



Big speech data privacy issues

BISON project Kick-off-Meeting
Brno, 16/01/2015



Relevant legislation

- Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (Data protection directive).
- Directive 2002/58/EC of the European Parliament and of the Council of 12.07.2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).



Reform of data protection legislation

- Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR)
- Planned for adoption soon, it will be directly applied in all EU Member States
- http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm



Key changes 1/2

- Right to be forgotten
- Consent to be given explicitly
- Increased responsibility and accountability of those who process personal data
- Companies refer to a single DPA in the country of establishment
- Removal of unnecessary administrative burdens (e.g. notification requirements for companies processing personal data)



Key changes 2/2

- Right of data portability (from one service to another)
- Obligation to notify serious data breaches without undue delay
- EU rules will apply to companies not established in the EU, if they offer goods or services in the EU or monitor the online behaviour of citizens
- Individuals will have the right to refer all cases to their home national DPA, even when their personal data are processed outside their home country



Personal data

Any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity



Personal data processing

Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction



Data controller

The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data (e.g. a company selling products or providing services as concerns the data of its clients)



Data processor

A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller (e.g. a contact center on behalf of its clients)



Application of DP Directive 1/3

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;



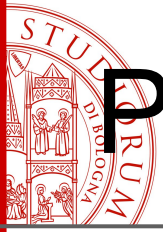
Application of DP Directive 2/3

- (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.



Application of DP Directive 3/3

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.



Principles for PD processing 1/3

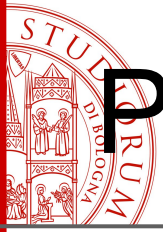
Personal data must be:

- (a) processed fairly and lawfully;
- (b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible provided that Member States provide appropriate safeguards;



Principles for PD processing 2/3

- (c) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;



Principles for PD processing 3/3

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. *Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use.*



Criteria for legitimate DP 1/2

Personal data may be processed only if:

- (a) the data subject has unambiguously given his consent; or
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject; or



Criteria for legitimate DP 2/2

- (d) processing is necessary in order to protect the vital interests of the data subject; or
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.



Special categories of processing 1/3

- Prohibition to process personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.
- This rule shall not apply where:
 - (a) the data subject has given his explicit consent to the processing of those data, *except where the laws of the Member State provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject's giving his consent*; or



Special categories of processing 2/3

- (b) processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or
- (c) processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent; or



Special categories of processing 3/3

- (d) processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects; or
- (e) the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defence of legal claims.



Information to the data subject 1/3

If data are collected from the data subject

The controller or his representative must provide the data subject with at least the following information, except where he already has it:

- (a) identity of controller and his representative, if any;
- (b) purposes of processing;
- (c) any further information such as
 - the recipients or categories of recipients of the data,
 - whether replies to the questions are obligatory or voluntary, possible consequences of failure to reply,
 - the existence of the right of access to and the right to rectify the data concerning him



Information to the data subject 2/3

If data have not been obtained from the data subject

1. Controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:
 - (a) identity of controller and his representative, if any;
 - (b) purposes of the processing;



Information to the data subject 3/3

- (c) any further information such as
- categories of data concerned,
 - recipients or categories of recipients,
 - existence of the right of access to and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.



Right of access to data 1/2

Data subjects have the right to obtain from the controller:

(a) without constraint at reasonable intervals and without excessive delay or expense:

- confirmation as to whether or not data relating to him are being processed and information at least as to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed,
- communication to him in an intelligible form of the data undergoing processing and of any available information as to their source,



Right of access to data 2/2

- knowledge of the logic involved in any automatic processing of data concerning him at least in the case of legal decisions based on automated processing (art. 15);
- (b) as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of the Directive, in particular because of the incomplete or inaccurate nature of the data;
- (c) notification to third parties to whom the data have been disclosed of any rectification, erasure or blocking carried out in compliance with (b), unless this proves impossible or involves a disproportionate effort.



Security of processing

- The controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
- Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.



Prior checking

- 1. Member States shall determine the processing operations likely to present specific risks to the rights and freedoms of data subjects and check that these processing operations are examined prior to the start thereof.*
- 2. Prior checks shall be carried out by the supervisory authority following receipt of a notification from the controller or by the data protection official.*
- 3. Member States may also carry out such checks in the context of preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which define the nature of the processing and lay down appropriate safeguards.*



Notification 1/3

Obligation to notify supervisory authority

1. Controller or representative must notify SA before carrying out any wholly or partly automatic processing operation or set of operations for a single purpose or several related purposes.
2. *Member States may provide for simplification or exemption from notification only:*
 - *where, for categories of processing operations unlikely to affect adversely the rights and freedoms of data subjects, they specify purposes of processing, data or categories of data undergoing processing, category or categories of data subject, recipients or categories of recipient to whom the data are to be disclosed and length of time the data are to be stored, and/or*



Notification 2/3

- *where the controller, in compliance with national law, appoints a personal data protection official, responsible in particular:*
 - a) *for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive*
 - b) *for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),*
- thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.*



Notification 3/3

3. Member States may provide that par. 1 does not apply to processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.

4. Member States may provide for an exemption from the obligation to notify or a simplification of the notification in the case of processing operations referred to in Art.8 (2) (d).

5. Member States may stipulate that certain or all non-automatic processing operations involving personal data shall be notified, or provide for these processing operations to be subject to simplified notification”.

Liability

- Any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered.
- The controller may be exempted from this liability, in whole or in part, if he proves that he is not responsible for the event giving rise to the damage.



DP in BISON

BISON involves the processing of personal data and needs to be fully compliant with applicable data protection rules at EU level and at the level of Member States.

It will be important for us to have a totally clear picture of the scheme of personal data processing by CCs and by the BISON system, beside the information already available in the BISON proposal.



What we need to know

- who processes the data, on behalf of whom,
- what data are collected/need to be collected, on the basis of what approvals/authorisations/notifications,
- if and when the data protection information was originally provided, what was its content (defining the scope and limits of data processing, the purposes, data communication to external subjects, etc.),
- how the relationship between the CCs and their clients (as data controller and data processor) has been defined,
- whether instructions on data processing have been provided by the data controller to the data processor, etc.), what security measures have been adopted, etc.



Deliverable 8.1

Ethical approvals for the data [M3]

This deliverable will complement the 1st version of the Data planning and management deliverable (D3.1) and contain ethical approvals for the planned collection and analyses of personal data by the competent University Data Protection Officer/ National DPAs.



Del 8.1 UNIBO tasks

- Review and check existing approvals of CCs by Data protection authorities (DPAs) from the legal point of view, to see whether they allow the processing of CC data for the purposes stated in the BISON DoA.
- If they are not covering this use, CCs will have to ask DPAs for new approvals or extension of existing ones.
- Copies of these approvals will be provided to the EC in Deliverable 8.1 and, if updates or new approvals are needed, also in D8.[2345].
- This is a very important step, as no work can be performed on the data before these approvals are issued.



D 8.1 Feedback needed

- We need the text of existing approvals of CCs by Data protection authorities (DPAs) and an explanation by CCs on their personal data processing flows in commercial activities.
- In case approvals are not covering the use of data in BISON, CCs will have to ask DPAs for new approvals or extension of the existing ones.



D 8.2 UNIBO tasks

“Legal, ethical and societal issues of BISON – General framework” (M6).

Provide detailed information on

- procedures to be implemented for data collection, storage, protection, retention and destruction and confirm that they comply with national and EU rules;
- planned/implemented informed consent procedures and their feasibility in massive CC data collection;
- potential dual use implications of BISON results.

Describe measures to prevent malevolent, criminal, terrorist abuse of BISON results.



D8.2 Feedback needed

How are legal and ethical issues currently managed?

Information and consent procedures

Procedures for data collection, storage, protection, retention and destruction

Security measures adopted

How is data transfer from and to non-EU countries managed?

Have you considered dual use implications?



Opt-out Registers

Opt-in: CCs may only process personal data if specific informed consent has been provided by data subject.

Opt-out: CCs may process personal data provided that data subjects have not explicitly denied it.

E.g.: Italy - any telephone number in a public register can be called unless the owner of the line has asked to be inserted in the “Registro delle opposizioni”. Ireland - National Directory Database.

BISON must comply with existing opt-out rules and constantly check that only numbers NOT inserted in the national Registers are called.



Publicly available data

Even if personal data are available on the Internet it does not automatically mean that they can be processed by anyone for whatever purposes.

Attention should be paid on the conditions upon which such personal data have been published, by whom and for what goals.

Difference between data which can be consulted on-line and data from public registers subject to a regime of public knowability.



ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA

Claudia Cevenini

claudia.cevenini@unibo.it

Italo Cerno

italo.cerno@unibo.it

<http://www.unibo.it>

<http://www.cse.unibo.it/en>

<http://apice.unibo.it/xwiki/bin/view/Main/?language=en>