EU Data Protection Reform:
what researchers should know

Jacob Kornbeck
19 September 2014
European Research Council Workshop
"Research Data Management and Sharing"
Brussels

Opinions expressed are personal

Strategy
2013-2014
The EDPS

The independent DPA for EU institutions / bodies:

- Supervise processing of personal information
- Advise on policies and legislation
- Cooperate with national DPAs, for consistency
- Appear before the EU courts
- Follow developments in new technology
- Raise awareness of data protection
## Timeline of developments

<table>
<thead>
<tr>
<th>Year</th>
<th>DP legislation</th>
<th>IT developments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1970</td>
<td>Hessen</td>
<td>Arpanet has 13 nodes</td>
</tr>
<tr>
<td>1974</td>
<td>US Privacy Act</td>
<td>Name “Internet”</td>
</tr>
<tr>
<td>1978</td>
<td>FR law, CNIL</td>
<td>1st spam email</td>
</tr>
<tr>
<td>1980</td>
<td>OECD Guidelines</td>
<td>Usenet (now Google groups)</td>
</tr>
<tr>
<td>1981</td>
<td>Convention 108</td>
<td>IBM PC</td>
</tr>
<tr>
<td>1990</td>
<td>UK Computer Misuse Act</td>
<td>www (December 25)</td>
</tr>
<tr>
<td>1995</td>
<td>Directive 95/46/EC</td>
<td>Amazon.com</td>
</tr>
</tbody>
</table>
# Timeline of developments

<table>
<thead>
<tr>
<th>Year</th>
<th>DP legislation</th>
<th>IT developments</th>
</tr>
</thead>
<tbody>
<tr>
<td>2000</td>
<td><strong>EU Charter Arts 7 &amp; 8</strong></td>
<td>Wikipedia (January 15, 2001)</td>
</tr>
<tr>
<td>2001</td>
<td><strong>Regulation 45/2001</strong></td>
<td>iPod (November 10)</td>
</tr>
<tr>
<td>2004</td>
<td>EDPS Decision</td>
<td>FaceBook</td>
</tr>
<tr>
<td>2006</td>
<td><strong>Data Retention Directive</strong></td>
<td>Twitter, iPhone (2007)</td>
</tr>
<tr>
<td>2009</td>
<td><strong>TFEU Art 16, TEU Art 6(1)</strong></td>
<td>iPad (April 3 2010)</td>
</tr>
<tr>
<td>2012</td>
<td>Com proposes DP reform</td>
<td>Google Glass testing</td>
</tr>
<tr>
<td>2013-14</td>
<td>Negotiations in EP and Council</td>
<td>Snowden - NSA</td>
</tr>
</tbody>
</table>
Challenges to Privacy
(2) EU Law on Privacy: two different fundamental rights

(a) the Right of Privacy

ECHR (1950), Article 8
Everyone has the right to respect for his or her private and family life, home and correspondence

EU Charter (2000), Article 7:
...and communications.
(b) the Right to Protection of Personal Data

an autonomous fundamental right to self-determination in the Information Society

EU Charter, Article 8

Article 16, EU Treaty:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.
Basic principles
(the rules of the road)

Scope and Jurisdiction

Obligations (controllers):
Fair and lawful processing, information, security and confidentiality, sensitive data, security, international transfers.

Rights (data subjects) transparency and control:
Access, rectification, blocking, erasure, objection

Enforcement
– Independent supervisory authority
– Judicial remedies, damages
Directive 95/46/EC: scope

- Personal data: any information relating to an identified or identifiable person
- Processing wholly or partly by automatic means; and manual processing of personal data which form part of a filing system
- Processing which falls within the scope of EC law and is not a purely personal or household activity
- Article 4(2) TEU: national security excluded
Definition of personal data

- any information: objective - subjective
- relating to: content – purpose – result
- identified or identifiable: can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to physical, physiological, mental, economic, cultural or social identity
- natural person: living individuals
- Cf anonymous/pseudonymous/encrypted WP 136, Opinion 4/2007 on the concept of personal data
Examples of personal data

CVs, diplomas, recommendation letters, criminal records, medical certificates

Students databases with all their administrative and evaluation related data held by their university

Medical data and health related data

Genetic data

Customer data held by telephone company, telephone calls and voice mails

Information held by email account provider

Transport data, body scanners in airports

Photos, video-surveillance
[2] fair processing: law, necessity and proportionality

ECHR, Article 8(2):
• In accordance with the law
• Necessary in a democratic society

EU Charter, Article 52(1)
• provided for by law
• proportionate and necessary for objectives of general interest or to protect the rights and freedoms of others
(3) The Data Protection Reform Package

Public consultation (May-Dec 2009)


Commission proposals - 25/1/12:

• “**General**” **Data Protection Regulation** *(COM(2012) 11 final)*

• **Directive for police and criminal justice authorities** *(COM(2012) 10 final)*
(1) main drivers of the Reform

- **Technological development**: more effective protection needed
- **Globalisation**: more consistency needed within EU and internationally
- **Lisbon Treaty**: a new legal base for horizontal EU-wide data protection law

Parallel Reform processes

- Modernisation of Convention 108
- Review of OECD Guidelines
The Snowden effect
Objectives of the Reform

• Continuity, build on existing framework: underlying principles still valid
• Make controllers more accountable
• Strengthen data subjects’ rights
• Improve harmonisation (Regulation) and consistency of approach by DPAs
• Strengthen supervision & enforcement
• Substantially increase the level of data protection in law enforcement
State of play

• Albrecht report: January 2013
• 4000+ amendments
• Council partial common position: June 2013
• LIBE vote: 21 October 2013
• European Council: 25 October 2013
• EP Plenary, 12 March 2014
(2) stronger obligations
> principle of accountability

- data controllers already legally responsible for compliance with DP rules
- but notification plus liability not enough
- controllers have to be proactive, design /adopt /implement concrete measures *in advance*
- The most effective way to protect personal data in the information society
- Complements/animates all controller obligations
- Scaleable, flexible, DPA control
Accountability

(Arts 5(f) and 22.1)
controller must ensure and demonstrate compliance
(ensure – demonstrate - verify)

• Huge shift: controllers responsible, not DPAs
• Non-exhaustive list of appropriate measures:
  specific requirements (*subject to threshold):
  ➢ *documentation (Art 28)
  ➢ implementing security requirements (Art 30)
  ➢ *performing an impact assessment (Art 33)
  ➢ prior authorisation/consultation (Art 34)
  ➢ *designating a DPO (Art 35.1)
  ➢ privacy by design / privacy by default
# (3) Stronger rights

<table>
<thead>
<tr>
<th>PRIVACY BY DEFAULT</th>
<th>PRACTICAL APPLICABILITY</th>
<th>FORESEEN PROBLEMS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DEFINITION</strong></td>
<td>By default processing by the SNS and sharing should be in the most limitative option</td>
<td>Goes against the business model of the SNS</td>
</tr>
<tr>
<td>Unless the user explicitly opts for a reduction in privacy safeguards, the most limitative option should be taken by default</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>RIGHT TO BE FORGOTTEN</strong></td>
<td>Account and “own” content should be deleted completely when a user closes his/her account or at the request for closing Also the “profiling” done by the SN</td>
<td>What happens with the data uploaded about a data subject by other users acting or not as data controllers?</td>
</tr>
<tr>
<td>If a data subjects requests so, the controller must delete all personal data associated to that data subject in the system</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>PORTABILITY</strong></td>
<td>It should be possible to export all personal data stored in the system, both own content and profiling into a format that should be “readable” from one SNS to another</td>
<td>Goes against the business model of the Social Network The main value is the network connections and that cannot be exported unless there is interoperability among Social Networks</td>
</tr>
<tr>
<td>Users should be able to carry their personal data from one provider to another</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
the right to be forgotten

CNIL (FR) – reports a growing problem
• 2012 - 6,000 complaints overall
• more than 1,000 re. right to be forgotten
• increase in complaints by 42% in one year

Case C-131/12, Google v AEPD
• complaint against continued publication of 1998 newspaper auction notice for unpaid debts
• requested erasure by Google Spain, Google Inc and by newspaper
• AEPD made order against Google only, Google challenge in Audiencia Nacional referred to CJEU
The reform: research, etc.

- "The processing of personal data for other purposes should be only allowed where the processing is compatible with those purposes for which the data have been initially collected, in particular where the processing is necessary for historical, statistical or scientific research purposes." (Recital 40)

- "Transfers which cannot be qualified as frequent or massive, could also be possible for the purposes of the legitimate interests pursued by the controller or the processor, when they have assessed all the circumstances surrounding the data transfer. For the purposes of processing for historical, statistical and scientific research purposes, the legitimate expectations of society for an increase of knowledge should be taken into consideration." (Recital 88)
The reform: research, etc.

- "The processing of personal data for the purposes of historical, statistical or scientific research should, in order to be lawful, also respect other relevant legislation such as on clinical trials." (Recital 125)

- "Scientific research for the purposes of this Regulation should include fundamental research, applied research, and privately funded research and in addition should take into account the Union's objective under Article 179(1) of the Treaty on the Functioning of the European Union of achieving a European Research Area." (Recital 126)
The reform: research, etc.

Overarching principles still apply:

• "Personal data must be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject; (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; (...)” (Article 5 draft General Regulation)

• “The processing of personal data, revealing race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited.” (Article 9 (1) draft General Regulation)
The reform: research, etc.

But the needs of researchers have been taken into account:

• "Paragraph 1 shall not apply where: (i) processing is necessary for historical, statistical or scientific research purposes subject to the conditions and safeguards referred to in Article 83” (Article 9 (2) draft General Regulation)

• “Within the limits of this Regulation, personal data may be processed for historical, statistical or scientific research purposes only if:
  – (a) these purposes cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject;
  – (b) data enabling the attribution of information to an identified or identifiable data subject is kept separately from the other information as long as these purposes can be fulfilled in this manner.” (Article 83 (1) draft General Regulation)
The reform: research, etc.

But the needs of researchers have been taken into account:

• “Bodies conducting historical, statistical or scientific research may publish or otherwise publicly disclose personal data only if:
  • (a) the data subject has given consent, subject to the conditions laid down in Article 7;
  • (b) the publication of personal data is necessary to present research findings or to facilitate research insofar as the interests or the fundamental rights or freedoms of the data subject do not override these interests; or
  • (c) the data subject has made the data public.” (Article 83 (2) draft General Regulation)
The reform: research, etc.

But the needs of researchers have been taken into account:

• “The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying the criteria and requirements for the processing of personal data for the purposes referred to in paragraph 1 and 2 as well as any necessary limitations on the rights of information to and access by the data subject and detailing the conditions and safeguards for the rights of the data subject under these circumstances.” (Article 83 (3) draft General Regulation)
The reform: research, etc.

But use of consent has been restricted:

- **Deleted**: “Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller.” (Article 7 (4) draft General Regulation, Commission’s legislative proposal)

- **Maintained**: "In order to safeguard that consent has been freely-given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller and this imbalance makes it unlikely that consent was given freely in all the circumstances of that specific situation. (.)“ (Recital 34 draft General Regulation)
But use of consent has been restricted:

- Maintained: "For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended; consent should not be regarded as freely-given if the data subject has no genuine and free choice and is unable to refuse or withdraw consent without detriment." (Recital 33 draft General Regulation)

- Maintained: "Processing of personal data shall be lawful only if (…) the data subject has given unambiguous consent to the processing of their personal data for one or more specific purposes". (Article 6(1)a) – (The word "unambiguous" is new.)

- Maintained: where Article 6(1)(a) applies, "the controller shall be able to demonstrate that unambiguous consent was given by the data subject". (Article 7(1)) – (entirely new provision)
Thank you for your attention!

For more information:

jacob.kornbeck@edps.europa.eu
www.edps.europa.eu
edps@edps.europa.eu
@EU_EDPS