EMPEA

Legal & Regulatory Bulletin

27

CONTENTS

Issue No. 27 | 2019

Personal Data Flows from the European Union

By Dr. Thomas Schürrle, Partner, Christopher Garrett, Associate, and Friedrich Popp, Associate at Debevoise & Plimpton LLP

Cross-border information flows in a globally connected world are essential to conducting international business. Personal information is in the European Union protected by a fundamental right to data protection under the General Data Protection Regulation (GDPR) and supplementing EU Member State laws. This article explains the legal framework for personal data transfers from the Union, in particular if the data protection level in the recipient country is below the European standards, and provides an assessment of some of the practical issues for global businesses.

I. The European Data Protection Concept

Appreciating the issues involved in relation to cross-border personal data flows requires an understanding of the overall GDPR framework. In May 2018 the GDPR replaced the various harmonized, but still fragmented data protection regimes in the EU Member States with law that is, in essence, uniform across the Union.[1] In particular, the Regulation abolished in the field of data transfers a myriad of Member State peculiarities that were considered an unnecessary obstacle for economic activities across the borders.

The new law applies to the processing of personal information of individuals, known as data subjects in the terminology of the GDPR, in the EU without regard to citizenship. Personal information is any information identifying an individual and may include the name, birth date, health status, bank account details, online identifiers such as IP address etc. Processing is any use of data, including the collection, storage or, as will be discussed below, the transfer of personal information.

The GDPR imposes duties on data controllers, the persons who determine the means and purposes of data processing, and data processors, who process the personal data on behalf of the controller. For example, controllers and processors must maintain written records of processing activities that also describe the envisaged transfers of personal data to countries not covered by the GDPR.

The GDPR applies to controllers and processors established in the EU or in Iceland, Liechtenstein and Norway (known collectively as the European Economic Area, EEA), even if the actual processing for the establishment occurs outside this area, as long as the processing is taking place in the context of the EEA establishment. It further applies to businesses established outside the EU that target individuals in the Union with the offering of goods or services, or monitor their behavior, e.g. via online tracking.

Several principles like lawfulness, fairness and transparency govern the data processing. For example, the data subject must be informed, generally in a privacy notice, about the details of a transfer, including its legal basis. The amount of data processed should be minimized to what is necessary in relation to the processing purpose. Re-use of data for a reason which is incompatible with the initial processing purpose is prohibited. A controller is under a general duty to demonstrate data protection compliance vis-à-vis the authorities.

The data subject has several data protection rights, including a right to information and access to verify the lawful use of its data, or the right to erasure ("right to be forgotten"). It can enforce its rights by bringing a complaint before an independent supervisory authority. It can also bring

1. See for an introduction to the GDPR: Friedrich Popp. "EU General Data Protection Regulation: A primer for funds and portfolio companies", available at https://www.empea.org/app/uploads/2018/12/LRB_Fall_2018_Debevoise.pdf

a claim to material and non-material damages against the controller or the processor before a home court in the Union. Criminal courts punish the most severe violations of the GDPR.

The supervisory authorities can use their investigative, corrective, and advisory powers when monitoring the application of the Regulation and can order, e.g., the suspension of data flows to non-EEA countries. They can also issue administrative fines, in the extreme, to EUR20 million. or 4% of the annual group turnover, in case of any violation of the GDPR that may amount.

Representatives of the European supervisory authorities convene in the European Data Protection Board (formerly known as the Article 29 Working Party), a body tasked to ensure the consistent application of the Regulation across the Union, in particular by issuing of guidelines. The European Court of Justice (CJEU) has the final say on the interpretation of the GDPR.

II. Data Transfers to "Third Countries"

1. Data Transfer Risks

The GDPR concept of transfer is broad and does not necessarily involve a physical move of the information. Thus the rules apply also in case the data is merely made accessible elsewhere by, e.g., granting remote access to a database. The rules must be considered again in relation to any onward transfer of personal data, depending on how the personal data has been lawfully transferred initially.

A personal data transfer within the EEA raises no specific data protection concerns as both the transferor and the recipient are bound by the GDPR. The analysis may change if the recipient is located in a jurisdiction outside the EEA, (a "Third Country"), in particular if that country provides for a lower level of data protection.

EU based companies, or groups with an EU establishment within them, must fully understand their data flows in order to assess their need to comply with the GDPR requirements relating to data transfers and the most appropriate of the various options which may be available to them. The first step in the assessment is to ask whether the processing has a lawful basis under GDPR. As a second step it must be considered whether the recipient country either provides for adequate data protection (see 2. below) or the parties to the transfer contractually provide for enforceable data protection rights (see 3. below). If neither of the transfer instruments works, the transferor would need to rely on one of the specific GDPR exceptions (see 4. on page 23).

2. Adequacy-based Transfer

A data transfer to a Third Country does not require any specific authorization, or reliance on any other transfer mechanism or exception, if the EU Commission has determined that a Third Country, a territory, or a specified sector within the Third Country ensures an adequate level of protection. The Commission reviews its adequacy decisions regularly, in particular if criteria like rule of law, relevant legislation or enforcement no longer ensure an essentially equivalent status.

The EU issued so far adequacy decisions with respect to Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay, and the EU-US Privacy Shield framework. In the beginning of 2019, the EU and Japan complemented their recent trade agreement with a reciprocal adequacy decision, recognizing each other's data protection systems as adequate and permitting personal data to be transferred safely between the EU and Japan, what is considered to be the greatest area of GDPR-compliant data flows.

In relation to the US, the 2016 EU-US Privacy Shield permits unhindered data transfers to (currently) approx. 4,500 US companies that self-certify adherence to the framework. The validity of the Shield mechanism is challenged since 2016 before the CJEU for alleged excessive access of US national security agencies to transferred EU data.

The EU Commission plans the next adequacy decisions for South-Korea, India, and possibly also for the United Kingdom once it left the Union.

3. Transfer Secured by Adequate Safeguards

If the transfer is to be made to a Third Country which does not benefit from an adequacy decision, a controller or processor may transfer personal data if it secures the transfer with suitable safeguards that provide for enforceable data subject rights and effective legal remedies.

Currently, most data transfers to Third Countries rely on standard data protection clauses (the "SCCs"), adopted by the European Commission. Both the transferor and the recipient of data contractually commit to comply with European data protection standards and to grant data subjects enforceable rights. If left unamended, the clauses provide for a relatively simple transfer mechanism and it is this simplicity which has led to them being widely used. Different versions are used dependent on whether the recipient of the data transfer is a data controller or a data processor.

The situation changes if the parties to the transfer seek to amend the clauses or individually negotiate for clauses as these require prior supervisory authority approval in an EU-wide procedure. In 2018 the Irish High Court referred a number of questions relating to the adequacy resulting from SCCs to the CJEU and there is a risk that the court invalidates this transfer mechanism. Whilst entering into the SCCs is straightforward, supervisory authorities will expect to see the terms of the SCCs complied with and enforced between the parties, even if within the same corporate group.

In 2018 Equifax Limited was fined GBP500,000 by the UK Information Commissioner's Office for breaches which included failing to exercise its right under SCCs to audit its parent company and data processor, Equifax Inc., or carry out adequate checks to ensure that it complied with the relevant security requirements.

Further, corporate groups should ensure that they are able to comply with the provisions of the SCCs relating to onward transfers before concluding that SCCs are the best option for their international data flows.

The GDPR treats intra-group data transfers between EU and non-EU members of a multinational group like any other Third Country data transfer, unless the group members enter into Binding Corporate Rules, BCRs, authorized by supervisory authorities. BCRs contain privacy principles, such as transparency, data quality, security, tools of effectiveness (e.g., audit, training, or complaint handling systems) and an element proving that the rules are binding. It is important, therefore, for global groups to identify the flows of data precisely, to ensure that all recipients of the data are signed up to an appropriate agreement.

While SCCs and BCRs already existed under prior data protection laws, there is only limited experience to date with new GDPR data transfer mechanisms in form of approved codes of conducts or certification mechanisms.

4. Exceptions-based Transfer

If a transfer can be based neither on an adequacy decision nor on appropriate safeguards, it can be made on the basis of specific exceptions set out in the GDPR. These exceptions include, amongst others,

- where an individual has explicitly consented to the proposed transfer after having been provided with all necessary information about the risks associated with the transfer;
- where the transfer is necessary for the performance or the conclusion of a contract between the individual and the controller or the contract is concluded in the interest of the individual;
- if the data transfer is necessary for the establishment, exercise or defense of legal claims; or
- if the data transfer is necessary for the purposes of compelling legitimate interests of the organization.

Supervisory authorities take the view that these exceptions must be interpreted restrictively and applied only on an occasional, non-repetitive basis as the data subjects no longer enjoy enforceable and effective data protection rights once the data have left the territorial scope of the GDPR. Consent is considered a weak basis for data transfers as it must be fully informed, freely given and may also be withdrawn any time. The remaining exceptions require the data exporter to demonstrate that the transfer of certain personal data is actually necessary to achieve the purpose of the transfer.

Notably absent from the list of exceptions is where the transfer is necessary to comply with a foreign legal obligation. Organizations which are subject to both the GDPR and foreign legal obligations to transfer or disclose personal data to third parties outside the EEA need to consider the circumstances carefully in order to conclude whether a transfer is permitted under GDPR, which will not always be the case even if the requirements of the relevant foreign law specifically require it.

III. Summary

The GDPR has led to unprecedented awareness of business and individuals of data protection issues, including the transfer of data to non-EEA countries. European supervisory authorities have already started to check the practices of businesses operating in the EU and the now uniform data transfer rules allow the authorities to adopt a consistent application across the EU. Upcoming CJEU rulings on the Privacy Shield and the SCCs will add to legal certainty for businesses but may provide some challenges.

Compliance with the requirements relating to transfers to Third Countries does not just happen behind the scenes. The data subject must be informed in privacy notices about the transfer and, if relevant, asked for explicit informed consent. The records of processing activities which every controller must maintain must identify the recipient country and document the adequate contractual safeguards, unless the transfer can be based on an adequacy decision or, as a last resort, on an exception. If the transferor cannot demonstrate GDPR compliance in accordance with the accountability principle, supervisory authorities may impose administrative fines or order the suspension of data flows. Needless to say, it is far too late to be considering these issues when a supervisory authority comes calling.

About the Authors

Thomas Schürrle is Partner at Debevoise & Plimpton LLP

Christopher Garrett is Associateat Debevoise & Plimpton LLP

Friedrich Popp is Associate at Debevoise & Plimpton LLP