Data Protection Law – Aspects of International Jurisdiction

Outline

§ 1 Introduction
§ 2 Applicable Law
§ 3 International Jurisdiction
§ 4 Concluding Remarks
§ 1  Introduction

A. The Globalization of Data Processing
   – Traditional situation
     • National markets
       – Distribution of products and services across borders relatively rare
         » Segregated markets
         » Services provided from abroad practically excluded
         » Only certain products from abroad
       – International distribution via sales partners or subsidiaries in the respective market
         » Sales partners or subsidiaries collected, processed and used the data
         » Subject to the respective national data protection law, if any

   – Paper based data collection and processing
     • Difficulties of transportation (costs – volume, weight, duration)
       » Collection of data from abroad cumbersome
       » Transfer of data to a foreign country cumbersome
     – Difficulties to handle too large volumes
   • Limited interest in processing and using data abroad
     – Markets not globalized
     – Linguistic barriers
     – Cultural differences
§ 1 Introduction

A. The Globalization of Data Processing
   – Today’s situation
     • Globalization of the markets for goods and services
       – Low barriers to distribution abroad
         » Few restrictions on importation and exportation
         » Low, if any, customs duties
         » Low costs of transportation
         » Provision of information services online
       – Higher demand for products and services from abroad
         » Easily available information influences demand and allows a comparison
         » Low, if any, additional costs
         » Communication per e-mail or online form

   – Electronic data collection and processing
     • No difficulties of transportation
       » Collection of data from abroad creates no major problems
       » Sending in a click
       » Place of storage irrelevant, direct use from abroad
     – No difficulties in handling large volumes
     • Interest in processing and using data from foreign countries
       – Globalized markets
       – Linguistic barriers less significant
       – Cultural differences decrease
§ 1 Introduction

B. International Situations
   - Transfer of data to foreign controllers, processors or other recipients
     • From a legal point of view, rather simple situation
       - Domestic controller very probably subject to
         » domestic law with its rules on the transfer of data
         » domestic Data Protection Agency
         » domestic courts
§ 1 Introduction

B. International Situations

– Transfer of data to foreign controllers, processors or other recipients

Art. 6 Swiss Federal Act on Data Protection (FADP). Cross-border disclosure

(1) Personal data may not be disclosed abroad if the privacy of the data subjects would be seriously endangered thereby, in particular due to the absence of legislation that guarantees adequate protection.

(2) In the absence of legislation that guarantees adequate protection, personal data may be disclosed abroad only if: …

(3) The Federal Data Protection and Information Commissioner (the Commissioner, Art. 26) must be informed of the safeguards under paragraph 2 letter a and the data protection rules under paragraph 2 letter g. The Federal Council regulates the details of this duty to provide information.

Art. 25 Directive 95/46/EC. Principles

(1) The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

(2) The adequacy of the level of protection afforded by a third country shall be assessed …

(3)-(5) …

(6) The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals. …

Art. 26 Directive 95/46/EC. Derogations

(1)-(4) …
§ 1 Introduction

B. International Situations
   – Transfer of data to foreign controllers, processors or other recipients

Art. 44 Regulation (EU) 2016/679. General principle for transfer
Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.

Art. 45 Regulation (EU) 2016/679. Transfers on the basis of an adequacy decision
(1)-(9) ...

Art. 46 Regulation (EU) 2016/679. Transfers subject to adequate safeguards
(1)-(5) ...

(1)-(3) ...

Art. 48 Regulation (EU) 2016/679. Transfers or disclosures not authorised by Union law
Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State, without prejudice to other grounds for transfer pursuant to this Chapter.

Art. 49 Regulation (EU) 2016/679. Derogations for specific situations
(1)-(6) ...

Art. 50 Regulation (EU) 2016/679. International cooperation for the protection of personal data
...
§ 1 Introduction

B. International Situations

– Transfer of data to foreign controllers, processors or other recipients
  • From a legal point of view, rather simple situation
    – Domestic controller probably subject to
      » domestic law with its rules on the transfer of data and
      » domestic Data Protection Agency (DPA)
    » domestic courts

CJEU. Judgment of 6 October 2015, Case C-362/14 – Maximilian Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650

“1. … a decision ..., such as Commission Decision 2000/520/EC ..., by which the European Commission finds that a third country ensures an adequate level of protection, does not prevent a supervisory authority of a Member State ... from examining the claim of a person concerning the protection of his rights and freedoms in regard to the processing of personal data relating to him which has been transferred from a Member State to that third country when that person contends that the law and practices in force in the third country do not ensure an adequate level of protection. 2. Decision 2000/520 is invalid.”
§ 1 Introduction

B. International Situations
   – Foreign controller or processor carries out domestic activity
     • From a legal point of view, more difficult situation
       – Question of whether, and if so, when, the foreign controller
         or processor is subject to
         » domestic law
         » domestic Data Protection Agency (DPA)
     • Normally, in the area of administrative law, the applicable law
       and the jurisdiction of the relevant administrative authorities go
       hand in hand
     • However, this is not necessarily the case in the area of data
       protection law

§ 2 Applicable Law

A. Possibilities
   – Location of the data
     • Problems
       – Location of server etc. seems to be irrelevant
       – Determination if data not already collected – location of data
         subject, place of entering the data, contents of the data?
     – Location of the data subject
       • Problems
         – Stable (nationality, residence) – what in case of travel?
         – Versatile (current place) – which moment shall be decisive?
     – Territory where data is collected and/or processed
       • Problems
         – Location of server etc. seems to be irrelevant
         – Place where user is sitting or where orders are carried out?
§ 2  Applicable Law

A. Possibilities
   – Territory where the controller or processor has its seat/headquarters
     • Problems
       – May result in low level of protection for nationals
       – Allows for forum shopping
       – Lack of predictability
       – Enforcement is difficult: Foreign DPA has low interest,
         domestic DPA would have to apply foreign law
   – Territory where the controller or processor has an establishment
     • Problems
       – Same problems as with seat/headquarters
       – What in case of more than one establishment?

   – Territory where the controller or processor uses equipment
     • Problems
       – Location of server etc. seems to be irrelevant
       – May reach too far
§ 2 Applicable Law

B. Solutions

– Frequently, there is no clear legal provision

• Either determination on a case by case basis using the possible connecting factors as arguments

• Or application of the principle of territoriality

Swiss Bundesgericht [Federal Court], Judgment of 31 May 2012, Case 1C_230/2011 – Google Inc. and Google (Switzerland) GmbH v. Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB [Federal Data Protection and Information Commissioner FDPIC] sub F.3.2:

“… The FADP contains no explicit provisions on its territorial scope of application. As Art. 29 FADP is a provision pertaining to the area of public law, the principle of territoriality applies. Thus, the provisions of the FADP apply to the processing of personal data in Switzerland which might violate the constitutional right to privacy (Art. 13 of the Federal Constitution) …”

§ 2 Applicable Law

B. Solutions

– EU law contains provisions on the applicable law

Art. 4 Directive 95/46/EC. National law applicable

(1) Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State’s territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

(2) …
§ 2 Applicable Law

B. Solutions
   - EU law contains provisions on the applicable law
     • Provisions of Directive 95/46/EC quite complicated

Source: Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law
§ 2 Applicable Law

B. Solutions

– EU law contains provisions on the applicable law

• Provisions of Directive 95/46/EC quite complicated

Source: Article 29 Data Protection Working Party, Opinion 8/2010 on applicable law

CJEU, Judgment of 13 May 2014, Case C-131/12 – Google Spain SL and Google Inc. v. AEPD, ECLI:EU:C:2014:317

“Article 4(1)(a) of Directive 95/46 is to be interpreted as meaning that processing of personal data is carried out in the context of the activities of an establishment of the controller on the territory of a Member State, within the meaning of that provision, when the operator of a search engine sets up in a Member State a branch or subsidiary which is intended to promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State.”
§ 2 Applicable Law

B. Solutions
- EU law contains provisions on the applicable law
  - Member States’ data protection law may provide for a higher level of protection than the Directive
  - Scope of application with respect to controllers or processors not established in the EU may be defined somewhat differently

CJEU, Judgment of 1 October 2015, Case C-230/14 – Weltimmo, ECLI:EU:C:2015:639
"1. Article 4(1)(a) of Directive 95/46/EC… must be interpreted as permitting the application of the law on the protection of personal data of a Member State other than the Member State in which the controller with respect to the processing of those data is registered, in so far as that controller exercises, through stable arrangements in the territory of that Member State, a real and effective activity — even a minimal one — in the context of which that processing is carried out. …"
§ 2 Applicable Law

B. Solutions

– EU law contains provisions on the applicable law

Art. 3 Regulation (EU) 2016/679. Territorial scope

(1) This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

(2) This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:
   (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
   (b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

(3) This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.
§ 2 Applicable Law

B. Solutions
   – EU law contains provisions on the applicable law

Recitals Regulation (EU) 2016/679
(22) Any processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union should be carried out in accordance with this Regulation, regardless of whether the processing itself takes place within the Union. Establishment implies the effective and real exercise of activity through stable arrangements. The legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect.

Recitals Regulation (EU) 2016/679
(23) ... In order to determine whether such a controller or processor is offering goods or services to data subjects who are in the Union, it should be ascertained whether it is apparent that the controller or processor envisages offering services to data subjects in one or more Member States in the Union. Whereas the mere accessibility of the controller’s, processor’s or an intermediary’s website in the Union, of an email address or of other contact details, or the use of a language generally used in the third country where the controller is established, is insufficient to ascertain such intention, factors such as the use of a language or a currency generally used in one or more Member States with the possibility of ordering goods and services in that other language, or the mentioning of customers or users who are in the Union, may make it apparent that the controller envisages offering goods or services to data subjects in the Union.
§ 2 Applicable Law

B. Solutions
   - EU law contains provisions on the applicable law

Recitals Regulation (EU) 2016/679
(24) The processing of personal data of data subjects who are in the Union by a
controller or processor not established in the Union should also be subject to this
Regulation when it is related to the monitoring of the behaviour of such data
subjects in so far as their behaviour takes place within the Union. In order to
determine whether a processing activity can be considered to monitor the
behaviour of data subjects, it should be ascertained whether natural persons are
tracked on the internet including potential subsequent use of personal data
processing techniques which consist of profiling a natural person, particularly in
order to take decisions concerning her or him or for analysing or predicting her or
his personal preferences, behaviours and attitudes.

Aspects of International Jurisdiction

§ 2 Applicable Law

B. Solutions
   - In case a controller or processor is sued by a data subject for
     violation of the data subject’s right to privacy, the determination of
     the applicable law is a question of private international law
     • In the EU, not governed by Regulation Rom II
     • In Member States, mostly no special rules, i.e., normal rules for
torts apply

Art. 40 German Introductory Act to the Civil Code. Tort
(1) Tort claims are governed by the law of the country in which the liable party has
acted. The injured party can demand that instead of this law, the law of the
country in which the injury occurred is to be applied. The option can be used only
in the first instance court until the conclusion of the pretrial hearing or until the
end of the written preliminary procedure.
(2)–(4) …

   • In Switzerland, Art. 139 of the Federal Act on Private
     International Law (FAPIL)
§ 2 Applicable Law

B. Solutions
- In case a controller or processor is sued by a data subject for violation of the data subject’s right to privacy, the determination of the applicable law is a question of private international law.

Art. 139 FAPIL. Violation of the right to privacy
(1) Claims based on a violation of the right to privacy by the media, especially by the press, the radio, television and by any other means of public information, are governed, at the victim’s own choice,
   a. by the law of the State in which the victim has her permanent residence, insofar as the offender would have had to expect that the result occurs in this State;
   b. by the Law of the State in which the offender has her establishment or permanent residence, or
   c. by the Law of the State in which the result of the violation occurs, insofar as the offender would have had to expect that the result occurs in this State.
(2) ...
(3) Paragraph 1 applies also to violations of the right to privacy which are the result of processing personal data as well as to obstructions of the exercise of the right to access personal data.

§ 3 International Jurisdiction

A. Possibilities
- Location of the data
  • Problems
    - Location of server etc. seems to be irrelevant
    - Determination if data not already collected – location of data subject, place of entering the data, contents of the data?
  - Location of the data subject
    • Problems
      - Stable (nationality, residence) – what in case of travel?
      - Versatile (current place) – which moment shall be decisive?
  - Territory where data is collected and/or processed
    • Problems
      - Location of server etc. seems to be irrelevant
      - Place where user is sitting or where orders are carried out?
§ 3 International Jurisdiction

A. Possibilities

– Territory where the controller or processor has its seat/headquarters
  • Problems
    – May result in low level of protection for nationals
    – Allows for forum shopping
    – Lack of predictability
    – Enforcement is difficult: Foreign DPA has low interest, domestic DPA would have to apply foreign law

– Territory where the controller or processor has an establishment
  • Problems
    – Same problems as with seat/headquarters
    – What in case of more than one establishment?

– Territory where the controller or processor uses equipment
  • Problems
    – Location of server etc. seems to be irrelevant
    – May reach too far
§ 3 International Jurisdiction

B. Solutions

– Frequently, there is no clear legal provision
  • Determination on a case by case basis using the possible connecting factors as arguments
  • Jurisdiction always given if domestic law is applicable
  • Application of the principle of territoriality

Swiss Bundesgericht [Federal Court], Judgment of 31 May 2012, Case 1C_230/2011 – Google Inc. and Google (Switzerland) GmbH v. Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB [Federal Data Protection and Information Commissioner FDPIC] sub F.3.2:

“... The FADP contains no explicit provisions on its territorial scope of application. As Art. 29 FADP is a provision pertaining to the area of public law, the principle of territoriality applies. Thus, the provisions of the FADP apply to the processing of personal data in Switzerland which might violate the constitutional right to privacy (Art. 13 of the Federal Constitution). ...

3.3 The pictures used in Street View are taken in Switzerland, contain information about persons, streets and squares in Switzerland and are so published that they can be accessed from Switzerland. Thus, there is a preponderant connecting factor to Switzerland. That the pictures are processed abroad and are not uploaded to the internet from Switzerland does not alter the fact that a potential violation of the right to privacy occurs via pictures taken in Switzerland. The evaluation of such measures is part of the tasks of the FDIPC (Art. 29 FADP). Thus the lower instance court was right in affirming the jurisdiction of the FDIPC in the present case. ...
§ 3 International Jurisdiction

B. Solutions
– EU law contains some provisions on jurisdiction of DPA

Art. 28 Directive 95/46/EC. Supervisory authority
(1)-(2) …
(3) Each authority shall in particular be endowed with:
- investigative powers, such as …
- effective powers of intervention, such as …
- the power to engage in legal proceedings …
(4)-(5) …
(6) Each supervisory authority is competent, whatever the national law applicable to the processing in question, to exercise, on the territory of its own Member State, the powers conferred on it in accordance with paragraph 3.
Each authority may be requested to exercise its powers by an authority of another Member State. The supervisory authorities shall cooperate with one another to the extent necessary for the performance of their duties, in particular by exchanging all useful information.

Art. 55 Regulation (EU) 2016/679. Competence
(1) Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State.
(2) Where processing is carried out by public authorities or private bodies acting on the basis of point (c) or (e) of Article 6(1), the supervisory authority of the Member State concerned shall be competent. In such cases Article 56 does not apply.
(3) Supervisory authorities shall not be competent to supervise processing operations of courts acting in their judicial capacity.
§ 3 International Jurisdiction

B. Solutions

– EU law contains some provisions on jurisdiction of DPA

Art. 56 Regulation (EU) 2016/679. Competence of the lead supervisory authority

(1) Without prejudice to Article 55, the supervisory authority of the main
establishment or of the single establishment of the controller or processor shall
be competent to act as lead supervisory authority for the cross-border processing
carried out by that controller or processor in accordance with the procedure
provided in Article 60.

(2) By derogation from paragraph 1, each supervisory authority shall be competent
to handle a complaint lodged with it or a possible infringement of this Regulation,
if the subject matter relates only to an establishment in its Member State or
substantially affects data subjects only in its Member State.

(3)-(5) …

(6) The lead supervisory authority shall be the sole interlocutor of the controller or
processor for the cross-border processing carried out by that controller or
processor.

– Both Directive and new Regulation: Territoriality
– New Regulation
  – “One-stop-shop” approach for controllers or processors with
an establishment in the EU
  – Not possible for controllers or processors without an
establishment in the EU
  » Every national DPA has jurisdiction for its territory
  » However, uniform legal provisions of the Regulation
  apply
§ 3 International Jurisdiction

B. Solutions

– Jurisdiction of courts
  • Typically, no special rules
  • Disputes about measures taken by a DPA
    – Courts of the country of the respective DPA have jurisdiction
    – Within the EU, national courts may ask the CJEU for a preliminary ruling

– Disputes between a data subject and a controller/processor (cease and desist, damages)
  • General rules apply; civil matter; general jurisdiction and tort jurisdiction
  • If defendant has a domicile in the European Union, the Brussels I bis Regulation applies
    EU courts may ask the CJEU for a preliminary ruling (on the jurisdictional rules of the Brussels I bis Regulation or European Data Protection Law)
  • If defendant has a domicile in a Contracting State of the Lugano Convention, this convention applies
§ 4 Concluding Remarks

– Today, data protection is an international topic
– Substantive law across countries is very different
– As a consequence, in international settings, the determination of the applicable law and international jurisdiction of Data Protection Agencies and courts are as important as substantive rules
– Still, many questions are unresolved
– A harmonization of the rules on the applicable law and international jurisdiction appears to be desirable