GDPR Update: Transfer of Personal Data (outside the EEA)

November 22, 2017

Introduction

In this GDPR update, we will address the transfer of personal data outside the European Economic Area (EEA).

Similar as under the current Data Privacy Directive 95/46/EC (the Directive), the transfer of personal data outside the EEA remains restricted under the General Data Protection Regulation (the GDPR). However, the GDPR introduces several changes in this respect, including new derogations for the cross-border data transfers.

Adequate level of protection

As a general rule, the transfer of personal data to a country outside the EEA (generally referred to as a "third country") may only take place if that country ensures an adequate level of data protection.

The European Commission (the Commission) has the power to determine that a third country, a territory or a specified sector within that third country, or an international organisation ensures an adequate level of protection for data transfers. After the Commission has recognised a third country as providing an adequate level of protection, personal data can be transferred without any further protective measures or authorisation. The GDPR obliges the Commission to review its adequacy decisions at least every four years.

In determining whether a third country, territory or specified sector or an international organisation ensures an adequate level of protection, the Commission will take into account, inter alia:

i. the rule of law, respect for human rights and relevant legislation e.g. with regard to (the (onward) transfers of) personal data and the effective and enforceable data subject rights;
ii. the existence and effective functioning of one or more independent supervisory authorities, with authority and responsibility for ensuring and enforcing compliance with the data protection rules; and
iii. international commitments by the third country or international organisation, or other obligations arising from legally binding conventions or instruments in relation to the protection of personal data.

The existing adequacy decisions by (including notably the decision on the EU - US Privacy Shield), adopted by the Commission under the Directive, shall remain in force until amended, replaced or repealed by the Commission in accordance with the GDPR.

Transfer of personal data to third countries that do

not ensure an adequate level of protection

In the absence of an adequacy decision by the Commission, personal data may only be transferred to a third country if (i) the controller or processor provides appropriate safeguards, and (ii) enforceable data subject rights and effective legal remedies for data subjects are available.

These safeguards may be provided, without requiring any specific authorisation from a supervisory authority, by:

i. a legally binding and enforceable instrument between public authorities or bodies;
ii. Binding Corporate Rules;
iii. standard contractual clauses adopted by the Commission;
iv. standard contractual clauses adopted by the supervisory authority and approved by the Commission;
v. approved codes of conduct; and
vi. approved certification mechanisms.

Below, we will address the three safeguards that in practice are likely to be the most relevant.

Binding Corporate Rules

Binding Corporate Rules (BCRs) are internal rules adopted by a multinational group of undertakings which define its global policy with regard to the international transfers of personal data within the same corporate group to entities in countries which do not provide an adequate level of protection.

Under the GDPR, BCRs must:

1. be approved by the competent (lead) supervisory authority;
2. be legally binding and apply to and are enforced by every member concerned of the group of undertakings;
3. confer enforceable rights on data subjects with regard to the processing of their personal data; and
4. contain specific information on, inter alia: (a) the structure and contact details of the group; (b) the data transfers including the categories of personal data; (c) the type of processing and its purposes; (d) the type of data subjects affected; (e) the identification of the third countries in question; (f) the application of the general data protection principles; (g) the rights of the data subjects; (h) the acceptance of liability by the controller or processor established in the EU for any breaches of the BCRs by a group member not established in the EU; (i) the tasks of the data protection officer; and (j) the complaint procedures.

Standard contractual clauses adopted or approved by the Commission

The transfer of personal data to a third country that does not provide an adequate level of protection is also allowed if standard contractual clauses adopted by the Commission or by a supervisory authority (and approved by the Commission) are used.

The GDPR explicitly states that standard contractual clauses can be included in a wider agreement and parties are allowed to add other clauses or safeguards, provided that they do not contradict the standard contractual clauses or prejudice the data subjects' fundamental rights or freedoms.

Ad hoc contractual clauses may also be used, but these require supervisory authority approval prior to the cross-border transfer.

The Commission has currently issued three sets of standard contractual clauses: two sets for transfers from data controllers established in the EEA to data controllers established outside the EEA and one set for the transfer from data controllers established in the EEA to processors established outside the EEA. No standard contractual clauses exist for the cross-border transfer from processors established in the EEA to sub-processors established outside the

EEA.

The approved sets of standard contractual clauses remain valid, but the GDPR leaves open the possibility for these sets to be repealed (and replaced by a new set of standard contractual clauses).

Approved codes of conduct

Under the GDPR, the use of codes of conduct is encouraged to serve as a tool to demonstrate compliance with the GDPR. Codes of conduct may also serve as appropriate safeguards for the cross-border transfer of personal data.

Codes of conducts may be prepared by associations or other bodies representing controllers or processors and must be submitted to the supervisory authority for prior approval.

Adherence to an approved code of conduct combined with commitments by a controller or processor outside the EEA to apply the appropriate safeguards, can demonstrate that the controller or processor outside the EEA has implemented adequate safeguards.

Derogations for specific situations

The GDPR contains various derogations from the prohibition to transfer personal data outside the EEA without adequate protection. These derogations are largely similar to the derogations under the Directive. The derogations apply when:

1. the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards (i.e. it is insufficient to just mention that data will be transferred to a third country);
2. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
3. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party;
4. the transfer is necessary for important reasons of public interest;
5. the transfer is necessary for the establishment, exercise or defence of legal claims;
6. the transfer is necessary to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; and
7. the transfer is made from a register that, according to EU or member state law, is intended to provide information to the public and that is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions set out in Union or Member State law for consultation are fulfilled in the particular case.

Finally, if the transfer cannot be based on standard contractual clauses, BCRs or any of the other derogations set out above, the transfer may take place if:

1. it is not repetitive;
2. concerns only a limited number of data subjects;
3. is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests and freedoms of the data subjects;
4. the controller has assessed all circumstances and has provided suitable safeguards;
5. the controller informs the supervisory authority of the transfer.

This final derogation allows for some flexibility but also requires a careful assessment and proper documentation and should only be applied as an exception.

Practical recommendations

Failure to comply with the GDPRs' provisions on data transfers to third countries are subject to fines up to EUR 20,000,000 or 4% of the total worldwide annual turnover, whichever is higher. Therefore, organisations would do well to review and map (key) cross-border data flows and assess whether the current cross-border mechanisms continue to be appropriate.

In general we do not recommend relying on consent for your onward transfers of personal data. Data subjects can withdraw their consent at any time and if they do, you no longer have a valid basis for the transfer of personal data outside the EEA. As data storage becomes more and more cloud based and may be stored in various data centres across the world (which may not even be the same data centre every time), having to deal with withdrawal of consent may create a complex and time-consuming puzzle. Where possible, it is better to rely on other forms of safeguards, such as BCRs or model clauses, or to store data within the EEA and avoid onwards transfers.

Please click here to subscribe to our monthly updates on the GDPR.

Overview of subjects

January 2017	Territorial scope of the GDPR(Dutch)
February 2017	The Concept of Consent
March 2017	Sensitive Data
April 2017	Accountability, Privacy by Design and Privacy by Default
May 2017	Rights of Data Subjects (information notices)
June 2017	Rights of Data Subjects (access, rectification and portability)
July2017	Rights of Data Subjects (erasure, restriction, objectand automated individual decision-making)
August 2017	Data Processors
September 2017	Data Breaches and Notifications
October 2017	Data Protection Officers
November 2017	Transfer of Personal Data (outside the EEA)
December 2017	Regulators (competence, tasks and powers)
January 2018	One Stop Shop
February 2018	Sanctions
March 2018	Processing of Personal Data in Employment Context
April 2018	Profiling and Retail
May 2018	Overview

Your Key Contacts

Marc Elshof
Partner, Amsterdam
D +31 20 795 36 09
M +31 6 46 37 61 08

marc.elshof@dentons.com