RIGHT TO BE FORGOTTEN.
THE FUNDAMENTAL RIGHT OF THE PERSON
AND THE DANGER OF THE “MINISTRY OF TRUTH”

2012 Symposium of the Fundamental Rights Agency
“The EU Data Protection Reform: New Fundamental Rights Guarantees”

WOJCIECH WIEWIÓROWSKI PhD
Inspector General for Personal Data Protection, Poland
Faculty of Law and Administration, University of Gdansk

Vienna, May 10th, 2012
LADIES AND GENTLEMEN,
DEAR DATA SUBJECTS...
THE RIGHT TO BE FORGOTTEN

Article 17 provides the data subject's right to be forgotten and to erasure. It further elaborates and specifies the right of erasure provided for in Article 12(b) of Directive 95/46/EC and provides the conditions of the right to be forgotten, including the obligation of the controller which has made the personal data public to inform third parties on the data subject's request to erase any links to, or copy or replication of that personal data. It also integrates the right to have the processing restricted in certain cases, avoiding the ambiguous terminology “blocking”.

Vienna, May 10th, 2012
...ARE YOU AWARE OF YOUR RIGHT TO BE FORGOTTEN?
(53) Any person should have the right to have personal data concerning them rectified and a 'right to be forgotten' where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation. **This right is particularly relevant, when the data subject has given their consent as a child, when not being fully aware of the risks involved by the processing**, and later wants to remove such personal data especially on the Internet. However, the **further retention of the data should be allowed where it is necessary for historical, statistical and scientific research purposes**, for reasons of public interest in the area of public health, **for exercising the right of freedom of expression**, when required by law or where there is a reason to restrict the processing of the data instead of erasing them.

Vienna, May 10th, 2012
THE RIGHT TO BE FORGOTTEN

(54) To strengthen the 'right to be forgotten' in the online environment, the right to erasure should also be extended in such a way that a controller who has made the personal data public should be obliged to inform third parties which are processing such data that a data subject requests them to erase any links to, or copies or replications of that personal data. To ensure this information, the controller should take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible. In relation to a third party publication of personal data, the controller should be considered responsible for the publication, where the controller has authorised the publication by the third party.
THE RIGHT TO BE FORGOTTEN

Article 17

Right to be forgotten and to erasure

1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:

(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;

(c) the data subject objects to the processing of personal data pursuant to Art.19;

(d) the processing of the data does not comply with this Regulation for other reasons.
THE RIGHT TO BE FORGOTTEN

Article 17 (...) 2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.

3. The controller shall carry out the erasure without delay, except to the extent that the retention of the personal data is necessary:

(a) for exercising the right of freedom of expression in accordance with Art. 80;
(b) for reasons of public interest in the area of public health in accordance with Art. 81;
(c) for historical, statistical and scientific research purposes in accordance with Art. 83;
(d) for compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued;
(e) in the cases referred to in paragraph 4.
THE RIGHT TO BE FORGOTTEN

4. Instead of erasure, the controller shall restrict processing of personal data where:

   (a) their accuracy is contested by the data subject, for a period enabling the controller to verify the accuracy of the data;
   (b) the controller no longer needs the personal data for the accomplishment of its task but they have to be maintained for purposes of proof;
   (c) the processing is unlawful and the data subject opposes their erasure and requests the restriction of their use instead;
   (d) the data subject requests to transmit the personal data into another automated processing system in accordance with Article 18(2).

5. Personal data referred to in paragraph 4 may, with the exception of storage, only be processed for purposes of proof, or with the data subject's consent, or for the protection of the rights of another natural or legal person or for an objective of public interest.

6. Where processing of personal data is restricted pursuant to paragraph 4, the controller shall inform the data subject before lifting the restriction on processing.
THE RIGHT TO BE FORGOTTEN

7. The controller shall implement mechanisms to ensure that the time limits established for the erasure of personal data and/or for a periodic review of the need for the storage of the data are observed.

8. Where the erasure is carried out, the controller shall not otherwise process such personal data.

9. The Commission shall be empowered to adopt delegated acts in accordance with Article 86 for the purpose of further specifying:

   (a) the criteria and requirements for the application of paragraph 1 for specific sectors and in specific data processing situations;

   (b) the conditions for deleting links, copies or replications of personal data from publicly available communication services as referred to in paragraph 2;

   (c) the criteria and conditions for restricting the processing of personal data referred to in paragraph 4.

Vienna, May 10th, 2012
THE RIGHT TO BE FORGOTTEN AND FREEDOM OF EXPRESSION

Article 80 Processing of personal data and freedom of expression

1. Member States shall provide for exemptions or derogations from the provisions on the general principles in Chapter II, the rights of the data subject in Chapter III, on controller and processor in Chapter IV, on the transfer of personal data to third countries and international organisations in Chapter V, the independent supervisory authorities in Chapter VI and on co-operation and consistency in Chapter VII for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic or literary expression in order to reconcile the right to the protection of personal data with the rules governing freedom of expression.

2. Each Member State shall notify to the Commission those provisions of its law which it has adopted pursuant to paragraph 1 [in two years from the date the regulation comes into force] and, without delay, any subsequent amendment law or amendment affecting them.

Vienna, May 10th, 2012
Wolfgang Werlé and Manfred Lauber are German half-brothers who were convicted of the 1990 murder of actor Walter Sedlmayr.

On October 27, 2009, lawyers for Wolfgang Werlé sent the Wikimedia Foundation a cease and desist letter requesting that Werlé's name be removed from the English language Wikipedia article "Walter Sedlmayr", citing a 1973 Federal Constitutional Court decision that allows the suppression of a criminal's name in news accounts once he is released from custody. Previously, the attorney for both men, Alexander H. Stopp, had won a default judgment in German court, on behalf of Lauber, against the Wikimedia Foundation. Werlé's lawyers also challenged an Internet service provider in Austria which published the names of the convicted killers.
THE RIGHT TO BE FORGOTTEN AND THE MINISTRY OF TRUTH

Wikimedia is based in the United States, where the First Amendment protects freedom of speech and freedom of the press, under which the articles on Wikipedia would fall. In Germany, the law seeks to protect the name and likenesses of private persons from unwanted publicity. On Jan. 18, 2008, a court in Hamburg supported the personality rights of Werlé, which under German law includes removing his name from archive coverage of the case.

On Nov. 12, 2009, The New York Times reported that Wolfgang Werlé has a case pending against the Wikimedia Foundation in a German court. The German language Wikipedia article about the Sedlmayr case removed the names of the murderers. The Guardian observed that the lawsuit has led to the Streisand effect, an upsurge in publicity for the case resulting from the legal action.

On Dec. 15, 2009, the German Federal Court of Justice ruled that German websites do not have to check their archives in order to provide permanent protection of personality rights for convicted criminals.
THE RIGHT TO BE FORGOTTEN AND THE MINISTRY OF TRUTH

Original photo shows Trotsky; Stalin-era version does not.
Vienna, May 10th, 2012
Slettmeg.no offers advice and guidance to people of all ages who find offending material about themselves on the Internet. Offending material might be photos published without permission, fake profiles on different Internet services, incorrect personal information or harassment. People who have published this information themselves, but regret it and want this information removed, may also get in touch with slettmeg.no for support.

Slettmeg.no has no mandate to demand anything removed from the Internet. The service is only meant to give advice and guidance on how to act if you want information about yourself on the Internet deleted or corrected.

The website contains informative self-help articles on subjects related to privacy violations online, articles informing about the relevant legal rights on the Internet and contact details for the most important Internet service providers.

Slettmeg.no is, however, more than a web page. People may contact the service by phone, e-mail or Contact Form. The opening hours are Monday to Thursday from 10 am - 8 pm and Friday from 10 am – 3 pm.

Questions? Call + 47 08 247, or write an e-mail to hjelp@slettmeg.no.
THE RIGHT TO BE FORGOTTEN
GOOD PRACTICES
Article 18 introduces the data subject's right to data portability, i.e. to transfer data from one electronic processing system to and into another, without being prevented from doing so by the controller. As a precondition and in order to further improve access of individuals to their personal data, it provides the right to obtain from the controller those data in a structured and commonly used electronic format.
(55) To further strengthen the control over their own data and their right of access, data subjects should have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain a copy of the data concerning them also in commonly used electronic format. The data subject should also be allowed to transmit those data, which they have provided, from one automated application, such as a social network, into another one. This should apply where the data subject provided the data to the automated processing system, based on their consent or in the performance of a contract.
DATA PORTABILITY

Article 18 Right to data portability

1. The data subject shall have the right, where personal data are processed by electronic means and in a structured and commonly used format, to obtain from the controller a copy of data undergoing processing in an electronic and structured format which is commonly used and allows for further use by the data subject.

2. Where the data subject has provided the personal data and the processing is based on consent or on a contract, the data subject shall have the right to transmit those personal data and any other information provided by the data subject and retained by an automated processing system, into another one, in an electronic format which is commonly used, without hindrance from the controller from whom the personal data are withdrawn.

3. The Commission may specify the electronic format referred to in paragraph 1 and the technical standards, modalities and procedures for the transmission of personal data pursuant to paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 87(2).

Vienna, May 10th, 2012
Interoperability, within the context of European public service delivery, is the ability of disparate and diverse organisations to interact towards mutually beneficial and agreed common goals, involving the sharing of information and knowledge between the organisations, through the business processes they support, by means of the exchange of data between their respective ICT systems.


Look also:

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions 'Towards interoperability for European public services' - Annex II - European Interoperability Framework (EIF) for European public services
INTEROPERABILITY

Cooperating partners with compatible visions, aligned priorities, and focused objectives

- Political Context
- Legal Interoperability
  - Legislative Alignment

- Organisational Interoperability
  - Organisation and Process Alignment

- Semantic Interoperability
  - Semantic Alignment

- Technical Interoperability
  - Interaction & Transport

Aligned legislation so that exchanged data is accorded proper legal weight

Coordinated processes in which different organisations achieve a previously agreed and mutually beneficial goal

Precise meaning of exchanged information which is preserved and understood by all parties

Planning of technical issues involved in linking computer systems and services

Vienna, May 10th, 2012
Interoperability agreements should be drafted with sufficient detail to achieve their aim — to provide a European public service — while leaving each organisation maximum internal autonomy. At legal level, interoperability agreements are rendered specific and binding via legislation, including European directives and their transposition into national legislation, or bilateral and multilateral agreements, which are outside the scope of the EIF.

At organisational level, interoperability agreements can, for example, take the form of MoUs or SLAs that specify the obligations of each party participating in cross-border business processes. Interoperability agreements at organisational level will define expected levels of service, support/escalation procedures, contact details, etc., referring, when necessary, to underlying agreements at semantic and technical levels.

At semantic level, interoperability agreements can take the form of reference taxonomies, schemes, code lists, data dictionaries, sector-based libraries and so forth.

At technical level, interoperability agreements include interface specifications, communication protocols, messaging specifications, data formats, security specifications or dynamic registration and service discovery specifications.
While interoperability agreements at legal and organisational level will usually be very specific to the European public service concerned, interoperability agreements at technical level and, to a lesser extent, at semantic level can often be mapped onto existing formalised specifications.

**Recommendation 20.** Public administrations, when establishing European public services, should base interoperability agreements on existing formalised specifications, or, if they do not exist, cooperate with communities working in the same areas.
When trying to implement interoperability agreements, at technical or semantic level, there may be a choice between a number of equivalent, competing specifications, all of which may be able to provide a basis for such agreements. Public administrations may decide to support multiple formalised specifications or technologies to communicate with citizens and businesses. However, for reasons of efficiency, they should reduce, as much as possible, the number of formalised specifications and technologies when working together to provide a European public service.

Similar decisions are often taken not just to provide a single European public service but within a wider context of cooperation within or among organisations. In this context, they should be aware that internal interfaces may become external in the future when new European public services are created.

Decisions on what formalised specifications and technologies to use to ensure interoperability for European public services should be based on transparency, fairness and non-discrimination. One way to do this is to agree on a common assessment methodology and selection process.
5.2 Assessing and selecting formalised specifications

When public administrations select the formalised specifications or technologies to ensure interoperability, they should assess relevant formalised specifications. This assessment should be tailored to the specific interoperability needs of the public administrations in question, but based on objective criteria, primarily related to functional interoperability needs.

When several formalised specifications meet functional interoperability needs, additional criteria on quality of implementation, market support, potential for reusability and openness can be used.

Recommendation 21. Public administrations should use a structured, transparent and objective approach to assessing and selecting formalised specifications.
THANK YOU FOR YOUR ATTENTION!