Data Privacy Event

Trends in Enforcement of Data Protection Law in Europe

13 February 2014, Brussels
Agenda

► Trends on Enforcement of Data Protection Law in Europe
► Current non alignment among EU Member States
► Recent trends of selected European Data Protection Authorities (DPAs)
► Spanish DPA’s (AEPD) decision against Google Inc
► Proposed new European Regulation
## Remedies, Liability and Sanctions

<table>
<thead>
<tr>
<th>Remedies</th>
<th>Liability</th>
</tr>
</thead>
<tbody>
<tr>
<td>► Judicial remedies before national courts</td>
<td>► Compensation for suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to the Directive</td>
</tr>
<tr>
<td>► Judicial remedies before ECJ</td>
<td></td>
</tr>
<tr>
<td>► Administrative remedies before National Data Protection Authorities (DPAs)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Sanctions</th>
<th>Sanctions</th>
</tr>
</thead>
<tbody>
<tr>
<td>► Warning</td>
<td>► Fines (pecuniary sanction, monetary penalty)</td>
</tr>
<tr>
<td>► Public warning</td>
<td></td>
</tr>
<tr>
<td>► Measures for remedy</td>
<td></td>
</tr>
<tr>
<td>► Nullity of transaction</td>
<td></td>
</tr>
<tr>
<td>► Prohibition to use personal data or database</td>
<td></td>
</tr>
<tr>
<td>► Destruction of data or database</td>
<td></td>
</tr>
</tbody>
</table>
Non-alignment among EU Member States

- Necessary means to perform duties:
  - Powers of investigation
  - Intervention
- Each Member State shall provide that one or more public authorities are responsible for monitoring the application within its territory of the provisions adopted by the Member States pursuant to this Directive, Art. 28 (1)
- The authorities shall act with complete independence in exercising the functions entrusted to them, Art. 28 (2)
- Each Member State independently implemented the Directive to enforce local data protection regulations
  - National legislations on Data Protection vary within EU
Non-alignment among EU Member States (contd)

<table>
<thead>
<tr>
<th></th>
<th>France</th>
<th>Germany</th>
<th>Italy</th>
<th>Spain</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandatory registration of personal data file with DPA</td>
<td>Yes</td>
<td>No</td>
<td>For limited cases</td>
<td>Yes</td>
</tr>
<tr>
<td>Data Protection Officer in companies</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Inspection by hearing upon summons</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Emergency procedure</td>
<td>Yes</td>
<td>Yes</td>
<td>For Telcos</td>
<td>No</td>
</tr>
<tr>
<td>Financial penalties</td>
<td>Max. €300,000</td>
<td>Max. €300,000</td>
<td>Max. €1,44m</td>
<td>Max. €600,000</td>
</tr>
<tr>
<td>Criminal sanctions</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
## Enforcement Cases (2012)

<table>
<thead>
<tr>
<th>Country</th>
<th>Agency</th>
<th>Violations notified</th>
<th>Sanctions issued</th>
<th>Criminal violation notified to prosecutors</th>
<th>Audits completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>France</td>
<td>CNIL</td>
<td>65</td>
<td>19</td>
<td></td>
<td>385</td>
</tr>
<tr>
<td>Italy</td>
<td>Garante privacy</td>
<td>578</td>
<td>118</td>
<td>58</td>
<td>395</td>
</tr>
<tr>
<td>Spain</td>
<td>AGPD</td>
<td>896</td>
<td>557</td>
<td></td>
<td>306</td>
</tr>
</tbody>
</table>
## Enforcement Cases (2010-12)

### Italy, Garante privacy

<table>
<thead>
<tr>
<th>Year</th>
<th>Total sanctions (€/m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>4,0</td>
</tr>
<tr>
<td>2011</td>
<td>3,0</td>
</tr>
<tr>
<td>2012</td>
<td>3,8</td>
</tr>
</tbody>
</table>

### Spain, AGPD

<table>
<thead>
<tr>
<th>Year</th>
<th>Total sanctions (€/m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>17,5</td>
</tr>
<tr>
<td>2011</td>
<td>19,6</td>
</tr>
<tr>
<td>2012</td>
<td>21,1</td>
</tr>
</tbody>
</table>

### France, CNIL (2012)

- 5 Sanctions: 1x €100,000, 1x€50,000, 1x €20,000, 2x €10,000
- 10 Warnings
- 1 Warning + emergency procedure
- 2 Dismissals
European DPAs vs. Google Inc.
Dec 19, 2013 AEPD Director’s Decision
Milestones of the Investigation Procedure

- **Jan 24, 2012:** Google Inc. announced that it was going to put in place a New Privacy Policy (NPP) in substitution of its former 70 polices, applicable to all its services and products.

- **Feb 2, 2012:** The European Data Protection Authorities (WP29) requested Google Inc. to postpone the NPP’s entry into force date after having started to analyze the NPP. Google however took the decision not to postpone. Therefore, WP29 decided to carry out a coordinated analysis of the NPP, led by CNIL.

- **March 1, 2012:** NPP came into force, after a new petition requesting its postponement.

- **October 2012:** WP29 and 27 European DPAs sent a letter to Google. They identified several NPP’s provisions that were in violation of the European Data Protection Legislation.

- **February 26, 2013:** After having confirmed that Google had not put in place the WP29’s recommendations, the WP29 and 27 European DPAs decided to initiate national investigation against Google Inc.

- **April 2, 2013:** An investigation procedure was opened by the AEPD.

- **Dec 19, 2013:** AEPD Director’s Administrative Decision was issued, imposing €900,000 penalty to Google Inc.\(^1\)

Note: (1) The aim of this presentation is only to describe the content of the AEPD Director’s Administrative Decision issued on December 19th, 2013. It is not our intention to evaluate or give any positive or negative opinion in relation to its grounds or the opposing arguments submitted by Google.
The Spanish Data Protection Law is applicable to the Personal Data Processing carried out by Google Inc. (a non-European Resident Entity).

When the processing is carried out in Spanish territory as part of the activities of an establishment belonging to the person responsible for the processing.

(Article 2.1 Spanish Data Protection Act (SDPA) and Article 4 of the European Directive 95/46/CE (Directive))

- The activities developed by Google Inc. in Spain are mainly supported by publicity incomes (inserted in its services). Without publicity, Google Inc. is unable to render the services.
- The main activity of Google Spain, S.L., a Spanish resident entity, is to reach publicity agreements with local companies. Therefore, without the activities carried out by the local establishment (Google Spain), Google Inc. can not render the services and the data processing.

When the person responsible for the processing is not established on the territory of the European Union and is using for the processing some means located in Spanish territory.

(Article 2.1 SPPA and Article 4 Directive)

- When the services are not supported by publicity, Google Inc. uses for the processing MEANS, situated in the local territory. Google Inc. use “Cookies” to store data within the users’ computer equipment, located in Spain. (Document WP 56, dated May, 30, 2002).
AEPD Director’s Decision
Preliminary Aspects (contd)

Google collects Personal Data and processes them.

- AEPD said that Google collects data from:
  - Registered Users.
  - Non Registered Users who use Google’s services.
  - Non Registered Users who use other third parties web pages which use Google services (Translators, Google Analytics, etc.).

- Google and AEPD agreed that the data collected from registered user are personal data (name, email, phone number, credit card data, etc.)

- AEPD said that such data collected by Google in relation to the computer equipment, IP address, localization data, cookies, etc… are also personal data, because (i) Google may use reasonable means to identify and connect the data with a person (it is not necessary to know the name of the person); (ii) cookies must be considered as personal data, etc.

- Google said that such data collected from a non registered user who uses its services are not personal data because it can not identify the person.
AEPD Director’s Decision
Data Protection Infractions

Quality of Data

According to Article 4.1 SDPA and Consideration 28 Directive:
► The data to be collected and processed must be adequate, relevant and not excessive in relation to the purpose for which they are processed. Consequently, it is forbidden to collect and process data that is not necessary to the purpose that justified the processing.
► The purposes must be explicit and legitimate and must be determined at the time of collection of the data. It is forbidden to collect and process data for future purposes or unknown by the data subject, at the time of collection.

According to Google NPP: Google collects data in order to provide, maintain and improve the services, to develop new ones, to protect the services and users, to offer personalized content and advertising to the users.

AEPD opinion:
► Purposes, such as ‘improvement of the service’ or ‘the offering of personalized advertising’ are too broadly defined to offer an appropriate framework to judge the legitimacy of the purpose. (WP 148. 04/04/2008)
► The purposes indicated in the NPP are indefinite, generic and not clear. The data to be collected is not connected with a purpose. The data subjects can not know the ground that justified the collection and the processing of their data and how Google is going to use them.
► The data subject believes that the collected data is going to be processing only in relation to the service that he/she is using, but not in relation to other Google services. (Google understands all its services and products as a one service. AEPD understands that it is not one services but several ones).
AEPD Director’s Decision
Data Protection Infractions (contd)

Quality of Data (contd)

According to Article 4.1 SDPA and Consideration 28 Directive:
► The purposes of processing shall not be incompatible with the purposes as they were originally specified. It is forbidden to collect and process data for future purposes or unknown by the data subject, at the time of collection.
► The data only may be processed for the purpose indicated at the time of its collection.

According to Google NPP: Google may use unlimitedly the collected data among all its services.

AEPD opinion:
► Google may combine the collected personal data among all its services, but not only from those collected from the registered user, but also from those who are not registered, even though when they are not using a Google service. (By means of Cookies).
► Google justified the aforementioned unlimited combination and the use of them for future services. The company wants to be entitled to use the collected data when Google wishes and for the purpose that Google wishes.
AEPD Director’s Decision
Data Protection Infractions (contd)

Right of information in the collection of data
According to Article 5 SDPA and Article 10 Directive:

► Data subjects whose personal data is requested must be previously informed explicitly, precisely and unequivocally of the following:
  a) **The existence of a file** or personal data processing operation, the purpose of collecting the data, and the recipients of the information.
  b) The obligatory or voluntary nature of the reply to the questions put to them.
  c) The consequences of obtaining the data or of refusing to provide them.
  d) The possibility of exercising rights of access, rectification, erasure and objection.
  e) The identity and address of the controller or of his representative, if any.

► Where the controller is not established in the territory of the European Union, and the controller is using for the processing means situated in Spanish territory, he must, unless these means are being used for transit purposes, designate a representative in Spain, without prejudice to any action which may be taken against the controller himself.

AEPD opinion:

► Google does not inform about the existence of a file. The Company informed about the existence of processing, but in undefined way.
► The purposes indicated in the NPP are indefinite, generic and not clear.
► Google is identified as a controller, but the NPP does not indicate its address. Google Inc. does not designate a representative in Spain.
► Google does not inform clearly to the data subject if the data to be collected is obligatory or voluntary.
► Google collects and processes personal data which its owner is unaware of.
Consent of the data subject.

According to Article 6,1 SDPA:

► Processing of personal data shall require the unambiguous consent of the data subject, unless laid down otherwise by law.

AEPD opinion:

► The lack of information commented above, particularly, the lack of information about the purposes does not justify to assume that the data subjects has given his/her consent.
► Google collects and processes personal data whose subjects are unaware. So they have not given any consent.
► Google said that the consent is not necessary because the registered user and users of its services have entered into an agreement with Google.
► AEPD disagrees with this ground. In a few cases, the users have to enter into a contract. There is no global contacts between the user and all the services provided by Google. The user does not enter into a contract as a consequence of the use of the services or for accepting the terms and conditions.
AEPD Director’s Decision
Data Protection Infractions (contd)

Obligation to erase those data not necessary for the purpose

According to Article 4,5 SDPA:

► Personal data shall be erased when it has ceased to be necessary or relevant for the purpose for which it was obtained or recorded.
► Data shall not be kept in a form which permits identification of the data subject for longer than necessary for the purposes for which it was obtained or recorded.

According to Article 4,5 SDPA:

► Rectification or cancellation shall apply to data whose processing is not in accordance with the provisions of this Law and, in particular, when such data is incorrect or incomplete.

AEPD opinion:

► Google maintains the personal data for an undefined term. Only in some cases the NPP set a term to maintain the data, but Google does not justify the reason for this term or period.
► If a user requests the cancellation of its data, Google says that it must reject the petition for security reasons.

Right of access, rectification, cancellation and objection (Article 15 and 16 SPDA)

AEPD opinion:

► The procedure stated that the NPP is very difficult for users.
► There is not a unique method to exercise the rights, but several. The user must use all of the methods stated by Google if he wishes to exercise his rights.
► The NPP states that Google may reject the petition for security reasons and in circumstances where Google has to use disproportionate means to rectify, cancel or give access to the data.
Proposed new European Regulation
Proposed new European Regulation

► Chapter 8 of the EU draft regulation
  ► The supervisory authority shall act with complete independence
  ► Investigation powers
  ► Power to issue administrative sanctions (up to 5% of annual worldwide turnover or €100 million fine)
  ► Mitigations in case of European Data Protection Seal
  ► Applies not only to concrete privacy violations but also in case of lack of privacy organization and documentation
  ► Right of the individual to lodge a complaint with a supervisory authority
  ► Right of the individual to a judicial remedy against a supervisory authority
  ► Right of the individual to a judicial remedy against a controller or processor
  ► The supervisory authority of the main establishment of the controller shall be competent for activities in all Member States
Art. 77 of the EU draft regulation

Right to compensation and liability

1. Any person who has suffered damage, including non-pecuniary damage, as a result of an unlawful processing operation or of an action incompatible with this Regulation shall have the right to claim compensation from the controller or the processor for the damage suffered.

2. Where more than one controller or processor is involved in the processing, each of those controllers or processors shall be jointly and severally liable for the entire amount of the damage, unless they have an appropriate written agreement determining the responsibilities pursuant to Article 24.
Proposed new European Regulation (contd)

► Art. 79 of the EU draft regulation
  ► 2a. To anyone who does not comply with the obligations laid down in this Regulation, the supervisory authority shall impose at least one of the following sanctions:
    a) a **warning** in writing in cases of first and non-intentional non-compliance
    b) **regular periodic** data protection **audits**
    c) a **fine** up to 100 m EUR or up to 5% of the annual worldwide turnover in case of an enterprise, whichever is greater

► Sanctions should be fixed in each individual case **proportionate** to the specific situation, with due regard in particular to the **nature**, **gravity** and **duration** of the **breach**
Questions?
Thank you

José Dominguez Leandro, abogado, EY Spain
Luigi Neirotti, avvocato, EY Italy