GDPR (i.e. as controller or processor) to determine which set of SCCs must be concluded. In addition, as a result of the so-called *Schrems II* judgement of the Court of Justice of the European Union (the «CJEU») dated 16 July 2020 (C-311/18), using SCCs requires making a data transfer risk assessment to verify on a case-by-case basis if the law of the data recipient's country (i.e. UK law in case of a no-deal Brexit) ensures a level of protection of the personal data transferred that is essentially equivalent to that guaranteed in the EEA. If there is a risk that the level of protection would not be adequate, supplementary measures to protect the privacy of the transferred personal data should be put in place.

The European Data Protection Board (the «EDPB») very recently adopted recommendations on these supplementary measures (Recommendations 01/2020 dated 10 November 2020[2]). Supplementary measures may be contractual, organisational and/or technical depending on the specific data transfer and risks identified. Technical measures are recommended in cases where there is a risk in order to impede or render ineffective access by public authorities to personal data in third countries. These measures may include certain methods of pseudonymisation and encryption (at rest and in transit) of the data, which notably involve keeping the additional information allowing identification and the encryption keys in the EEA or in another country offering adequate protection[3].

Derogations for specific situations. Organisations can rely on any of the derogations that are exhaustively listed in Article 49 of the GDPR. However, the scope of these derogations is limited and several derogations will only apply to occasional and not repetitive data transfers. The CNPD in the aforementioned guidance underlines that these derogations are subject to a strict interpretation and that controllers should aim to implement appropriate safeguards as opposed to relying on derogations. This is in line with the recent EDPB recommendations on supplementary measures mentioned above which make clear that derogation should only be relied upon in exceptional cases.

2. What should Luxembourg organisations do in practice to prepare for a no-deal Brexit?

Given the uncertainty surrounding the outcome of the EU-UK negotiations and the need to ensure that a transfer tool covers data transfers to the UK if the UK suddenly becomes a third country on 1st January 2021, Luxembourg organisations that have not yet taken all steps to address these data transfer related issues should take the following actions.

Identify your personal data transfers to the UK. This is especially important in respect of those transfers that are key to the organisation's core activity or critical in terms of the number or sensitivity of data transferred. The organisation's record of data processing activities could help in identifying these transfers. Three elements must be taken into account when performing this exercise. First that the notion of «data transfer» not only includes transmission of personal data from a Luxembourg-based organisation to an organisation established in the UK, but also includes access by the UK entity to the Luxembourg-based organisation's personal data. Secondly, it makes no difference whether the transfer takes place between group entities or with external entities. Thirdly, personal data transfers may concern all sorts of data subjects such as employees, directors, shareholders/investors/customers who are individuals as well as individuals related to legal entities (e.g. contact persons or employees of institutional investors or suppliers).

Identify the role of the Luxembourg organisation transferring the data and the role of the UK organisation receiving the data under the GDPR. Reviewing any contract with the UK entity receiving the data (especially its data protection terms) would help in this respect. This exercise will allow the Luxembourg organisation to determine which party should be taking the required compliance steps (controllers being ultimately responsible for ensuring that a transfer tool is in place). It will also allow organisations relying on SCCs to determine which set of clauses must be concluded. Currently, two sets of SCCs exist to cover transfers from controllers to controllers and transfers from controllers to processors. On 12 November, the European Commission published a draft version of updated SCCs[4] which would also cover transfers from processors to processors and certain transfers from processors to controllers. Luxembourg organisations acting as processors and transferring personal data to UK entities acting as sub-processors should be careful that their agreements with controllers will still allow such transfers in case the UK becomes a third country (and for instance do not prohibit personal data outside the EEA). In case these agreements will no longer allow transfers to the UK, contractual adjustments must be made (e.g. by way of an amendment agreement).

Assess whether a derogation under Article 49 applies and, if so, document that the conditions for the derogation to apply are met. Since it is likely that an adequacy decision from the European Commission in respect of the UK will ultimately be adopted (and thus serve as a transfer tool for all transfers to the UK), Luxembourg organisations could in the meantime assess whether they can invoke a derogation to justify certain (and not all) personal data transfers to the UK. This transfer tool should however be used in limited cases where it is clear that all the conditions to rely on an Article 49 derogation, which are described in detail in the EDPB Guidelines on derogations of Article 49 (2/2018), are met in respect of a particular transfer or set of transfers. Documenting that the conditions are met will be key in ensuring that the Luxembourg organisation acting as controller complies with its accountability obligation under the GDPR. In practice, the most relevant derogations will often be those of paragraphs (a), (b) and (c) of Article 49, the derogation consisting in obtaining the data subjects' consent leading to practical difficulties in relation to many data transfers.

Assess whether SCCs can be used and, if so, prepare their conclusion. Most personal data transfers, especially those taking place on a regular or non-occasional basis, will likely require implementing appropriate safeguards for the data transfer to continue, often in the form of SCCs. As mentioned above, this will require carrying out a data transfer risk assessment. Such assessment must take into account the «EU Essential Guarantees» as outlined in the (very recent) EDPB Recommendations 02/2020[5], which also provide a brief list of possible sources of information to assess foreign protections. This entails a legal analysis to determine the impact of UK laws (and particularly its surveillance laws) on the specific data transfers. The assessment will in any event be less complex and less time-consuming than any assessment made in respect of data transfers to the US (and other non-EEA countries) given the fact that the UK has been a member of the EU. In parallel to this assessment, organisations should choose the right set of SCCs for its transfers (bearing in mind that the updated SCCs recently published by the European Commission are not yet final), start adapting the SCCs' appendices to cover the transfers at stake and determine whether the SCCs should be incorporated into an existing agreement.

Conclusion

Luxembourg organisations transferring personal data to the UK are facing a high degree of uncertainty in relation to the compliance of their transfers with the GDPR. These organisations should monitor the EU-UK negotiations on a future partnership closely and regularly, as it still possible that a solution is found whereby a transfer tool would not be necessary for data transfers to the UK. Simultaneously, however, Luxembourg organisations should take the steps described above to prepare for a no-deal Brexit scenario as there is currently no sign that there will be grace period in such event. We can of course assist you in relation to these, especially if Brexit-related data transfer issues have not been on your radar (which is understandable considering what 2020 has been like!).

Vincent WELLENS,
Avocat à la Cour (picture) (Luxembourg) / Avocat (Bruxelles)
IP & Tech Law partner, NautaDutilh
vincent.wellens@nautadutilh.com

Lindsay KORYTKO, Avocat à la Cour (Luxembourg)
IP & Tech Law senior associate, NautaDutilh
lindsay.korytko@nautadutilh.com

1) https://cnpd.public.lu/en/dossiers-thematiques/transferts-internationaux-donnees-personnelles/brexit1.html
2) https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf
3) Please see our newsflash for a detailed analysis of the EDPB's recommendations on supplementary measures: https://www.nautadutilh.com/en/information-centre/news/finally-some-practical-edpb-guidance-on-how-to-make-international-data-transfers-lawful
4) https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries
5) https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

Les employés luxembourgeois souhaitent plus de flexibilité au télétravail en 2021

Une nouvelle enquête intitulée «Workforce of the Future» indique que les salariés luxembourgeois souhaiteraient continuer à télétravailler partiellement à l'avenir. Ce rapport mené par Cisco a été réalisé auprès de 10.000 employés européens dans 12 pays, dont le Luxembourg.

A l'avenir, les interrogés verraient leur nouveau mode de travail avec plus d'autonomie (61%), plus de collaboration avec les collègues à distance (65%) et des décisions prises plus rapidement qu'auparavant (64%). Les résultats de l'enquête montrent que les travailleurs européens perçoivent l'année 2020 comme un tournant majeur dans la culture du travail. Si seulement 5% des employés interrogés travaillaient déjà principalement à domicile avant le confinement, une grande majorité d'entre eux préférerait garder l'autonomie qu'ils ont acquise depuis. Neuf Luxembourgeois sur dix (91%) désireraient décider eux-mêmes de leurs heures de travail ou de leurs jours de présence en entreprise.

Vers une forme de travail plus hybride

A la lumière des six derniers mois, les deux tiers des interrogés (66%) évaluent désormais mieux les avantages et les défis liés au télétravail. Pendant le confinement, ils ont ressenti plus de confiance de la part de leurs supérieurs hiérarchiques (51%). Ils ont pu mieux concilier leur vie professionnelle et privée : 65% d'entre eux ont pratiqué davantage d'activités sportives en-dehors du travail. Afin de gagner en productivité et efficacité, 61% des employés souhaiteraient moins de trajets à l'avenir.

Selon Arnaud Spirlet, General Manager de Cisco BeLux, un vrai déclic sur le télétravail s'est produit cette année : «L'idée reçue de l'employé moins productif de chez lui est dépassée. Le confinement a prouvé qu'il est possible d'être plus efficace à domicile. Ces nouveaux aménagements du travail auront un impact positif sur la mobilité, sur les frais des entreprises ou sur les espaces de travail, entre autres.

Au fur et à mesure que le télétravail gagnera en importance, les entreprises seront amenées à ajuster leurs stratégies. Elles devront faire des choix en matière de ressources humaines et informatiques, pour un travail d'équipe plus fluide et une cybersécurité complète.»

Plus d'investissements dans les technologies

S'ils étaient à la tête de leur entreprise, les employés luxembourgeois interrogés se concentreraient sur une bonne communication et la collaboration. Ils investiraient dans le matériel informatique et les logiciels pour faciliter le télétravail, en plus des protections sanitaires afin de retourner au bureau en toute sécurité. 3/4 d'entre eux (75%) estiment que les entreprises devraient fournir des technologies équivalentes à domicile et au bureau. Une majorité (54%) pense que le confinement a révélé qu'il n'est plus utile d'être dans la même pièce pour travailler ensemble efficacement. Les travailleurs de tous âges réclament également plus d'apprentissage : 77% pensent que plus de formations au numérique et de compétences informatiques seront essentielles pour l'avenir des entreprises.