The end of national data localisation obligations within the EU

The Regulation (EU) 2018/1807 on free flow of non-personal data (FFD Regulation) in the EU is about to put into question the national rules on data localisation. Its aim is to boost the data economy and the development of emerging technologies. Its consequence will be a drastic limitation of the EU Member States legislators and regulators' room to establish new national data localisation obligations within the EU.

Purpose

The EU legislator observed that data localisation policies within the EU have led to "*a lack of competition between cloud service providers, to various vendor lock-in issues and to a serious lack of data mobility*". In order to fight against this phenomenon, the FFD Regulation aims to open the data market within the EU, for the private sector as well as for the public authorities and bodies.

It is even expected from the latter that they "*lead by example by taking up data processing services and that they refrain from making data localisation restrictions when they make use of data processing services*". This will not be an easy task as public authorities traditionally prefer a storage of their datasets in their own country for sovereignty reasons.

Non personal data

The FFD Regulation targets "non" personal data, i.e. data that do not fall under the definition of personal data under the GDPR. Such "non" personal data are for instance "*aggregate and anonymised datasets used for big data analytics, data on precision farming that can help to monitor and optimise the use of pesticides and water, or data on maintenance needs for industrial machines*". Where non-personal data is inextricably linked to personal, the FFD Regulation shall not prejudice the application of the GDPR.

Yet, the GDPR underlines the same objective as the FFD Regulation, stating in its first article "*the free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data*". The impact of the distinction non-personal data vs. personal data within the context of the data localisation prohibition does therefore not seem to have much impact and both type of data seem thus by default to be encompassed in this FFD Regulation.

Prohibition of data localisation requirements

The core provision of the FFD Regulation is the prohibition of data localisation requirements, unless they are justified on grounds of public security in compliance with the principle of proportionality.

It must be noted that «data localisation requirements» is defined in rather broad fashion and encompasses «*any obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practices in a Member State and in bodies governed by public law*», which «*imposes the processing of data in the territory of a specific Member State or hinders the processing of data in any other Member State*».

Especially, the exact extent of the notion of «hindering» the processing of data in another EU Member State may be difficult to grasp. The said prohibition seems to cover only legal or administrative provisions and/or practices that impose some burden to process data in another EU Member State. Processing obligations that prima facie apply irrespective the place of processing could nevertheless come within the scope of this prohibition to the extent that such obligations would indirectly affect more the processing of data abroad. However, in our opinion it still will be possible for EU Member States to positively define a framework that does not impose any localisation obligations but which does confer some extra rights to companies and organisations when storing or otherwise processing data on their territory.

As from 28 May 2019, national legislators and regulators will be prohibited to adopt new data localisation requirements unless they are justified on grounds of public security in compliance with the proportionality principle. In the event a national legislator intends to insert a new national data localisation requirement or modify an existing one, it shall immediately inform thereof the European Commission.

EU Members States have until 30 May 2021 to repeal the current national data localisation requirements, unless they can justify to the Commission that it has to remain in force on grounds of public security. In the event the Commission disagrees with the justification, it may recommend the amendment or the repeal of the measure.

EU Member States will have to make national data localisation obligations publicly available via a national online single information point. This tool will most probably be very useful to enable service providers to target more easily a sector or another in other EU Member States.

Availability of data to competent authorities

The FFD Regulation specifies that it shall not affect the powers of competent authorities to request, or obtain, access to data for the performance of their official duties. Access to data by competent authorities may not be refused on the basis that the data are processed in another EU Member State. For example, if tax related documents of a company that is based in country A, are stored in country B, the authorities of country A still are entitled to have access to these data.

Where, after requesting access to data, a competent authority does not obtain access and if no specific cooperation mechanism exists under EU law or international agreements to exchange data between competent authorities of different EU Member States, that competent authority may request assistance from a competent authority in another EU Member State in accordance with the new cooperation mechanism that the FFD Regulation has introduced.

This new mechanism allows a competent authority in an EU Member State to request assistance via a single point of contact in the other relevant EU Member State in order to obtain access to data. The relevant competent authority so requested has a margin of appreciation of the request. In the event it does not consider that the conditions for requesting assistance have been met, it may reject the request.

This facilitated availability for authorities with respect to data that are processed in another EU Member State will exist alongside with other similar initiatives such as the future EU e-evidence framework. This framework (which includes the draft Regulation on European Production and Preservation Orders for electronic evidence in criminal matters) would *inter alia* create a EU order allowing a judicial authority in one EU Member State to obtain electronic evidence directly from an electronic communication, information society or internet domain name and IP numbering service provider in another EU Member State in criminal matters.

A challenge (for the financial sector) and an opportunity for Luxembourg

It goes without saying that the FFD Regulation is a challenge for the regulation of Luxembourg financial sector, which traditionally subjected the processing of client related data abroad to rather strict conditions. In a preliminary study assessing the need for rules on the free flow of data in the EU, Circular CSSF 12/552 on central administration, internal governance and risk management for credit institutions, investment firms and professionals performing lending operations was identified to contain data localisation requirements. Point 201 of this circular provided that «*where the processing centre is abroad, no confidential data which enables the identification of a customer of the institution can be stored therein, unless it is encrypted and provided that the decryption can only be carried out within the institution or a support PFS* [and thus only in Luxembourg] *within the context of its service provision or if all customers of the institution fulfil the conditions of express and informed consent*». The CSSF has anticipated the FFD Regulation in 2017 and has abolished this encryption requirement and the corresponding obligation to carry out the decryption in Luxembourg.

It must be noted, however, that despite this amendment, there is still the obligation of professional secrecy in the financial sector (also commonly called: the banking secrecy). This obligation, in principle, prohibits outsourcing activities that would lead to the storage of readable customer related data by entities that are not regulated in Luxembourg. In February 2018 an explicit «outsourcing» exception to the banking secrecy has been introduced, which makes it possible for Luxembourg financial institutions to outsource to non-regulated entities or entities abroad on the condition that the clients of the institution have agreed thereto.

One of the key questions will be how these rules must be assessed under the FFD Regulation. On the one hand, it is a fact that the consent requirement for outsourcing in the financial sector does not exist in most EU Member States. Even when the requirement of consent applies both to processing of data in Luxembourg or abroad, it is expected to have more impact on outsourcing activities and the processing of data abroad. Therefore, under a very broad interpretation of the FFD Regulation, the consent requirement could be considered to hinder the storage of customer related data abroad. On the other hand, it must be recalled that the consent requirement is a measure that has been taken in order to enable the processing and storage of data abroad, which was not possible before with that degree of legal certainty. Therefore, according to a more realistic interpretation of the FFD Regulation, the consent requirement for outsourcing activities in the financial sector does not necessarily conflict with this regulation. On the contrary, it is in line with the rationale of the FFD Regulation by opening up the banking secrecy in order to facilitate operations which require a processing or storage of data abroad.

Now this being said, the prohibition of data localisation requirements under the FFD Regulation will also lead to data localisation restrictions in the other EU Member States, which may also be an opportunity for Luxembourg to attract important datasets for storage and to confirm its status as a country of choice in this respect.

The Grand Duchy counts many data centres on its territory, several offering Tier4 performances, and has developed a real *savoir faire* in this area. The security of the data in the Grand Duchy has for instance been recently highlighted by the choice of several countries (Estonia) or organisations (the European Commission and the European Patent Office) to store their data in Luxembourg. But also from a legal perspective, Luxembourg offers several important advantages for the hosting of data on its territory. Indeed, it is one of the only countries in the world that explicitly confers a right to data holders to claim back their data from bankrupt data hosting and storage service providers.

The FFD Regulation will thus force national legislators and regulators to perform a "cleaning" exercise and to adopt a more European approach in terms of data hosting. This exercise will be an opportunity for the Grand Duchy to export more easily its hosting services and develop this - already growing - sector.

Vincent WELLENS (picture), Avocat à la Cour
Partner NautaDutilh Avocats Luxembourg S.à r.l.
vincent.wellens@nautadutilh.com

Anne-Sophie MORVAN, Avocate à la Cour (Luxembourg & Paris)
Senior Associate NautaDutilh Avocats Luxembourg S.à r.l.
annesophie.morvan@nautadutilh.com

POST Luxembourg se positionne au niveau européen dans le déploiement de la 5G

Etabli conjointement par le ministère de l'Économie et par le ministère du Développement durable et des Infrastructures en collaboration avec leurs homologues français et allemands, un site expérimental pour la conduite autonome et connectée sera mis en place entre le Luxembourg, l'Allemagne et la France. Le site traduit la volonté commune des 3 pays de promouvoir le développement et l'expérimentation de différentes technologies dans un contexte réel et transfrontalier.

POST Luxembourg vient d'être sélectionné par la Commission européenne dans le cadre du projet de recherche européen 5GCroCo (5G Cross-Border Control) pour fournir la couverture 5G de la section luxembourgeoise du tronçon d'autoroute reliant Metz, Merzig et le Grand-Duché en vue de réaliser des tests grandeur nature de la technologie 5G appliquée aux besoins de la conduite autonome et connectée. Impliquant plusieurs grands acteurs européens du secteur automobile et des communications mobiles, le projet portera sur trois cas d'étude concrets: la conduite à distance, la génération et la diffusion en temps réel de cartes en haute définition ainsi que l'évitement anticipé de collisions. Les premiers tests sont prévus en 2019.

Doté d'un budget de 17 millions d'euros, dont 13 millions seront financés directement par la Commission européenne, le projet 5GCroCo regroupe au total 24 partenaires européens originaires de 6 pays de l'UE. Le projet repose sur la technologie 5G pour assurer la connectivité numérique qui permet la communication transfrontalière entre les véhicules automatisés, les infrastructures et les autres usagers de la route.

Les réseaux de télécommunication ultra-réactifs 5G constitueront une infrastructure clé de la société numérique au cours des années à venir, en particulier pour développer la conduite autonome et connectée préconisée à la fois dans l'étude stratégique de la troisième révolution industrielle dite Rifkin et dans de la stratégie du gouvernement en matière d'introduction de la 5G au Luxembourg.

LIST et SnT impliqués dans des projets pilotes paneuropéens pour le déploiement de la 5G

À côté de POST Luxembourg, d'autres acteurs luxembourgeois participent à des projets pilotes paneuropéens dans le cadre du pré-déploiement et de l'introduction de la technologie 5G dans l'Union européenne en contribuant à la recherche, à l'essai et à la validation de solutions techniques ou réglementaires dans un contexte de conduite autonome et connectée transfrontalière. Ainsi, le Luxembourg Institute of Science and Technology (LIST) est impliqué dans la stratégie européenne de 5G en tant que responsable de la gestion globale de la qualité du projet 5G-MOBIX (5G for cooperative & connected automated MOBility on X-border corridors) qui est coordonné par l'association européenne pour les systèmes de transport intelligents (ERTICO). Le LIST interviendra également sur les aspects réseau et simulation routière, notamment en étudiant l'impact de la topologie routière sur la connectivité des réseaux afin de formuler des recommandations sur les stratégies de déploiement et de positionnement des antennes. Ceci permet aux opérateurs de télécommunications de fournir un meilleur service à moindre coût.

Le LIST participe en outre à l'évaluation des impacts économiques et sociaux des technologies et modèles économiques testés dans les corridors transfrontaliers afin de renforcer l'économie luxembourgeoise et d'améliorer la qualité de vie par l'innovation technologique. En outre, l'Interdisciplinary Centre for Security, Reliability and Trust (SnT) de l'Université du Luxembourg est chargé dans le cadre du projet 5G-MOBIX de promouvoir la recherche sur la mobilité coopérative, connectée et automatisée ainsi que les résultats qui en découlent afin d'accroitre l'impact du projet dans l'UE, la Chine, la Corée et au-delà.

Le Centre soutient les accords de coopération avec la communauté internationale de la 5G et les projets similaires. En outre, le SnT participe aux activités de normalisation en formulant des recommandations et en participant aux discussions sur l'attribution des fréquences pour les véhicules autonomes, connectés et coopératifs. Le SnT est également impliqué dans l'évaluation de l'impact commercial et sociétal des résultats du projet et des applications démontrées dans les corridors transfrontaliers 5G européens et les sites d'essais.

Dans le cadre du projet 5G-DRIVE, le SnT est responsable des activités portant sur l'évaluation et la vérification des vulnérabilités des communications véhiculaires dans le contexte de la conduite connectée. Afin de sécuriser la mobilité connectée, le Centre est également en charge de la recherche sur les aspects de sécurité de la 5G et de l'Internet des véhicules, notamment en explorant des techniques basées sur la technologie blockchain. Le SnT participera aux efforts de standardisation de la 5G et de l'Internet des objets (IoT) afin de faciliter une adoption à grande échelle de ces technologies, et donnera plus particulièrement des recommandations pour la coopération entre l'UE et la Chine.

Source : ministère de l'Économie