
# Big speech data analytics for contact centers

# BISON

http://bison-project.eu/

**European Horizon 2020 project No. 645323**


## Deliverable D8.3
## Legal, ethical and societal issues of BISON II

**Due date:** 31/12/2015 **Submission date:** 23/12/2015
**Project start date:** 01/01/2015 **Duration:** 36 months
**Lead beneficiary:** UNIBO **Revision:** 1
**Lead Author:** Claudia Cevenini (UNIBO)
**Contributors:** Enrico Denti (UNIBO), Italo Cerno (UNIBO), Silvia Bisi (UNIBO), Andrea Omicini (UNIBO), Johan Minne (MyForce), Luis Angel Galindo (TME), Patricia Romero (TME), Javier Julian Ortega Reyes (COMD), Jan "Honza" Černocký (BUT).

| **Dissemination level** | |
|---|---|
| CO: Confidential, only for members of the consortium (including the Commission Services) | X |
| PU: Public | |

# Summary

This Deliverable, as stated in the DoW, is intended as an update of D8.2 submitted for the first project review. Due to its nature of living document[1], its goal is to go beyond a mere updating, providing a further analysis of the legal, ethical and societal issues connected with the development and use of BISON results and technologies, following the needs emerged by the interaction with technical partners.

This Deliverable addresses WP8 objectives, in that it contributes to:

- identifying and analysing the legal requirements of speech data processing systems;
- investigating the relevant legal framework;
- exploring the impact of legal, ethical and societal issues on the deployment of BISON;
- examining how BISON shall be designed and used so as to comply with the applicable legal framework.

More precisely, in coherence with the WP8 tasks, it:

- defines a first taxonomy of the different legal issues;
- monitors the evolution of the EU legal framework;
- identifies and examines the relevant ethical and societal issues of big speech data analytics systems.

D8.3 builds incrementally upon the general framework developed in D8.2 (M6), broadening the analysis on the one side, and focussing on the specific needs of the technical partners on the other.

In order to conjugate readability with effectiveness, the previous content is not re-included – so that the new contribution can be caught at a glance – but at the same time short summaries and pointers to D8.2 are provided, so as to guarantee that the document is self-contained and autonomously readable.



[1] This deliverable is part of a living document articulated in four steps, aimed at supporting the technical partners throughout the whole project: D8.2, submitted in M6; D8.3, the present one; and the following ones, D8.4 due in M24 and D8.5 due in M36.

# Glossary

API – Application Programming Interface
ASR – Automatic Speech Recognition
CC – Contact Center
Conv – EU Convention
CRM – Customer Relationship Management
Dir – EU Directive
DoW – Document of Work
DPWP – Data Protection Working Party
GDPR – General Data Protection Regulation
IPR – Intellectual Property Rights
KWS – KeyWord Spotting
LGBT – Lesbian, Gay, Bisexual, Transgender
NDA – Non-Disclosure Agreement
OHIM – Office for Harmonization in the Internal Market (trademarks and designs)
P2P – Peer to Peer
Reg – EU Regulation
WIPO – World Intellectual Property Organization
wp – working paper
WP – Work Package

# Table of Contents

# 1. Introduction

In coherence with the WP8 objectives and tasks, this deliverable aims to:

- identify and further analyse the legal requirements of speech data processing systems;
- define a basic taxonomy of the most relevant legal issues;
- explore the impact of legal, ethical and societal issues on the deployment of BISON;
- examine how BISON shall be designed and used to abide by the law.

In the spirit of a living document conjugating readability with effectiveness, this document adopts an incremental approach: the previous content is not re-included but short summaries and pointers to D8.2 and D8.1 are provided whenever necessary.

The Deliverable is structured as follows:

- Section 2 presents the taxonomy of the relevant legal issues: its purpose is to broaden the D8.2 perspective, which was mainly focused on the protection of personal data, so as to provide partners with an insight on all the main legal aspects in the specific BISON context.
- Section 3 is devoted to the analysis of data legal issues: again, the goal is to broaden the D8.2 context, which focussed on the data gathered by partner CCs. Here we consider the other types of data identified in the DoW – namely, standard R&D data and data from public sources – to investigate if, and under which circumstances, they may be legitimately used for speech data mining system training.
- Section 4 provides a deeper techno-legal analysis of the anonymisation issue (previously developed in D8.2 §4.2.3) in connection with the technical document on "Recordings within BISON environment" drafted by MyForce.[2]
- We have then identified and examined the most relevant ethical and societal issues raised by BISON, going beyond the mere compliance with legal rules and regulations (Section 5).
- Section 6 outlines the legal support provided to the partners in direct relation to the BISON activities – in particular, concerning the instructions for annotators, the contracts of CCs with clients, and the drafting of Non-disclosure Agreements (NDAs).
- An update on Ethical approvals for the planned collection and analyses of personal data is provided (Section 7). A thorough analysis of Ethical Approvals is to be found in D8.1.
- Section 8 provides a short update on the evolution of the data protection legal framework, with special regard to *i)* the content and impact of the recent decision of the European Court of Justice, which has invalidated the "Safe Harbour"; and *ii)* the current state of the General Data Protection Regulation (GDPR), which is still awaiting publication.
- Finally, Section 9 reports the relevant legal references mentioned in this Deliverable, to provide a knowledge base for partners for consultation and further analysis.

[2] The document is an internal working report which was drafted by MyForce to have a technical basis on BISON anonymisation for discussion between the partners.

# 2. Legal issues taxonomy

As required by Task 8.1, this Section outlines a first taxonomy of the legal issues which apply to the design and deployment of big speech data analytics systems, both at EU and at selected Member States' level, with particular attention to the partners' national rules.

We have broadened and schematized the D8.2 general framework: the previous Deliverable (in particular § 2, 3, and 5) mainly focused on data protection, the first and foremost issue to be considered to guarantee the law-abidingness of the partners' activities. Here, instead, we encompass legal issues in a wide sense, highlighting their relevance both for the BISON project and for the post-BISON scenario.

As mentioned above, the purpose of this Section is not merely to identify and list the legal issues of interest, but specifically to connect them to the BISON context – both for the project activities and for the future perspective after the project conclusion. This systematisation of the legal information in the BISON perspective shall provide technical partners with a reference framework on a broader set of aspects which need to be considered, also in connection with the scenarios identified in D2.1 § 2 and examined in D8.2 § 5.

## 2.1 Identification and synthesis of relevant legal issues

In schematising legal issues which need to be taken in consideration for BISON, different aspects should be examined and their impact depends of the specific phase of the BISON project.

Therefore, three different stages of the BISON research and development have been identified:

- the *preliminary phase* (which summarizes D8.2's main concepts and issues),
- the *development phase*, and
- the *after-development* phase.

Each phase is detailed separately in an ad-hoc section of the table, so as to present the inter-connected relevant information in an effective and easy-to-read way. More precisely:

- the first column identifies each major legal issue;
- the second column identifies its relevant reifications in the BISON context;
- the next two columns provide the proper references to the relevant rules and regulations both at EU level (third column) and at national level (fourth column);
- finally, the last two columns shortly highlight whether each item is relevant for BISON both during the project (fifth column) and subsequently in the post-project commercial phase (sixth column).

The acronyms and abbreviations used in Table 1 are listed in the "References" of this Deliverable, while the legal foundations of Table 1 are reported and discussed in the following Section 2.2.

**Table 1 - Relevant legal issues**

| Legal Issue | Meaning in the BISON context | EU Level | Member states level | Relevance for BISON project | Relevance post-BISON project |
|---|---|---|---|---|---|
| **Preliminary phase** | | | | | |
| Personal Data Processing | Lawful collection of personal data to be used in software development | ▪ Dir 2002/58/EC<br>▪ Dir 97/66/EC<br>▪ Dir 95/46/EC<br>▪ Conv 108/1981<br>▪ Additional Protocol - Conv 108/1981 | ▪ CZ 101/2000<br>▪ E 15/1999<br>▪ E RD 994/1999<br>▪ E RD 1332/1994<br>▪ E RD 428/1993<br>▪ IT 259/2003<br>▪ IT 196/2003<br>▪ L 02.08.2002 | Yes – Even though the BISON project will only process anonymous data, in the perspective of post-BISON scenario partners need to be aware of the applicable rules. The development of smallBISON and then of bigBISON shall comply with data protection rules from the earliest design phases, according to the "privacy by design" principle | Yes – BISON will need to process large amounts of personal data and this shall be done in compliance with all legal principles (necessity, information and consent, adequate security measures, data quality, legitimate data processing, etc. – see D8.2, § 2 and 3) set by EU rules and regulations, as applied at national level |
| | Anonymisation of personal data | ▪ Opinion 5/2014 DPWP[3]<br>▪ Opinion 3/2013 | ▪ CZ 101/2000<br>▪ E 15/1999<br>▪ E RD 994/1999 | Yes – The BISON project will strongly rely on effective data | Yes – In compliance with the necessity and purpose principles, personal data |

[3] "Data Protection Working Party", also called "Article 29 Data Protection Working Party" or "Article 29" is an independent advisory body set up by the Data Protection Directive, see http://ec.europa.eu/justice/data-protection/article-29/index_en.htm Its contribution has also been mentioned in D8.2 §2 and §4.

| | | | | | |
|---|---|---|---|---|---|
| | | DPWP<br>▪ Dir 95/46/EC | ▪ E RD 1332/1994<br>▪ E RD 428/1993<br>▪ IT 196/2003<br>▪ L 02/08/2002 | anonymisation (see D8.3 § 4 for details) | shall be anonymised whenever not necessary to achieve the processing purposes. BISON should enable this, with the highest anonymisation level set as default. |
| | Transferring data among partners | ▪ Opinion 8/2010 DPWP<br>▪ Opinion 1/2010 DPWP<br>▪ Dir 95/46/EC | ▪ CZ 101/2000<br>▪ E 15/1999<br>▪ E RD 994/1999<br>▪ E RD 1332/1994<br>▪ E RD 428/1993<br>▪ IT 196/2003<br>▪ L 02/08/2002 | Yes – To develop smallBISON and bigBISON there may be the need to transfer data from one partner to another. No legal issue arises when the transferred data have been the subject of a correct and preventive process of anonymisation. However, in the rare event that it may be necessary to transfer personal data that have not been anonymised it will be necessary to observe the European legislation on transfer of personal data and the guidelines provided by the DPWP | |

| **Development phase** | | | | | |
|---|---|---|---|---|---|
| Assignment of responsibilities | Need to have different levels to access of information | ▪ Dir 95/46/EC | ▪ CZ 101/2000<br>▪ E 15/1999<br>▪ E RD 994/1999<br>▪ E RD 1332/1994<br>▪ E RD 428/1993<br>▪ IT 196/2003<br>▪ L 02/08/2002 | Yes – bigBISON should be able to assign different privileges and authorisation levels to operators | Yes – bigBISON should be able to handle the assignment of different privileges and authorisation levels to operators |
| Balance between the right of workers not to be controlled and efficiency of BISON | Need to keep track of people who enter data or modify data or performing operations | ▪ Recommendation CM/Rec(2015)5<br>▪ Dir 95/46/EC | ▪ CZ 101/2000<br>▪ E 15/1999<br>▪ E RD 994/1999<br>▪ E RD 1332/1994<br>▪ E RD 428/1993<br>▪ IT 196/2003<br>▪ IT 300/1970<br>▪ L 02/08/2002 | Yes – bigBISON should design data processing operations in such a way as to prevent or at least minimise the risk of interference with the employees' fundamental rights and freedoms | Yes – Need to inform contact center operators before using bigBISON about the introduction of information systems and technologies enabling the monitoring of their activities. Mention should be made in employment contracts |
| Secure identification of the customer | Need to ask the customer security questions | ▪ Dir 95/46/EC | ▪ CZ 101/2000<br>▪ E 15/1999<br>▪ E RD 994/1999<br>▪ E RD 1332/1994<br>▪ E RD 428/1993 | Yes – bigBISON should be able to indicate to the operators different security questions to use | Yes – bigBISON should be able to handle the selection of security questions |

| | | | | | |
|---|---|---|---|---|---|
| | | | ▪ IT 196/2003<br>▪ L 02/08/2002 | | |
| General information | Information requirements set by law:<br>▪ information on providers (i.e. contact centers' clients) and their services<br>▪ consumer information requirements for distance and off-premises contracts | ▪ Dir 2011/83/EU<br>▪ Dir 2006/123/EC | ▪ CZ 89/2012<br>▪ CZ 222/2009<br>▪ CZ 198/2009<br>▪ CZ 634/1992<br>▪ E 3/2014<br>▪ E RD 1/2007<br>▪ IT 59/2010<br>▪ IT 206/2005 | Yes – bigBISON should be able to handle information set by law | Yes – bigBISON should be able to handle information set by law |
| Unsolicited calls to customer | Need to have the customer's consent to receive calls for purposes of direct marketing | ▪ Dir 2002/58/EC<br>▪ Dir 97/66/EC | ▪ CZ 89/2012<br>▪ CZ 480/2004<br>▪ CZ 40/1995<br>▪ CZ 634/1992<br>▪ E 3/2014<br>▪ E 29/2009<br>▪ E RD 1/2007<br>▪ IT 206/2005 | Yes – bigBISON should keep track of consent or of the failure to provide it by the customer | Yes – bigBISON should be able to handle changes in the customer's consent |

| | | | | | |
|---|---|---|---|---|---|
| | | | ▪ IT 196/2003 | | |
| Contract making | Need to track all the phases of contract making between the contact center and the end user such as: a) day and time of the telephone contact and response; b) date of sending of the contract on paper to the customer; c) date of receipt of the signed contract | ▪ Dir 2011/83/EU | ▪ CZ 89/2012<br>▪ CZ 634/1992<br>▪ E 3/2014<br>▪ E RD 1/2007<br>▪ IT 206/2005<br>▪ IT 262/1942 | Yes – bigBISON should not interfere with the CRM in keeping track of all the phases of contract making between the contact center and the end user | Yes – bigBISON should not interfere with the CRM in keeping track of all the phases of contract making between the contact center and the end user |
| Personal Data Processing | Requirement of information and consent prior to the processing of personal data | ▪ Dir 95/46/EC | ▪ CZ 101/2000<br>▪ E 15/1999<br>▪ E RD 994/1999<br>▪ E RD 1332/1994<br>▪ E RD 428/1993<br>▪ IT 196/2003<br>▪ L 02/08/2002 | Yes – bigBISON should keep track of the data protection information submitted to customers whose data are processed by the software and the consent expressed by these (including any change) | Yes – bigBISON should be able to handle information and consent to the processing of personal data |
| | Security of | ▪ Dir 95/46/EC | ▪ CZ 101/2000 | Yes – bigBISON should be | Yes – bigBISON should be |

| | | | | | |
|---|---|---|---|---|---|
| | personal data | | ▪ IT 196/2003<br>▪ E 15/1999<br>▪ E RD 994/1999<br>▪ E RD 1332/1994<br>▪ E RD 428/1993<br>▪ L 02/08/2002 | able to implement and handle adequate security measures to prevent damages to third parties | able to implement and handle security measures to prevent damages to third parties |
| | Rights of the data subject | ▪ Dir 95/46/EC | ▪ CZ 101/2000<br>▪ E 15/1999<br>▪ E RD 994/1999<br>▪ E RD 1332/1994<br>▪ E RD 428/1993<br>▪ IT 196/2003<br>▪ L 02/08/2002 | Yes – bigBISON should react to the data subject's requests based on its rights (access to personal data, revocation of the consent with subsequent cancellation of all or some personal data, etc.) | Yes – bigBISON should be able to handle rights of the data subject |
| **After development phase** | | | | | |
| Trademark protection | Trademark registration | ▪ Council Regulation 207/2009<br>▪ Dir 2008/95/EC | ▪ CZ 441/2003<br>▪ E RD 1/1996<br>▪ IT 30/2005<br>▪ IT 262/1942 | Yes – It may be advisable to register the trademark of the "BISON" name and logo (or another suitable different name or logo if "BISON" had already been registered by third parties as a trademark for the same categories of interest) | Yes – It will be necessary to protect the name "BISON" from any use and abuse by third parties |

| | | | | | |
|---|---|---|---|---|---|
| License | Definition of the contractual relationship with the prospective buyers | ▪ Dir 2009/24/EC | ▪ CZ 121/2000<br>▪ E RD 1/1996<br>▪ IT 633/1941<br>▪ IT 262/1942 | | Yes – It will be necessary to draft contracts for the commercial exploitation |
| Advertising | Correct information and commercial communication to the prospective buyers | ▪ Dir 2011/83/EU<br>▪ Dir 2006/114/EC<br>▪ Dir 2000/31/EC | ▪ CZ 89/2012<br>▪ CZ 480/2004<br>▪ CZ 40/1995<br>▪ CZ 634/1992<br>▪ E 3/2014<br>▪ E 29/2009<br>▪ E RD 1/2007<br>▪ IT 145/2007<br>▪ IT 70/2003 | Yes – advertising in the form of dissemination on BISON shall be carried out in compliance with the General Annex | Yes – It will be necessary to adopt a law-abiding and correct form of advertising to promote BISON's results |
| Software distribution | Providing software at a distance, by electronic means, at the individual request of a recipient of services | ▪ Dir 2000/31/EC<br>▪ Dir 98/34/EC | ▪ CZ 222/2009<br>▪ CZ 480/2004<br>▪ IT 70/2003 | | Yes – Speech analytics may be provided at distance, by electronic means, at the individual request of a recipient of services. This should comply with EU rules on the provision of information society services |

## 2.2 Explication of legal issues and concepts of Table 1

The content of Table 1 is built around the following three different stages of the BISON research and development: a) Preliminary phase; b) Development phase; c) After development phase.

### *A) Preliminary phase*

The first section of Table 1 pays attention to the checks to be necessarily made before starting the development of BISON in order to process personal data.

*A.1) Personal data processing*

Even though the BISON project will only process anonymous data, in the perspective of the post-BISON scenario, partners need to be aware of the applicable rules. The development of smallBISON and then of bigBISON shall comply with data protection rules from the earliest design phases, according to the "privacy by design" principle.

BISON will need to process large amounts of personal data (so said "big data") and this shall be done in compliance with all legal principles (necessity, information and consent, adequate security measures, etc. – see D8.2 § 2 and 3) set by EU rules and regulations, as applied at national level.

In particular:

- the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [Conv 108/1981] and the Additional Protocol [Additional Protocol – Conv 108/1981] signed by the member States of the Council of Europe show the necessity to secure in the territory of each State for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to the automatic processing of personal data relating to him.

  To achieve this purpose, personal data undergoing automatic processing shall be:

  a) obtained and processed fairly and lawfully;

  b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

  c) adequate, relevant and not excessive in relation to the purposes for which they are stored;

  d) accurate and, where necessary, kept up to date;

  e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored (Art. 5).

Appropriate security measures shall also be taken for the protection of personal data stored in automated data files against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination (Art. 7).

- In a similar way, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, briefly "Data Protection Directive" [Dir 95/46/EC] states the so-called "**Principles relating to data quality**" establishing that Member States shall provide that 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;

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;

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 (Art. 6).

The Data Protection Directive also lists "**Criteria for making data processing legitimate**", establishing that Member States shall provide that 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

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 (Art. 7).

In terms of **security of processing**, the Data Protection Directive states that member States shall provide that the controller must implement appropriate technical and organisational 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.

Other principles relating to the processing of personal data in the Data Protection Directive have been examined in D8.2, § 2 ("Legal and Ethical Framework of data processing in the BISON perspective") and 3 ("From the DPD to the General Data Protection Regulation – general outline").

In the European legal system, other rules are in force which regulate personal data protection in the telecommunications and in electronic communications sectors.

In particular:

- Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy **in the telecommunications sector** [Dir 97/66/EC], and the Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy **in the electronic communications sector** (Directive on privacy and electronic communications) [Dir 2002/58/EC] confirm the principle of the necessity of a **prior consent by the user or subscriber** to the processing of personal data and they require that the provider of a publicly available telecommunications or electronic communications service must take **appropriate technical and organisational measures to safeguard security** of its services. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

*A.2) Anonymisation of personal data*

During the BISON project, only anonymous data will be used for the development of smallBISON and bigBISON.

The principles of protection of personal data – as highlighted by the Data Protection Directive – do not apply to data rendered anonymous in such a way that the data subject is no longer identifiable (Whereas No. 26).

With reference to this issue, the Art. 29 Data Protection Working Party (DPWP) adopted on 10 April 2014 Opinion 5/2014 on **anonymisation techniques** – wp 216 [Opinion 5/2014 DPWP]. In this Opinion, the DPWP analyses the effectiveness and limits of existing anonymisation techniques against the EU legal background of data protection and provides recommendations to handle these techniques by taking account of the residual risk of identification inherent in each of them.

The BISON project will strongly rely on effective data anonymisation (see Section 4 of D8.3 for details as well as D8.2 §4.2; D8.1 §4.1 and §5; D6.1 §2.4; and D3.1 §3).

Data anonymisation is also important in the post-project commercial phase of BISON. In compliance with the necessity and purpose principles, personal data shall be anonymised whenever not necessary to achieve the processing purposes. BISON should enable this, with the highest anonymisation level set as default.

This setting shall be adopted in BISON, as discussed with the technical partners based on the preliminary working report by MyForce on anonymisation.

The purpose principle – stated in the Data Protection Directive (Art. 6) – is also the subject of Opinion 3/2013 on **purpose limitation** adopted on 2 April 2013 by the Art. 29 Data Protection Working Party (DPWP) – wp 203 [Opinion 3/2013]. This Opinion provides guidance for the principle's practical application under the current legal framework. Purpose limitation protects data subjects by setting limits on how data controllers may use their data while also offering some degree of flexibility for data controllers. The concept of purpose limitation has two main building blocks: personal data must

be collected for "specified, explicit and legitimate" purposes (purpose specification) and not be "further processed in a way incompatible" with those purposes (compatible use).

*A.3) Transferring data among partners*

The development of smallBISON and bigBISON may require the transfer of data from one partner to the others.

No legal issue is involved when the transferred data have been the object of a correct and preventive process of anonymisation. However, in the rare event that it may be necessary to transfer personal data that have not been anonymised it will be necessary to observe the European legislation on the transfer of personal data and the guidelines provided by the DPWP.

In particular:

- The Data Protection Directive provides specific rules on the **transfer of personal data to "third" countries** (extra-EU). The transfer of personal data to third countries is prohibited in principle (Art. 25, par. 1), unless the country in question ensures an "adequate" level of protection; the Commission has the power to establish such suitability through specific decisions (Art. 25, par. 6). Notwithstanding this prohibition, the transfer to third countries is also allowed in the cases mentioned in Art. 26, par. 1 (data subject's consent, transfer necessary for the conclusion or performance of a contract, overriding public interest, etc.), and based on contractual instruments that offer adequate safeguards (Art. 26, par. 2).

  This discipline is not of interest here, because any transfer of data to be performed between the partners during the project shall take place within the EU.

  The **transfer of personal data within the EU** is instead allowed (Art. 1), however, all the rules on personal data protection must be respected, such as those on purpose limitation (Art. 6), on information to be provided to the data subject (in particular concerning "the recipients or categories of recipients", Art. 10 and 11) and on the designation as data processor (Art. 17, par. 2-3-4).

  It is important to point out that, under Art. 17, the applicable law for security of processing shall be the national law of the member State where the processor is established and not the controller (see D8.2 §2.3).

- The DPWP adopted on 16 February 2010 Opinion 1/2010 on the **concepts of "controller" and "processor"** – wp 169 [Opinion 1/2010 DPWP] that defines the concepts and responsibilities of the controller and processor determining which national law is applicable to a processing operation or set of processing operations (see D8.2 §2.3).

- The DPWP adopted on 16 December 2010 the Opinion 8/2010 on **applicable law** – wp 179 [Opinion 8/2010 DPWP] that clarifies the scope of application of the Data Protection Directive, and in particular of its Art. 4, which determines which national data protection law(s) adopted pursuant to the same Directive may be applicable to the processing of personal data.

  A clear understanding of the applicable law helps to ensure both legal certainty for controllers and processors and a clear framework for data subjects.

### *B) Development phase*

During the development phase of BISON, partners will need to implement the software in order to achieve compliance with several rules and regulations.

The following ones have been identified as the main legal issues to be taken into account at this stage.

*B.1) Assignment of responsibilities*

When processing personal data, different levels of access to information and different responsibilities should be assigned. This is on the one side required by the law, based on the necessity principle: no-one should have access to more personal data than needed to perform his tasks. On the other side, it is also a matter of adequate organisation and adoption of procedures to ensure smooth performance of activities.

bigBISON should be able to assign different privileges and authorisation levels to operators or categories of operators.

In particular:

- The Data Protection Directive states that the controller must implement appropriate technical and **organisational 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 (art. 17, par. 1).

*B.2) Balance between the right of workers not to be controlled and efficiency of BISON*

The EU legislation on the processing of personal data (Data Protection Directive) foresees that it should be kept track of people who enter data or modify data or perform operations, as organisational security measure (Art. 17).

This is important for a correct assignment of responsibilities (see above *B.1*).

However, it requires a prior information on data protection.

Therefore, in the BISON context, it is necessary to inform contact center operators before using bigBISON about the introduction of information systems and technologies enabling the monitoring of their activities.

Indeed, the use of data processing methods by employers should be guided by principles designed to minimise any risks that such methods might pose to employees' rights and fundamental freedoms, in particular their right to privacy.

In particular:

- Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of **personal data in the context of employment** [Recommendation CM/Rec(2015)5] specifies that employers should provide employees the following information:
    - the categories of personal data to be processed and a description of the purposes of the processing;

- the recipients, or categories of recipients of the personal data;
- the means employees have of exercising the rights of access and rectification;
- any other information necessary to ensure fair and lawful processing (Art. 10).

Employers should also ensure the respect of the following safeguards, in particular:

- carry out a risk analysis of the potential impact of any intended data processing on the employees' rights and fundamental freedoms (Art. 20);
- consult employees' representatives in accordance with domestic law or practice, before any monitoring system can be introduced or in circumstances where such monitoring may change (Art. 21).

*B.3) Secure identification of the customer*

To identify with certainty the person with whom the operator comes in contact it is necessary to previously ask security questions to the customer.

This issue has also been examined in D2.1 §2.1.2, as the secure identification of the customer is a relevant part of the Operation scenario "Reduction of calls from people who are not entitled to act" (see also D8.2 §5.1).

If the operator should disclose personal information to a person other than the data subject, then the data processing would be unlawful.

In particular:

- Directive 95/46/EC on data protection recognizes **only** the data subject the right to obtain from the controller:

  (a) confirmation as to whether or not data relating to him are being processed; information on the purposes of the processing, the categories of data concerned and the recipients or categories of recipients to whom the data are disclosed;

  (b) communication to him in an intelligible form of the data undergoing processing and of any available information as to their source (Art. 12).

*B.4) General Information*

There is much information set by law that a service provider (i.e. contact center's client) must provide to the recipient of services; bigBISON should be able to handle these.

In particular:

<u>Information on providers and their services</u>

Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market [Dir 2006/123/EC] states that providers should make the following information available to the recipient of the services:

(c) the name of the provider, its legal status and form, the geographic address at which it is established and details enabling it to be contacted rapidly and communicated with directly and, as the case may be, by electronic means;

(d) where the provider is registered in a trade or other similar public register, the name of that register and the provider's registration number, or equivalent means of identification in that register;

(e) where the activity is subject to an authorisation scheme, the details of the relevant competent authority or the single point of contact;

(f) where the provider exercises an activity which is subject to VAT, its VAT identification number;

(g) in the case of regulated professions, the professional body or similar institution with which the provider is registered, the professional title and the Member State in which that title has been granted;

(h) the general conditions and clauses, if any, used by the provider;

(i) the existence of contractual clauses, if any, used by the provider concerning the law applicable to the contract and/or the competent court;

(j) the existence of an after-sales guarantee, if any, not imposed by law;

(k) the price of the service, where a price is pre-determined by the provider for a given type of service;

(l) the main features of the service, if not already apparent from the context;

(m) the professional liability insurance or guarantees, and in particular the contact details of the insurer or guarantor and the territorial coverage.

The above-mentioned information, according to the provider's preference:

(a) is supplied by the provider on its own initiative;

(b) is made easily accessible to the recipient at the place where the service is provided or can be easily accessed by the recipient electronically by means of an address supplied by the provider;

(c) appears in any information documents supplied by the provider to the recipient, which set out a detailed description of the service it provides.

At the recipient's request, providers must supply the following additional information:

(a) where the price is not pre-determined by the provider for a given type of service, the price of the service or, if an exact price cannot be given, the method for calculating the price so that it can be checked by the recipient, or a sufficiently detailed estimate;

(b) as regards regulated professions, a reference to the professional rules applicable in the Member State of establishment and how to access them;

(c) information on providers' multidisciplinary activities and partnerships which are directly linked to the service in question and on the measures taken to avoid conflicts of interest. That information shall be included in any information document in which providers give a detailed description of their services;

(d) any codes of conduct to which the provider is subject and the address at which these codes may be accessed by electronic means, specifying the language version available;

(e) where a provider is subject to a code of conduct, or is member of a trade association or professional body which provides for recourse to a non-judicial means of dispute settlement,

information in this respect. The provider shall specify how to access detailed information on the characteristics of, and conditions for, the use of non-judicial means of dispute settlement.

The information which a provider must supply should be made available or communicated in a clear and unambiguous manner, and in good time before or, where there is no written contract, before the service is provided (Art. 22).

Consumer information requirements for distance and off-premises contracts

Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights [Dir 2011/83/EU] states that before the consumer is bound by a distance or off-premises contract, or any corresponding offer, the trader must provide the consumer with the following information in a clear and comprehensible manner:

(a) the main characteristics of the goods or services, to the extent appropriate to the medium and to the goods or services;

(b) the identity of the trader, such as its trading name;

(c) the geographical address at which the trader is established and the trader's telephone number, fax number and e-mail address, where available, to enable the consumer to contact the trader quickly and communicate with it efficiently and, where applicable, the geographical address and identity of the trader on whose behalf he is acting;

(d) if different from the address provided in accordance with point (c), the geographical address of the place of business of the trader, and, where applicable, that of the trader on whose behalf he is acting, where the consumer can address any complaints;

(e) the total price of the goods or services inclusive of taxes, or where the nature of the goods or services is such that the price cannot reasonably be calculated in advance, the manner in which the price is to be calculated, as well as, where applicable, all additional freight, delivery or postal charges and any other costs or, where those charges cannot reasonably be calculated in advance, the fact that such additional charges may be payable. In the case of a contract of indeterminate duration or a contract containing a subscription, the total price shall include the total costs per billing period. Where such contracts are charged at a fixed rate, the total price shall also mean the total monthly costs. Where the total costs cannot be reasonably calculated in advance, the manner in which the price is to be calculated shall be provided;

(f) the cost of using the means of distance communication for the conclusion of the contract where that cost is calculated other than at the basic rate;

(g) the arrangements for payment, delivery, performance, the time by which the trader undertakes to deliver the goods or to perform the services and, where applicable, the trader's complaint handling policy;

(h) where a right of withdrawal exists, the conditions, time limit and procedures for exercising that right;

(i) where applicable, that the consumer will have to bear the cost of returning the goods in case of withdrawal and, for distance contracts, if the goods, by their nature, cannot normally be returned by post, the cost of returning the goods;

(j) that, if the consumer exercises the right of withdrawal after having made a request, the consumer must be liable to pay the trader reasonable costs;

(k) where a right of withdrawal is not provided for, the information that the consumer will not benefit from a right of withdrawal or, where applicable, the circumstances under which the consumer loses his right of withdrawal;

(l) a reminder of the existence of a legal guarantee of conformity for goods;

(m) where applicable, the existence and the conditions of after sale customer assistance, after-sales services and commercial guarantees;

(n) the existence of relevant codes of conduct, and how copies of them can be obtained, where applicable;

(o) the duration of the contract, where applicable, or, if the contract is of indeterminate duration or is to be extended automatically, the conditions for terminating the contract;

(p) where applicable, the minimum duration of the consumer's obligations under the contract;

(q) where applicable, the existence and the conditions of deposits or other financial guarantees to be paid or provided by the consumer at the request of the trader;

(r) where applicable, the functionality, including applicable technical protection measures, of digital content;

(s) where applicable, any relevant interoperability of digital content with hardware and software that the trader is aware of or can reasonably be expected to have been aware of;

(t) where applicable, the possibility of having recourse to an out-of-court complaint and redress mechanism, to which the trader is subject, and the methods for having access to it (Art. 6).

*B.5) Unsolicited calls to consumer*

The European legislation requires the customer's consent to calls made for purposes of direct marketing. bigBISON should be able to keep track of such consent - or lack thereof - expressed by the customer, and it should be able to handle any change in the customer's consent.

In particular:

- Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the **telecommunications sector** [Dir 97/66/EC] states that **unsolicited calls** for purposes of direct marketing are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these calls. This right applies to subscribers who are natural persons. Member States shall also guarantee, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited calls are sufficiently protected (Art. 12).
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the **electronic communications sector** (Directive on privacy and electronic communications) [Dir 2002/58/EC] states that **unsolicited communications** for purposes of direct marketing are not allowed either without the consent of the subscribers concerned or in respect of subscribers who do not wish to receive these communications. This right applies to subscribers who are natural persons. Member States shall also ensure, in the framework of Community law and applicable national legislation, that the legitimate interests of subscribers other than natural persons with regard to unsolicited communications are sufficiently protected (Art. 13).

*B.6) Contract making*

When a contract is concluded at a distance between the contact center and the end user, there emerges the need to track all the phases of contract making in accordance with the provisions of national laws such as:

a) day and time of the telephone contact and response;

b) date of sending of the contract to the customer in paper form;

c) date of receipt of the signed contract.

At EU level, in particular:

- The EU Directive on **consumer rights** [Dir 2011/83/EU] states that if the trader makes a telephone call to the consumer with a view to concluding a distance contract, it shall, at the beginning of the conversation with the consumer, disclose its identity, the identity of the person on whose behalf it is making that call, and the commercial purpose of the call. Where a distance contract is to be concluded by telephone, Member States may provide that the trader has to confirm the offer to the consumer, who shall be bound only once he has signed the offer or has sent his written consent. Member States may also provide that such confirmations have to be made on a durable medium (e.g. on paper) (Art. 8).

*B.7) Personal Data Processing*

bigBISON should be able to handle the processing of personal data (such as information, consent, exercise of rights of the data subject, security measures, etc.) in compliance with the provisions of applicable law.

As concerns the provisions of EU legislation on the processing of personal data – also in relation to the forthcoming General Data Protection Regulation – please refer to D8.2 § 2 and 3 and Section 8 of this D8.3 for the evolution of the legal framework.

***C) After-development phase***

The third branch of the Taxonomy takes into account the main legal issues related to relevant aspects of the after-development phase of BISON. These issues relate to the need for protection and circulation of the prospective business name and of the exploitation rights of the software developed, as well as its commercial distribution and promotion.

*C.1) Trademark protection*

The best way of protecting a trademark is to register it.

It may be decided to register the "BISON" name and logo (or another suitable different name or logo if "BISON" should already have been registered by third parties as a trademark for the same categories of interest)[4] to protect them against the possible use and abuse by third parties.

In particular:

[4]It will therefore be necessary, at the outset, to carry out a thorough trademark search in the OHIM database with the "BISON" name and logo https://oami.europa.eu/ohimportal/en/.

- Directive 2008/95/EC of the European Parliament and of the Council of 22 October 2008 to approximate the laws of the Member States relating to **trademarks** [Dir 2008/95/EC] states that a trademark may consist of any signs capable of being represented graphically, particularly words, including personal names, designs, letters, numerals, the shape of goods or of their packaging, provided that such signs are capable of distinguishing the goods or services of one undertaking from those of other undertakings (Art. 2).

  The registered trademark confers on the owner exclusive rights thereon. The owner is entitled to prevent all third parties not having its consent from using in the course of trade:

  (a) any sign which is identical with the trademark in relation to goods or services which are identical with those for which the trademark is registered;

  (b) any sign where, because of its identity with, or similarity to, the trademark and the identity or similarity of the goods or services covered by the trademark and the sign, there exists a likelihood of confusion on the part of the public; the likelihood of confusion includes the likelihood of association between the sign and the trademark (Art. 5).

- Council Regulation (EC) No. 207/2009 of February 26, 2009, on the **Community trademark** [Council Regulation 207/2009] provides for Community arrangements for trademarks whereby undertakings can by means of one procedural system obtain Community trademarks to which uniform protection is given and which produce their effects throughout the entire area of the Community. A Community trademark confers on the proprietor exclusive rights therein. The rights conferred by a Community trademark prevails against third parties from the date of publication of registration of the trademark. The proprietor is entitled to prevent all third parties not having his consent from using in the course of trade:

  (a) any sign which is identical with the Community trademark in relation to goods or services which are identical with those for which the Community trademark is registered;

  (b) any sign where, because of its identity with, or similarity to, the Community trademark and the identity or similarity of the goods or services covered by the Community trademark and the sign, there exists a likelihood of confusion on the part of the public; the likelihood of confusion includes the likelihood of association between the sign and the trademark;

  (c) any sign which is identical with, or similar to, the Community trademark in relation to goods or services which are not similar to those for which the Community trademark is registered, where the latter has a reputation in the Community and where use of that sign without due cause takes unfair advantage of, or is detrimental to, the distinctive character or the reputation of the Community trademark.

  The following, inter alia, may be prohibited:

  (a) affixing the sign to the goods or to the packaging thereof;

  (b) offering the goods, putting them on the market or stocking them for these purposes under that sign, or offering or supplying services thereunder;

  (c) importing or exporting the goods under that sign;

  (d) using the sign on business papers and in advertising (Art. 9).

*C.2) License*

In the after-development phase it will be necessary to regulate the contractual relationship with the prospective buyers of project results.

The use and circulation of software in the EU is usually regulated with the licensing system, because the software is protected under intellectual property and not as a product or invention. The license is an authorisation (by the licensor-the developer/owner of the software) to use the licensed material (by the licensee). A license under intellectual property law usually has different components including a term, the territory, renewal provisions and other limitations deemed important to the licensor.

In particular:

- Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal **protection of computer programs** [Dir 2009/24/EC] establishes that the exclusive rights of the author/owner of a software include the right to do or to authorise:

  (a) the permanent or temporary reproduction of a computer program by any means and in any form, in part or in whole; in so far as loading, displaying, running, transmission or storage of the computer program necessitate such reproduction, such acts shall be subject to authorisation by the right holder;

  (b) the translation, adaptation, arrangement and any other alteration of a computer program and the reproduction of the results thereof, without prejudice to the rights of the person who alters the program;

  (c) any form of distribution to the public, including the rental, of the original computer program or of copies thereof (Art. 4).

*C.3) Advertising*

In the after-development phase it will be necessary to adopt a correct form of advertising to promote BISON's results.

The EU legislation provides different rules on advertising depending whether the recipient is a "consumer" or a "trader".

- According to the Directive on consumer rights [Dir 2011/83/EU]:
  - "**consumer**" means any natural person who, in contracts, is acting for purposes which are outside his trade, business, craft or profession;
  - "**trader**" means any natural person or any legal person, irrespective of whether privately or publicly owned, who is acting, including through any other person acting in his name or on his behalf, for purposes relating to his trade, business, craft or profession in relation to contracts (Art. 2).

The prospective buyers of project results will be only "traders" (contact centers, system integrators, data-mining companies, etc.), therefore the main principles of European law on advertising in **B2B** (**business to business**) relationships shall apply:

- Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning **misleading and comparative advertising** [Dir 2006/114/EC] frames some basic concepts:

(a) "advertising": the making of a representation in any form in connection with a trade, business, craft or profession in order to promote the supply of goods or services, including immovable property, rights and obligations;

(b) "misleading advertising": any advertising which in any way, including its presentation, deceives or is likely to deceive the persons to whom it is addressed or whom it reaches and which, by reason of its deceptive nature, is likely to affect their economic behaviour or which, for those reasons, injures or is likely to injure a competitor;

(c) "comparative advertising": any advertising which explicitly or by implication identifies a competitor or goods or services offered by a competitor (Art. 2).

In determining **whether advertising is misleading**, account must be taken of all its features, and in particular of any information it contains concerning:

(a) the characteristics of goods or services;

(b) the price or the manner in which the price is calculated, and the conditions on which the goods are supplied or the services provided;

(c) the nature, attributes and rights of the advertiser, such as his identity and assets, his qualifications and ownership of industrial, commercial or intellectual property rights or his awards and distinctions (Art. 3).

**Comparative advertising** is permitted when the following conditions are met:

(a) it is not misleading;

(b) it compares goods or services meeting the same needs or intended for the same purpose;

(c) it objectively compares one or more material, relevant, verifiable and representative features of those goods and services, which may include price;

(d) it does not discredit or denigrate the trademarks, trade names, other distinguishing marks, goods, services, activities or circumstances of a competitor;

(e) for products with designation of origin, it relates in each case to products with the same designation;

(f) it does not take unfair advantage of the reputation of a trademark, trade name or other distinguishing marks of a competitor or of the designation of origin of competing products;

(g) it does not present goods or services as imitations or replicas of goods or services bearing a protected trademark or trade name;

(h) it does not create confusion among traders, between the advertiser and a competitor or between the advertiser's trademarks, trade names, other distinguishing marks, goods or services and those of a competitor (Art.4).

- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market, briefly "E-commerce Directive" [Dir 2000/31/EC] regulates **on-line advertising**. It states, in particular, that:

  (a) commercial communications must be clearly identifiable as such;

(b) the natural or legal person on whose behalf the commercial communication is made must be clearly identifiable (Art. 6).

**Unsolicited commercial communications** by electronic mail should also be identifiable clearly and unambiguously as soon as they are received by the customer. This provision should be applied together with what is foreseen by the EU framework on data protection, which forbids the use of personal data for commercial purposes in the absence of prior specific consent by the data subject.

*C.4) Software distribution*

Software results of the project may be provided at a distance, by electronic means, at the individual request of a recipient of services. In this case, the EU legislation on electronic commerce may be applicable.

In particular:

- Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations [Dir 98/34/EC] defines "service" as "**any Information Society service**, that is to say, any service normally provided for remuneration, *at a distance*, *by electronic means* and *at the individual request of a recipient of services*", where:
    - "**at a distance**" means that the service is provided without the parties being simultaneously present;
    - "**by electronic means**" means that the service is sent initially and received at its destination by means of electronic equipment for the processing (including digital compression) and storage of data, and entirely transmitted, conveyed and received by wire, by radio, by optical means or by other electromagnetic means;
    - "**at the individual request of a recipient of services**" means that the service is provided through the transmission of data on individual request (Art. 1).

- The E-commerce Directive [Dir 2000/31/EC] states:
    - that the service provider must render easily, directly and permanently accessible to the recipients of the service and competent authorities, general information such as its name; the geographic address at which it is established; its details, including its electronic mail address, which allow it to be contacted rapidly and communicated with in a direct and effective manner (Art. 5);
    - the legal effectiveness and validity of contracts made by electronic means (Art. 9);
    - that at least the following information is given by the service provider clearly, comprehensibly and unambiguously and prior to the order being placed by the recipient of the service:
        (a) the different technical steps required to conclude the contract;
        (b) whether or not the concluded contract will be filed by the service provider and whether it will be accessible;

(c) the technical means for identifying and correcting input errors prior to the placing of the order;

(d) the languages offered for the conclusion of the contract (Art. 10, par. 1);

- contract terms and general conditions provided to the recipient must be made available in a way that allows him to store and reproduce them (Art. 10, par. 3);
- that in cases where the recipient of the service places his order through technological means, the following principles apply:

(a) the service provider has to acknowledge receipt of the customer's order without undue delay and by electronic means,

(b) the order and the acknowledgement of receipt are deemed to be received when the parties to whom they are addressed are able to access them (Art. 11).

# 3. Legal usability of data

Data are essential raw material for speech processing algorithms, which need to be trained to discriminate between acoustically different events.

WP3 is devoted to gathering acoustic and metadata information of three different kinds: R&D data, CC data and data from public sources, to help adapt technologies currently available at research level to be usable in CCs.

In D8.2, especially in §2.2, we analysed the principles for the lawful processing of data, with particular attention to CC data, while here we focus on R&D data and data from public sources.

In the continuous effort to enrich and widen the training bases for automatic speech recognition (ASR) in BISON, it is very important to tackle the legal issues that derive from dealing with copyrighted or otherwise protected materials.

In fact, generally speaking, audiobooks, movies, radio and TV broadcasting, news, etc., which may be considered "public sources" because they are actually available to the public, cannot be deemed public in the meaning of "in the public domain" and, consequently, their use may be subject to restrictions, and prior authorisations may be required for fixing them on a support or otherwise using them.

For BISON's purposes, the legal analysis of possible infringements related to the use of protected works shall involve the detection of:

- the different kinds of works which may be used for training,
- the potential rights which may protect these works, and their duration, relevant exceptions and limitations,
- other forms of rights' restrictions set by contracts and agreements.

This section is hence aimed at addressing the correct handling of works through a systematisation derived from the relevant provisions set by:

- the Berne Convention for the Protection of Literary and Artistic Works;
- the Agreement on Trade Related Intellectual Property Rights (TRIPS, which is binding on all member states of the WTO);
- the WIPO Treaties[5] and
- Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (and subsequent modifications and supplements, hereinafter "Infosoc Directive").

First of all, it is necessary to recall what the Berne Convention means with the term "work".

According to its Article 2 "The expression "literary and artistic works" shall include every production in the literary, scientific and artistic domain, whatever may be the mode or form of its expression, such as books, pamphlets and other writings; lectures, addresses, sermons and other works of the same nature; dramatic or dramatico-musical works; choreographic works and entertainments in dumb

[5] The World Intellectual Property Organization (WIPO) administers 26 treaties on intellectual property, including the WIPO Convention. More details can be found here http://www.wipo.int/treaties/en/.

shows; musical compositions with or without words; cinematographic works to which are assimilated works expressed by a process analogous to cinematography; […]".

The copyright shall be acquired on the creation of a work that constitutes the particular expression of an intellectual effort; yet such a creation must be perceivable to the outside world regardless of the form or method adopted.

The Berne Convention states that it is up to the national legislation of Member States to prescribe whether, in general, works require fixation in some material form to be protected.

In the common law tradition, a **fixation** is required, i.e. the words must be written down or recorded in order to be protected. Thus, in the UK it may not be a copyright infringement to record an oral lecture or discussion. However, it should be observed that it may constitute a performance, in which case permission of the performer is required to record or film it. In any case, however, the act of recording is a fixation, so that permission would be required from the speakers to reproduce their work once it has been so fixated.

In the USA, common law copyright may extend to unfixed oral works, being the requirement of fixation under the Copyright Act of 1976 one that State laws are not bound to follow.

In most other countries fixation is not required, so recording an oral work always requires permission of the author. In other words, fixation is generally a matter of evidence and proof of a work, rather than a constitutive element of copyright itself.

The Berne Convention also requires copyright protection for derivative works, such as translations and adaptations, and collective works.

Thus, it seems immediately clear that an audiobook or a movie, for example, are works protected under copyright law, while other sources of speaking that may be used for ASR training purposes are perhaps not easily classifiable.

In addition, some countries extend copyright protection to works not included in the Berne Convention definition, i.e. by giving copyright protection to broadcasts as such, while in other countries these are granted "neighbouring rights"[6].

For BISON's purposes we shall temporarily limit the analysis to the speaking sources' taxonomy and their restrictions, if any.

## 3.1 Standard R&D data (licenses, usability, etc.)

It should be considered in the first instance that a large part of R&D training material is originally created especially for training purposes or is someway aimed at it from the very early project's stage.

The majority of the training material, which may be indicated as "standard R&D data", is composed by:

- non-creative/non-original works, which fall outside the scope of copyright protection and are fully and legally usable for BISON purposes: this is the case of large amounts of individuals'

[6] Also known as "related rights". See following footnote.

recorded speech, which may be freely used provided that personal data are anonymised (in compliance with data protection's law);

- creative and original works destined to the project's purposes either with the copyright owner's consent, or because the author has been specifically entrusted with creating that work: in this case the material may be freely used, nevertheless the moral right of the author must in any case be respected (e.g., with credits).

In copyright law, there is no specific exception for research purposes as such, but only for "illustration" in scientific research.

The InfoSoc Directive, Article 5 (3)(a) allows Member States to provide exceptions and limitations to the exclusive right of reproduction when the work is used "for the sole purpose of illustration for teaching or scientific research, as long as the source, including the author's name, is indicated, unless this turns out to be impossible and to the extent justified by the non-commercial purpose to be achieved".

Thus, it seems that there is no exception that may be invoked in BISON's context to use a work protected under copyright law without the owner's permission. At the same time, however, we must also consider that even if, as in the second case above and in the cases referred in the following paragraphs, a given material might actually be protected by copyright law, **its use in BISON is limited to serve as training basis for ASR systems**. As such, **this use does not compete with or prejudice the original work author's rights to economically exploit its own creations**. Then it could be affirmed that there is no conflict with the normal exploitation of the work by its author (or, if different, by the right holder) and that this does not prejudice the legitimate interests of the right holder, so that such limited use should be considered as falling outside the scope of the copyright protection.

## 3.2 Data from public sources

As mentioned above, it is important to distinguish when the training material – in abstract classifiable as "work" under copyright law – collected outside the cases analysed in the previous paragraphs is "public" because it is simply "available" or, instead, because it is "free to use".

BISON data collected from public sources may fall within the latter case – and may lawfully be used for ASR training purposes – either:

- when the term of copyright protection has expired, or
- when the author has authorised the free use (or, at least, the ASR training's specific use in BISON) of its works, or
- when the use falls in an exception set by the law or may be deemed as "fair use".

**Terms of protection of copyright and related rights**

As a general rule, copyright expires 70 years after the author's death. It has to be preliminarily determined who the author is with reference to different kinds of works, as we will see below.

As is explained more in detail in the table below, this term runs from:

- the death of the last surviving author, for works of joint ownership;
- the date of the first publication, for anonymous works or for works whose authorship cannot otherwise be established;
- from the date of first publication, in the case of collective works comprising distinguishable contributions.

As regards related rights'[7] terms of protection, the producers of phonograms, cinematographic or audiovisual works or of sequences of moving images have 50 years from the time of fixation, or from the date of the first publication or communication. For broadcasts, the term is 50 years from the first broadcast.

The term of a performer's rights is 50 years from the first performance, or from the first publication or communication.

The rights on works published or communicated to the public for the first time after copyright protection has expired last 25 years from the first lawful publication or communication to the public, or in the case of critical or scientific editions of works in the public domain, 20 years from their first lawful publication.

**Duration of copyright and related rights: the public domain**

Table 2 below summarises the terms after which the rights on different kinds of works expire and these may be freely used by anyone, as they have fallen in the so-said "public domain".

Such terms have been set at EU level by Directive 2006/116/EC of 12 December 2006 on the term of protection of copyright and certain related rights[8].

The terms shall be calculated from the first day of January of the year following the event which gives rise to them.

If the author of a work is not a Community national, and the country of origin of the work is a third country as intended by the Berne Convention[9], the term of protection granted by the Member States shall expire on the date of expiry of the protection granted in the country of origin of the work, but may not exceed the term of 70 years after the author's death.

[7] The purpose of related rights is to protect the legal interest of certain persons and legal entities who contribute to making works available to the public, or who produce subject matter which, while not qualifying as works under the copyright laws, contain sufficient creativity or technical and organisational skill to justify recognition of a copyright-like right. They are called *related* rights because they are somehow related to the protection of works of authorship under copyright. Traditionally, related rights are granted to performers, producers of phonograms and broadcasting organisations.

[8] See http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0116&from=EN.

[9] See http://www.wipo.int/treaties/en/text.jsp?file_id=283698

**Table 2 – Duration of copyright and related rights**

| Type of work/right | Duration of copyright/related rights |
|---|---|
| Works created by a single author | 70 years from the author's death, irrespective of the date when the work is lawfully made available to the public |
| Works created by multiple authors whose contributions are not distinguishable ("Joint ownership") | 70 years from the death of the last surviving author |
| Anonymous works | 70 years after the work is lawfully made available to the public |
| Pseudonymous works | 70 years after the work is lawfully made available to the public, or<br>70 years from the author's death if the author's identity is clear or if he discloses his identity |
| Works whose authorship cannot be established | 70 years after their first publication |
| Works created by multiple owners whose contributions are distinguishable ("Collective works") | 70 years after the work is lawfully made available to the public |
| Cinematographic or audiovisual works (the principal director is considered the author or co-author; Member States may designate other co-authors) | 70 years after the death of the last of the following persons (whether or not they are designated as co-authors): principal director, author of the screenplay, author of the dialogue, composer of the music specifically created for use in the work |
| Rights of performers | 50 years after the date of the performance, or<br>50 years from the date of first publication or communication to the public of the fixed performance, whichever is the earlier |
| Right of the producer of phonograms | 50 years from the date of fixation of the works. If, during this period, the work is lawfully published, 50 years after its first lawful publication or communication to the public |
| Right of producers of the first fixation of a film (cinematographic or audiovisual works or moving images, whether or not accompanied by sound) | 50 years after the fixation. If, during this period, the work is lawfully published, 50 years after its first lawful publication or communication to the public |
| Rights of broadcasting organisations | 50 years after the first transmission of a broadcast (by wire, over the air, including cable or satellite) |
| Rights on previously unpublished works, lawfully published or lawfully communicated to the public for the first time after copyright protection has expired | 25 years after lawful publication or lawful communication to the public |

**Publicly accessible works**

Conversely, a work may be still protected under copyright law, because the terms above have not expired yet, but at the same time be publicly accessible.

Right holders, i.e. authors – or those to whom authors have lawfully transferred their copyright (e.g. a publisher or a film distributor) – have the exclusive right to reproduce, modify and distribute their works. They may choose how to dispose of their rights in the way they wish and are the only ones who may authorise third parties to lawfully use their works.

Right holders may make their works available to the general public, for example, by uploading them on the Internet, a typical "public source". However, the simple accessibility of the works does not at all mean that these may be freely used for any purpose by all those who have the material possibility to download them.

In the following subsections, an exemplifying list of the different kinds of works that may be used as training material in BISON is shortly examined: Table 3 at the end of the chapter summarises the key aspects at a glance.

***A) Public performances and communication to the public***

The author of the work has the exclusive right to authorise its public performance or communication to the public; this applies both to dramatic, dramatico-musical or musical works (Berne Convention 11(1)), and the recitation of literary works (Berne 11ter), and the permission of the performer is needed to record a live performance.

Thus, if the training material consists of e.g. a recording of a reading of a book, a poem or a performance of a scene in a play, permission may be needed both from the author of the work and from those performing or reciting it.

The performer's right still applies even if the copyright on the work itself has expired.

However, it should be noted that a "performance" generally entails some special contribution, due to the skills or qualities of the performer (such as a singer or an actor), which in some way increases the artistic value of the work performed. This is unlikely to be the case if for example a lecture is simply read aloud by someone other than the author. Thus, lectures, seminar discussions and public debates are more likely to be protected as works expressed in oral form, and there would be no separate performer's right in them. **Recording of ordinary everyday casual speech is, indeed, unlikely to be treated either as a work or as a performance**.

The right to communicate to the public is essentially an extension of the performance right. It includes any means of communication to the public, or a section of the public. It covers works available on a website, webcasting, videoconferencing, etc., even if access is limited to defined users and subject to authentication.

***B) Audio or film recording***

The right on an audio or film recording covers fixations of phonograms (recordings of sounds) and first fixations of films (moving images), even if they do not constitute a "work" under copyright law.

This right belongs to the producer, normally the person (natural or legal person) who makes the investment to bring it about. This person's consent must be sought for any direct or indirect reproduction of the phonogram or film (InfoSoc Directive art. 2(c-d)).

The consent of the broadcasting organisation must be sought for any fixation of a broadcast (InfoSoc Directive art.2(e)), aside from any rights owned by the author of the work being broadcast. "Broadcast" includes wire, wireless, cable, satellite and any communication via the Internet. However, on-demand transmissions may be considered to be excluded, since they are "communications to the public" but not broadcasts (see above). Therefore, the permission of the person making available an on-demand transmission is not required to make a recording of it, although of course permission is required from the owner of the rights in the work or material transmitted (who may be the same person).

In any case, the BISON project does not presently require any reproduction of phonograms or films, nor the broadcasting of any data.

***C) Official documents***

Official documents such as legislation and decisions of all public courts and tribunals are generally not covered by copyright protection; therefore, their use is permitted without the need for prior authorisation.

This may also concern transcripts of speeches or debates in Parliament, and other parliamentary papers, as well as other official texts. In general terms, EU Member States have implemented the Article 5(3)(f) provision, which allows the "use of political speeches as well as extracts of public lectures or similar works or subject-matter to the extent justified by the informatory purpose and provided that the source, including the author's name, is indicated, except where this turns out to be impossible". In general terms, it is quite clear that this exception only covers the informatory purpose. However, a more extensive use is widely accepted, and in the BISON context it seems that the non-competitive use (see before, § 3.1) for the ASR training of these materials may be considered as not legally problematic.

It should also be noted that there may be a distinct copyright covering a compilation of official documents, and an edited version (e.g. in a court judgment) may be regarded as a new work. An example of a "new work" may be a review of all court judgements on a given subject matter, or a collection of laws regulating a given field, either annotated or not.

There is also great variation between countries as to the permission to use other material, which is considered owned by the State, e.g. geographical data, archives, etc.

***D) YouTube and contents covered by Creative Commons***

There has been criticism on the over-protection of copyright law, especially in recent years, and it still continues. It is worth pointing out that, for this reason, other systems for the distribution and diffusion of copyrighted material have begun to be adopted.

On the web, in particular, a large amount of works is licensed under open licensing schemes, like Creative Commons.

Creative Commons licenses provide a standard way for content creators to grant someone else permission to use their works.

For the BISON purposes, these licensing schemes are particularly relevant as they are used also by the YouTube platform, which allows users to mark their original videos with a Creative Commons Attribution (CC BY) license. This means that most of the works uploaded on the platform may be reproduced, shared and adapted, for any purpose, even commercial, provided that appropriate credit is given to the author.

It should be remembered that not all Creative Common licenses grant the same level of freedom to the licensee: each license should be examined with attention before using the work it pertains to. Some Creative Commons licenses, for example, prohibit the use for commercial purposes and the creation of derivative works (e.g. modification of the original work to create a new one).

However, if nothing is stated about licence terms, the default copyright rules must be considered to apply.

In any case, YouTube users are bound by the Service Terms and Conditions, which state that any content uploaded shall not contain any third party copyrighted material, or material that is subject to other third party proprietary rights (including rights of privacy or rights of publicity), unless the user has a formal licence or permission from the right holder, or is otherwise legally entitled, to post the material in question and to grant to each other YouTube user a worldwide, non-exclusive, royalty-free licence to access the uploaded material and to use, reproduce, distribute, prepare derivative works of, display and perform such material.

**Table 3 – Usability of public data**

This table refers to "usability" in the sense of any act which implies reproduction, modification or distribution of copyrighted works. In most cases, BISON technical teams instead make a simple legitimate use of the works (i.e. listening to audio content). It is in any case important to have a clear idea of what is allowed and on what conditions, in case further actions needed to be performed.

| Kind of data/material | Have IPR protection terms expired? | Reproduction/modification/distribution for BISON allowed? |
|---|---|---|
| A) Public performances and communication to the public | Yes | Yes |
| | No | Yes, with consent of the right-holder or in case of "fair use"[10], or in cases where limitations of the IP rights or exceptions are foreseen, such as for scientific research and no commercial purposes. |
| B) Audio or film recording | Yes | Yes |
| | No | Yes, with consent of the right-holder or in case of "fair use". |
| C) Official documents | Yes | Yes |
| | No | Yes for legislation and decisions of all public courts and tribunals, not covered by copyright protection.<br>Yes for parliamentary speeches/debates if limited to serve as training basis for ASR systems. |
| D) YouTube and contents covered by Creative Commons | Yes | Yes |
| | No | Default copyright rules apply but no copyrighted material shall be uploaded on YouTube or other P2P platforms.<br>For Creative Commons materials: yes, if limited to serve as training basis for ASR systems. |

[10] "Fair use" implies the possibility of a limited use of a copyrighted work without the need for permission of the right-holder. It is part of the limitations and exceptions to the exclusive rights set by the law. Examples are: commentary, search engines, criticism, parody, news reporting, research, teaching, library archiving and scholarship. It provides for the legal, unlicensed citation or incorporation of copyrighted material in another author's work based on a test checking the balance of interests.

# 4. The anonymisation process in BISON

## 4.1 General overview

As described in D8.2 §4.2, in the first stage of the BISON project the anonymisation process is performed mostly with manual procedures, both because of the limited data size and the lack of automatic tools.

The supervisor (Master Annotator) is the only person allowed to perform such anonymisation task for each CC partner, i.e. to access the full audio file and in charge of manually silencing any personal data by physically overwriting the relevant words with silence or some suitable "beep".

The anonymised call can then be passed to the annotator, who is in charge of tagging the file with keywords. The resulting annotated file is then further processed to extract statistics (features), which embed enough information to train the audio recognizers while making it impossible to reconstruct the original waveform and to trace back to the original personal data.

Besides, feature extraction from the annotated file is performed by another BISON partner (Phonexia) in the case of EBOS and COMDATA, and by TID, who also plays the role of Master Annotator, in the case of TME data. In this case, TME data are partially preprocessed, delivering to TID only the manually anonymised audio.

In the next stage of the BISON research, however, anonymisation is supposed to be mostly automated, so as to deal with big data efficiently: to this end, automatic transcription has to be added to the process. This change affects the stage where anonymisation takes place, since anonymisation is now performed on the original audio file (containing personal data) instead of on a manually pre-silenced audio file.

Moreover, this addition somehow reduces the process reliability, since no automatic transcriber can be considered 100% effective in identifying terms and items related to any possible personal data: therefore, the "anonymised" file in this case may still contain some (typically a small amount of) personal data.

Of course, any effort should be made to reduce these errors to the minimum: thus, the automatic anonymiser will be designed and trained with the greatest possible care, and tested according to the best available practices. The subsequent feature extraction helps to deal with this issue, because the extracted statistics make it impossible to reconstruct the original audio file.

Features are finally made available upon request to the BISON consortium for improving the recognisers with all languages and big data, under the requirement of signing the corresponding NDA.

In any case, as specified in D6.1 §2.4[11], data anonymisation takes place prior to the annotation of the recordings, which guarantees the full anonymisation afterwards.

After the BISON project, that is when the BISON results will enter the market, users will be allowed to anonymise personal data whenever identifying data are not needed in relation to the specific purposes of the processing, in a customisable way.

[11] D6.1 was drafted simultaneously with D8.2 (both were due in M6). Both teams of contributors kept in touch and exchanged information and feedback, with particular attention to anonymisation issues.

## 4.2 Challenges and customisation

As highlighted in D6.1 §2.4, BISON anonymisation has to be "future proof" both with respect to a continuously-evolving legal scenario and to the equally-evolving technology improvement. In addition, for the above reasons, the BISON system, including the anonymisation support, should be highly customisable.

In this context, D6.1 identified two main moments, detailed in five different situations, where anonymisation may be performed:

- during the call
    - based on specific flags in the agent's script (e.g., whenever a specific question is asked),
    - based on a specific action by an agent (for unforeseen circumstances);
- after the call
    - via manual enhancements of the recorded waveforms,
    - via feedback coming from the speech analytics (i.e., when the analytics spots a certain keyword and returns this feedback),
    - as a result of data-mining actions on the text-format (after a full transcription of the recorded voice files).

The combination of these five situations should make it possible to effectively support the optimisation of the anonymisation over time, taking maximal advantage of the evolution of new technology, while keeping in sync with the changing legal framework. The configuration of such options should be possible, in any case, only for some suitably-enabled users of the BISON platform.

## 4.3 Technological requirements

Although BISON is supposed to rely on automatic anonymisation, some manual adjustments are to be expected in the development and configuration phases. For this reason, automatic technologies (mainly based on KWS and speech mining) need to be coupled with some interactive tool, enabling the fine-tuning of the anonymisation process.

This is why a web-based *Recording Management Tool* is introduced in the smallBISON architecture presented in D6.1 §4.1: its purpose is to manage the recording environment, including the anonymisation actions. The Graphical User Interface, outlined in the mock shown in §4.2, is supposed to support the creation of user accounts with the corresponding restrictions – including viewing/edit rights and the suitable anonymisation options, which shall need to be better defined on a case-by-case basis in relation to the actual needs and the applicable legal framework.

The whole tool will be protected with adequate security measures, operating under a Virtual Private Network with suitable role-based authentication mechanisms.

In particular, in order to effectively support the above-mentioned manual fine-tuning, the *live monitoring* feature of this tool (§5.2.1) is expected to include a "quick anonymise" feature (reserved to the supervisor), who triggers on-the-fly anonymisation in the case that information is heard that needs to be anonymised but was not previously detected. As a consequence, the subsequent management of such "manually added anonymisation" is also foreseen (§5.2.3).

The *Contact Center API* introduced in D6.1 §4.3 also considers the management of anonymised recordings, assuming the presence of methods to access anonymised recordings (with proper restrictions) as well as to support their playback and export.

## 4.4 Legal analysis

The current legal framework foresees a set of essential principles that should inspire the design and development of any law-abiding information system processing personal data.

While some of such principles derive directly from the Data Protection Directive (namely, from the "Principles relating to data quality"), others concern the security measures that should be adopted, particularly, as concerns the "Security of processing". These principles are further strengthened and detailed in the forthcoming "Proposal for a General Data Protection Regulation".

The following list summarises such principles, which are all relevant for the BISON project:

***Principles about data protection and processing***

- Principle of lawfulness and fairness: any processing of personal data must be *lawful* and *fair* to the individuals concerned
- Principle of relevance and non-excessive use: personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed
- Principle of purpose: personal data must be collected for *specified, explicit* and *legitimate purposes* and *not further processed in a way incompatible with those purposes*
- Principle of accuracy: data must be *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;
- Principle of data retention: data must also be *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*.

***Principles about security measures***

- Principle of Privacy by design: the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that *appropriate technical and organisational measures be taken, both at the time of the design* of the processing system and *at the time of the processing itself*, particularly in order to *maintain security* and thereby to *prevent any unauthorized processing*; these measures must ensure *an appropriate level of security*, taking into account the *state of the art* and *the costs of their implementation* in relation to the risks inherent in the processing and the nature of the data to be protected.
- Principle of appropriateness of the security measures: the controller must implement *appropriate technical and organisational 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.

- Principle of Privacy by default: the controller shall implement mechanisms for *ensuring that, by default, only those personal data are processed which are necessary for each specific purpose* of the processing and are *especially not collected or retained beyond the minimum necessary* to achieve those purposes, both in terms of the *amount* of the data and the *time* of their storage. In particular, those mechanisms *shall ensure that by default personal data are not made accessible to an indefinite number of individuals*.

***Other relevant principles***

- Principle of least privilege (also known as the Principle of minimal privilege): in a given abstraction layer of a computing environment, every module (process, user, program) must be able to access only the information and resources that are necessary for its legitimate purpose.
- Principle of intentionality in performing any [critical] action – especially an action which is suitable to reduce the security level: examples include granting access to a wider set of users, selecting lower security settings, exporting data, reducing the number of anonymised items, etc.

***Consequences on the BISON system***

In the context of the BISON project, and in particular of the management of recordings and their anonymisation, these principles translate into actual system requirements ranging from the system configuration to the user management, the way data are processed, and the security measures in general.

Abstracting from any specific technical solution, the following issues can be identified at this stage:

1. Different user groups and different users, with different privileges and access rights, should be accounted for, so that each user is granted only the *minimum* set of rights that is *necessary* for his/her task, coupling maximum flexibility with maximum security → Consequences: role-based authentication model, fine-grained set of user rights, adequate authentication mechanisms
2. *Default* user profiles with the *minimum* set of rights, so that any addition of user rights giving access to data is always *intentional*
3. *Default* anonymisation configuration corresponding to the *maximum* level of anonymisation, so that any custom configuration implying a decrease of anonymisation level is always *explicitly authorised* and therefore *intentional and security-checked* before proceeding
4. Adequate support of *detailed* customised anonymisation levels, so that the system settings can be *fine-tuned to the specific customer necessity* – and no further

5. Multiple levels of security, with proper *warnings*, whenever the default (i.e., maximum security) settings are lowered for any reason (e.g. during the custom configuration by authorised and suitably authenticated personnel)
6. Clear identification of the use-case scenarios when (authorised) personnel is allowed to access personal data – that is, non-anonymised copies of recordings, lawfully stored for authorised processing
7. Severe restrictions on, or even denial of, *export* of non-anonymised data
8. Immediate removal of non-anonymised copies of data recordings that may have been made during the processing, if required by the processing itself, as soon as their presence is no longer required.

# 5. BISON ethical and societal issues

In D8.2 §6 we provided a first general outline of the main ethical and societal issues connected with biometric big speech data processing.

This section aims to examine more thoroughly ethical and social challenges when dealing with big data and provides a first guidance on how to comply with ethical principles when implementing big data initiatives, such as BISON.

## 5.1 Ethical issues

### 5.1.1 Big data and ethical issues

The automated processing of large amounts of data (so-called "big data"[12]) – such as the one BISON intends to carry out – requires considerations that go beyond the mere analysis of legal compliance, but also involve ethical issues (see D8.2, § 6).

Big data have indeed two fundamental characteristics:

1) the ability to generate new data other than those communicated by the data subject and of which he is aware; and
2) the volume of data used can be vastly greater than the one found in traditional structured databases.

The first characteristic makes it possible to derive new insights and predict outcomes concerning the needs and the behaviour of people. This results often in the use of big data for purposes different from those for which the data were obtained at the time they were initially collected. This change of purpose with regard to the use of data may create problems because each person should have full control of the personal data concerning him and should have notice of the use that others make of these data and freedom of choice. Persons should be informed on the way a company will use and share their personal information and be provided a meaningful choice with respect to such use and sharing.

Therefore, it is important that companies define what purposes they intend to pursue before collecting personal data and give prior notice to the data subject. They cannot change such purposes without first communicating this to the data subject and obtaining his consent.

Moreover, the information notice should be drafted in a clear and simple language, and should be designed to inform not only about the purposes but also about the logic behind the processing of big data; finally, the subject data should always be given the possibility to exercise his rights as set by the law.

[12] For an analysis of the issues related to big data, see: Danah Boyd-Kate Crawford,"*Six Provocations for Big Data*", 2011, available at http://ssrn.com/abstract=1926431 and Giuseppe D'Acquisto-Josep Domingo Ferrer-Panayiotis Kikiras-Vicenç Torra-Yves Alexandre de Montjoye-Athena Bourka, "*Privacy by design in big data. An overview of privacy enhancing technologies in the era of big data analytics*", 2015, available at https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/big-data-protection/

The second characteristic of big data that makes them different from traditional structured data is the sheer volume of the data.

Persons should be able to know what information a company collects about them so that they can effectively have the possibility to choose how that information is used. With a single database containing a manageable amount of information, this may not be too difficult. If, however, the dataset resides over multiple databases, and perhaps even with third-party data processors, providing the data subject with access, choice, and transparency may be difficult.

Therefore, companies should design their big data initiatives with the ability to provide access, choice, and transparency to data subjects.

The automatic application of predefined inference rules to a massive amount of data also determines a potential inaccuracy in the realisation of the "profile" of the data subject, which can distort and possibly compromise a person's identity.

From this point of view, it is therefore important to ensure access to information and transparency as concerns the expected effects of the attribution of a "profile" to the individual data subject: data should always be checked and updated, so as to ensure their high quality. Operators should be trained in order to provide clear answers to requests for information by the data subjects and to react promptly to any requests for correcting the data.

The following Table 4 summarises the main ethical issues and the appropriate conduct which should be adopted.

**Table 4 – Ethical issues – appropriate conduct and precautions**

| Ethical Issues | Details | Appropriate Conduct | Precautions |
|---|---|---|---|
| Change in purpose | Big data processed for purposes different from those for which they were obtained | - Preventive definition of purposes<br>- Prior notice of purposes<br>- Compliance with the identified purposes<br>- Use of personal data for different purposes only with informed and prior consent of the data subject<br>- Information on the logic behind the processing of big data<br>- Ensure access to data by the data subject (transparency) | - Use clear and simple language<br>- Avoid use of data not relevant to the declared purposes |
| Difficulty of access and transparency | If the dataset resides in multiple databases, possibly also at third-party data processors', providing the data subject with access, choice, and transparency can be difficult | - Design big data initiatives with the ability to provide access, choice, and transparency to data subjects | - Design and configure IT Technologies to allow for easier access<br>- Inform data subjects about the location of their personal data<br>- Connect different databases with appropriate agreements<br>- Provide information in a plain and simple way |
| Possible distortion of a person's identity | Potential inaccuracy in the definition of the data subject's "profile" | - Correct or delete inaccurate information (quality of data)<br>- Access to information and transparency on the expected effects of the attribution of the "profile" | - Training of operators |

### 5.1.2 Big data and BISON ethical approach

The challenge of "data protection" is to use personal data and protect them at the same time.

The intention of BISON is to protect personal data in the belief that this is necessary for the satisfaction of the data subjects.

The automatic processing of big data allows to customise, improve and speed up services. The choice BISON has made is to aim at achieving these objectives – accessible thanks to technological progress – both for the benefit of the data subjects and to ensure maximum transparency in the data processing and control over their data.

A real ethical sensitivity is demonstrated by the clarity and the concrete effort to minimize any issues, making sure that the benefits to data subjects always outweigh the potential costs.

This is based on the fact that higher customer satisfaction can be transformed from cost to a strategic opportunity, because it can be a competitive advantage for the company in terms of customer loyalty and greater ability to attract new customers.

### 5.1.3 Ethical commitments of the Universities and CC partners: schematic table

In the previous deliverables (see in particular D.8.1, § 3 and § 5; D.8.2, § 6) we highlighted the ethical commitments of the Universities and CC partners. They are reproduced in Table 5, with an integration by Telefónica Móviles which is better discussed below.

**Table 5 – Ethical commitments and principles of BISON partners**

| Partners | Ethical commitments | Main principles |
|---|---|---|
| ALL | - Lawfulness; | - See D.8.3, §2 |
| ALL | - The European Code of Conduct for Research Integrity | - Honesty in presenting research goals and intentions, in precise and nuanced reporting on research methods and procedures, and in conveying valid interpretations and justifiable claims with respect to possible applications of research results<br>- reliability in performing research (meticulous, careful and attentive to detail), and in communication of the results (fair and full and unbiased reporting)<br>- objectivity: interpretations and conclusions must be founded on facts and data able to stand the test of proof and secondary review; there should be transparency in the collection, analysis and interpretation of data, and verifiability of the scientific reasoning<br>- impartiality and independence from |

| | | |
|---|---|---|
| | | commissioning or interested parties, from ideological or political pressure groups, and from economic or financial interests<br>- open communication, in discussing the work with other scientists, in contributing to public knowledge through publication of the findings, in honest communication to the general public. This openness presupposes a proper storage and availability of data, and accessibility for interested colleagues<br>- duty of care for participants in and the subjects of research, be they human beings, animals, the environment or cultural objects. Research on human subjects and animals should always rest on the principles of respect and duty of care<br>- fairness, in providing proper references and giving due credits to the work of others, in treating colleagues with integrity and honesty<br>- responsibility for future science generations. The education of young scientists and scholars requires binding standards for mentorship and supervision<br>- data practices, including data management and storage, placing data at the disposal of colleagues who want to replicate the findings, adequate preservation of original data<br>- research procedures. Deviations from desired practices include insufficient care for research subjects, insufficient respect of human subjects, animals, the environment, or cultural heritage; violation of protocols; failure to obtain informed consent; insufficient privacy protection; or breach of trust (e.g. confidentiality). Improper research design, carelessness in experimentation and calculations that lead to gross errors, although the partition-wall between incompetence and dishonesty may be rather thin here<br>- publication-related conduct, including authorship practices. It is unacceptable to claim or grant undeserved authorship and to deny deserved |

| | | |
|---|---|---|
| | | authorship, or to inadequately allocate credit. Breaching of publishing rules, such as repeated publication, salami-slicing of publication, or a too long delay in publication, or insufficient acknowledgement of contributors or sponsors, fall within this category as well<br>- reviewing of scientific publications with independence and without conflict of interests, personal bias and rivalry, no appropriation of ideas |
| BUT | - The Magna Charta Universitatum<br>- The Code of Ethics for Researchers of the Czech Academy of Sciences<br>- The BUT Ethical Code | - Academic freedom and institutional autonomy<br>- Respect of the historical rules of the academic community such as openness, fairness, international relations, etc.<br>- Provision to the university community of freedom of research and promotion of international collaboration |
| UNIBO | - The Magna Charta Universitatum<br>- The European Charter for Researchers and the Code of Conduct for the Recruitment of Researchers<br>- The Bologna University Code of Ethics and Conduct | - Academic freedom and institutional autonomy<br>- Recognition of and compliance with personal rights and freedoms, as well as acceptance of ethical and social duties and responsibilities towards the own institution<br>- Excellence in research and the applications of inventions as fundamental elements for the progress of the whole community and for the improvement of the quality of life<br>- Provision of the university community with freedom of research and promotion of international collaboration |
| ComData | - Code of Conduct, endorsed by the Direct Marketing and Mail Order Trade Association | - Contribute to the protection of customer or consumer<br>- Protect the interests of association members against business entities with questionable business activities to the detriment of the whole industry<br>- Protect the good name of direct marketing, mail order and the reputation of the whole Association<br>- Provide quality and telemarketing staff training<br>- Ensure control of telemarketing operations |

| | | |
|---|---|---|
| | | - Ensure the accuracy and correctness of the telephone call<br>- Ensure the accuracy of the data recorded as results of telephone marketing<br>- Prohibit to conceal the telephone marketing purpose of the call, especially by pretending another purpose is being pursued or begin the call with misleading words |
| Telefónica Móviles | - Digital Manifesto<br>- Telefónica´s Code of Ethics | - Build Digital Confidence through a safer Internet experience and by empowering citizens to be in control of their personal data<br>- Create a Portable Digital Life for consumers by allowing them to use their data, information and applications regardless of their devices or platform<br>- Open up mobile Operating Systems, App Stores and other digital platforms to increase users' freedom, choice and competition<br>- Promote interoperable Internet applications, communication and messaging services to improve consumer experience and foster competition<br>- Improve transparency about the conditions of use for Internet services and the distinction between information and advertisement in online search results<br>- Create fairer policy frameworks by establishing the same rules for the same digital services and smarter regulation by relying more on outcome-based policy making and case-by-case supervision<br>- Make Internet available to everyone by establishing adequate conditions for private investment in broadband infrastructure<br>- Evolve the policy models of Global Internet Governance by building on its existing foundations and through the involvement of all stakeholders in an open manner and on equal footing<br>- Protect the confidentiality of any information, |

| | | |
|---|---|---|
| | | whether it is about employees, the company, customers, shareholders or suppliers<br>- Make customers, employees, shareholders, suppliers and partners know how Telefónica uses and stores their personal information. Also tell them how they can access it if they need to change it<br>- Keep that information secure. If security is ever compromised, act quickly and responsibly<br>- Avoid all forms of bribery. Do not permit promising, offering or giving any benefit or advantage of any nature to persons, to influence any kind of decisions (including official, administrative or judicial decisions) or obtain improper advantages for the company<br>- Respect the principles of the UN Universal Declaration of Human Rights, as well as the declarations of the International Labour Organisation<br>- Provide employees and partners with a safe working environment; establish suitable mechanisms to avoid workplace accidents, injuries or diseases associated with work activity through strict compliance with all relevant regulations and the preventive management of workplace hazards<br>- Offer customers high-quality products and services, which are innovative, reliable and reasonably priced; verify and ensure that products comply with manufacturing standards on safety and quality; disclose and resolve any instances in which health risks are detected<br>- Always provide customers with truthful, clear, practical and precise information when marketing products; make sure those products comply with all the required and advertised specifications; provide all the information needed to satisfy customers if they are ever unhappy with products and services<br>- Contribute to the technological and economic development of society, investing in |

| | | |
|---|---|---|
| | | telecommunications infrastructures, creating jobs and developing products and services<br>- Commit to sustainable development, protect the environment and reduce any negative impact. |
| EBOS | - Certificate of compliance with EN 15838[13] | - Establish procedures and responsibilities on protecting customers' privacy<br>- Make information on the handling of complaints readily available to customers and other interested parties<br>- Analyse the results from process quality monitoring and take appropriate action, in order to prevent unacceptable service delivery<br>- Ensure minimisation of mistakes in the processing of the contact or in the previously agreed output of the contact<br>- Provide back-up systems to replicate and restore data in the event of any malfunction outage or failures leading to data loss and to respond to any requirements agreed with the client organisation<br>- Create a working environment which promotes health, effectiveness and well-being of the employees<br>- Establish clear procedures on protecting CC agents' privacy regarding monitored data<br>- Establish performance indicators for CC agents, such as quality objectives, which are clear and comprehensible for each individual agent. |

***Addendum on Telefónica Móviles***

Telefónica Móviles approach to ethics deserves some further observations: the company has adopted a set of guidelines which steer its day to day activities and define how to develop its business ("Telefónica's Code of Ethics")[14].

Approved in December 2006, they apply to all employees and in all countries in which Telefónica Móviles operates. They are structured into the following General Principles:

[13] UNI Certification which sets parameters for service requirements provided by contact centers.

[14] See http://www.telefonica.com/en/about_telefonica/html/strategy/principactua.shtml and http://www.telefonica.com/en/about_telefonica/pdf/OurBusinessPrinciples.pdf

- honesty and trust,
- respect for the law,
- integrity,
- respect for human rights.

These are further detailed into other more specific principles in order to guarantee the trust of clients, staff, shareholders, suppliers and the society in general.

A confidential help channel allows Telefónica's staff to request guidance and ask questions associated with the compliance with the operational principles, especially when they observe cases of non-compliance.

Telefónica transmits the operational principles of responsible business contained in "Telefónica's Code of Ethics" to all of professional staff by means of a compulsory online training course. This training makes it possible to reflect on the importance of having ethical standards which help Telefónica perform its operational activities.

## 5.2 Societal issues

### 5.2.1 Big data and societal issues

The automated processing of large amounts of data poses several issues not only of ethical, but also of societal nature. It is therefore necessary to evaluate the impact of research both in terms of scientific progress and also of human dignity and socio-cultural fallout (see D8.2, § 6).

Relevant social issues that need to be investigated for BISON have been identified and will be outlined below.

1. ***Social exclusion and discrimination***

(a) The automatic processing of big data makes it possible – starting from data provided by the data subject - to generate further new data and create a trusted "profile" of an individual (see § 6.1.1).

This potential may, however, give rise to potential discriminations when someone decides to exclude some persons because they belong to certain groups (the elderly, persons with disabilities, persons of certain races or religious beliefs, or belonging to certain political parties, etc.).

It should also be considered that biometric data (such as speech) may disclose mental and physical conditions of a person thus leading to socially unwanted consequences if mishandled.

(b) Social exclusion can also be linked to the difficulty in accessing and being able to use certain technologies, such as Internet connection by certain categories of persons (e.g. the elderly, persons with disabilities or with low income, etc.). This prevents them from benefitting from new technologies and creates a widening knowledge gap between disadvantaged persons and the rest of the population.

2. ***Impact on the trust relationship between citizens and the Government***

The ability of companies to "know everything" about consumers - through the use of technological tools - can indirectly damage the trust relationship between citizens and the Government. Citizens may indeed believe that the Government does not protect their interests, leaving them at the mercy of companies (considered as the true "strong" subjects).

This may have a negative impact because the civil and peaceful living of social communities is based on the trust relationship between citizens and the Government.

3. ***Risk of erosion of civil liberties***

Building a "profile" of people (e.g. CC clients, Internet users, on-line consumers etc.) may reduce their freedom of choice. For example, commercial offers might always and only refer to certain categories of products – e.g., those that do not exceed a certain economic value – because the person belongs to a low-income category.

In order to customize services (benefit must be pursued), companies may therefore get to "cage" the consumer within the "categories" in which he is inserted, without the possibility of changing.

This would translate into a reduction of freedom of choice of the person but also, more in general, of the right to knowledge and self-determination.

4. ***Excessive control of the Government over the individuals***

The automated processing of big data may give rise to the temptation from part of the Government to exercise too much control over the individuals.

In this context, the Convention for the Protection of Human Rights and Fundamental Freedoms establishes that there shall be no interference by a public authority with the exercise of the right to the respect of private and family life "except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others" (art. 8)[15].

### 5.2.2 Big data and BISON social approach

To reduce the possible social issues regarding the automatic processing of big data, the following four main categories of actions may be identified.

1. ***Transparency***

Transparency about the activities is definitely the main action to be taken.

In particular, CCs should provide the following information to data subjects in a simple and clear way before the data collection:

[15] See http://www.echr.coe.int/Documents/Convention_ENG.pdf

a) that their data will be used in the context of profiling;
b) the purposes for which the profiling is carried out;
c) the categories of personal data used;
d) the identity of the controller and, if necessary, its representative;
e) the existence of appropriate safeguards;
f) all information that is necessary for guaranteeing the fairness of recourse to profiling, such as:
   - the categories of persons or bodies to whom or to which personal data may be communicated, and the purposes for doing so;
   - the possibility, where appropriate, for data subjects to refuse or withdraw consent and the consequences of withdrawal;
   - the conditions of exercise of the right of access, objection or correction, as well as the right to bring a complaint before the competent authorities;
   - the persons from whom or bodies from which the personal data are or will be collected;
   - the compulsory or optional nature of the reply to the questions used for personal data collection and the consequences of not replying for the data subjects;
   - the duration of storage;
   - the envisaged effects of the attribution of the profile to the data subject.

To this it should be added that the data subject who is being, or has been, profiled should be entitled to obtain from the controller, at his request, within a reasonable time and in an understandable form, information concerning:

a) his personal data;
b) the logic underpinning the processing of his personal data and that was used to attribute a profile to him, at least in the case of an automated decision;
c) the purposes for which the profiling was carried out and the categories of persons to whom or bodies to which the personal data may be communicated.

2. ***Data quality***

Appropriate measures should be taken by the controller to correct data inaccuracy factors and limit the risks of errors inherent in profiling.

The controller should periodically and within a reasonable time re-evaluate the quality of the data and of the statistical inferences used.

Data subjects should be entitled to the correction, deletion or blocking of their personal data.

3. ***Data security***

Appropriate technical and organisational measures should be taken to ensure the protection of personal data, to guard against accidental or unlawful destruction and accidental loss, as well as unauthorised access, alteration, communication or any other form of unlawful processing.

These measures should ensure a proper standard of data security having regard to the technical state of the art and also to the sensitive nature of the personal data collected and processed in the context of profiling, and evaluating the potential risks; they should be reviewed periodically and within a reasonable time.

Suitable measures should be introduced to guard against any possibility that the anonymous and aggregated statistical results used in profiling may result in the re-identification of the data subjects.

4. ***Equality and fairness***

The protection of fundamental rights and freedoms should also include the respect of the principle of non-discrimination; this shall be guaranteed during the collection and processing of personal data.

The enjoyment of the rights and freedoms shall be secured without discrimination on any ground such as sex, race, colour, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status[16].

Table 6 below schematises the relevant social issues, the categories of actions which may be taken and connects also with the considerations made in D.8.2 § 6.2.

**Table 6 –Social issues, actions and considerations**

| Social Issues | Categories of actions | Considerations |
|---|---|---|
| Social exclusion and discrimination | - Equality and fairness<br>- Transparency | - *Social inclusion* – CCs are one of the rare industries where workers with disabilities can find jobs and integrate into the society: therefore, by strengthening this industry, BISON indirectly promotes the inclusion of citizens with disabilities into a normal working environment, without unnecessary (and possibly embarrassing) charity measures<br>- *Reduction of work monotony* – while CC agents' work today is mostly monotonous, the new scenarios made possible by BISON can reduce this effect and promote the development of new, higher-level skills<br>- *Reduction of work stress and agents' control* – BISON strongly reduces the need for a call to be audited by a human supervisor, thus |

[16] See Art. 14 "Prohibition of discrimination" of Convention for the Protection of Human Rights and Fundamental Freedoms, Rome - 04.11.1950. Available at http://www.echr.coe.int/Documents/Convention_ENG.pdf.

| | | |
|---|---|---|
| | | indirectly checking the agent's way of working; more transparent and uniform control procedures are introduced<br>- *Improvement of the chances for teleworking* – thanks to the support for agent supervision also in distributed CCs, BISON could make it easier for CCs to accept teleworking, with a positive impact on workers' life, especially for women (reducing the need to commute, making life easier for mothers with kids, etc.)<br>- *Indirect improvement of job stability* – by strengthening the CCs competitivity and improving work conditions, the volatility of agents' jobs should be expected to decrease |
| Impact on the trust relationship between citizens and the Government | - Trasparency<br>- Data quality<br>- Data security | - *Respect of the rights of the citizen "by design"* – the creation of a system that takes into account the rights of people from the earliest design phases can increase the perception by the citizen to be protected by the Government |
| Risk of erosion of civil liberties | - Trasparency<br>- Data quality | - *Better control of personal data by the data subject* – an automated management of personal data allows the possibility of immediate control by data subject (e.g. correction of data, knowledge of the purposes of the processing, etc.) |
| Excessive control of the Government over the individuals | - Trasparency<br>- Data security | - *Specific purpose of data processing* – an automatic system for data processing designed for certain purposes can reduce the possibility of using the data for different purposes |

# 6. Practical support to partners

In the context of our WP8 tasks as foreseen by the DoW, we have interpreted our role in a broad sense, i.e. by discussing with technical partners legal issues arisen during day by day BISON design and development activities and providing specific legal support on BISON-related issues whenever needed.

This Section briefly outlines some issues which have been discussed and analysed together with BISON partners and some support activities provided.

## 6.1 Instructions for annotators

Annotation activities are the first ring of the BISON chain and need to be performed with the utmost accuracy, in particular as concerns anonymisation, so as to ensure privacy and data protection.

D3.1 "Data planning and management I" (delivered in M3) summarised the initial planning of data collection and annotation in BISON and provided detailed instructions for annotators, together with a scheme for checking the quality of annotations.

The instructions for annotators have been drafted in the form of an annotation manual and a quick help table, both enclosed to D3.1 as Appendix 1.

According to the manual, annotators have to transcribe speech literally, omitting nothing, with the aid of the Transcriber application.

The section of the manual that is relevant from the legal viewpoint is "Sequence containing information which should be abolished", which instructs annotators on how they should mark "sensitive information"[17].

The instructions tell annotators what information is to be regarded to as "sensitive data" and must be marked, that is: "generally all information that enables to identify the speaker or significantly narrows the range of people among whom the speaker could be located. It concerns mainly: family names associated with first name, address, phone numbers, account numbers, document numbers, social security numbers, etc." and add that "Some information may not be sensitive alone, but in the context of other information in the record may lead to the identification of the speaker, so it is need to take into consideration the whole record".

This content is correct in legal terms, albeit referred to "common" personal data. These are actually defined by the Data Protection Directive as "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".

Thus, it is basically a matter of terminology: in a broad, common language sense, much information may be deemed "sensitive". For example, a credit card number is very sensitive for its owner and

[17] See Phonexia "Speech Transcription Manual", pag. 7.

needs to be kept secret. However, the concept of sensitivity of data, as foreseen by the law, is different.

Sensitive data are a special category of data and according to the Data Protection Directive they include "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".

In subsequent, updated versions of the instructions, which may be enclosed to forthcoming Deliverable 3.2 "Data planning and management II", due in M15, a refinement of this provision may be agreed upon, so as to clarify:

- the concept of common personal data – which need to be detected, marked and deleted;
- the concept of sensitive data, which not only need to be deleted but to which a special attention should be paid;
- the fact that not only directly identifying data should be considered but also data which may indirectly identify a data subject, also based on a connection with data processed in other databases, also owned by third parties.

The following table summarises the main characteristics of the different types of personal data.

**Table 7 – Exemplification of personal data features**

| Type of personal data | Characteristics | Examples |
|---|---|---|
| Common personal data | - Any information that may identify a natural person which is not sensitive<br>- Direct or indirect identification<br>- Identification through ID number<br>- Identification through any factor relating to physical, physiological, mental, economic, cultural or social identity | - First and last name<br>- Telephone number<br>- E-mail<br>- VAT number<br>- Fidelity card number<br>- Social security number<br>- Fiscal code<br>- Credit card number |
| Sensitive personal data | Data which may reveal special conditions of a natural person:<br>- racial or ethnic origin<br>- political opinions<br>- religious beliefs<br>- philosophical beliefs<br>- trade-union membership<br>- health<br>- sex life | - Medical record<br>- Membership of a political party<br>- Membership of a trade union<br>- Belonging to a religious community<br>- Being part of the LGBT community |

## 6.2 MyForce anonymisation procedures – legal analysis

In the above sections, we discussed the set of essential principles at the roots of the EU legal framework which constitute the basis for design and development of any law-abiding information system processing personal data – independently of the specific technical solution and of the devised system architecture.

In the context of the BISON project, such principles are especially relevant for the management of recordings and their anonymisation: for this reason, we have also discussed how they translate into actual system requirements concerning, in particular, the system configuration and customisation, user rights and user management, and security measures in general.

In the following table we summarise how such requirements have influenced the design and implementation of the smallBISON prototype (and in perspective of the subsequent bigBISON), developed by MyForce.

**Table 8 – Legal principles and their impact onto the BISON design**

| Principle | Impact on BISON design |
|---|---|
| Principle of lawfulness and fairness | ▪ Need for the BISON system to abide not only by the applicable law but also by wider principles of correctness (e.g. if informed user consent has been provided for the specific purposes, etc.) |
| Principle of relevance and no excess of data | ▪ Unnecessary data should not be collected (and if collected unintentionally, should be removed as fast and easily as possible)<br>▪ [Manual anonymisation support] If previously enabled by the manager/administrator, an agent can manually start/stop anonymisation "on the fly" so as to guarantee that only relevant data are actually recorded (e.g. to cope with the customer saying unexpected personal data in a non-standard way)<br>▪ CC Operators should be guided by the BISON system not to request non-pertaining data or excessive data |
| Principle of purpose | ▪ Data are collected for the purposes explained in the data protection information and consent forms and only processed for such purposes<br>▪ BISON should enable CC operators to be aware of the specific purposes for which consent has been given by the customer (data subject) |
| Principle of necessity | ▪ [Export] Export of non-totally anonymised data is not only restricted to selected power users with proper rights, but subject to different *export levels* corresponding to different access limitations, so that access to data is always allowed only when strictly necessary<br>▪ [Deletion of unnecessary data copies] Should a recording be copied from the recording server to a different speech server for processing, this copy is immediately deleted from the speech server after use (that is, after keyword analysis) |

| | |
|---|---|
| Principle of data retention | ▪ [Anonymisation] Data are anonymised as soon as possible in the process chain ("[…] keep in a form which permits identification of data subjects for no longer than is necessary") |
| Principle of Privacy by design | ▪ [User rights] Only the personnel who is directly involved in data management is authorised to access data, and only for the specific purpose<br>▪ [Automatic anonymisation support] Anonymisation parameters can be added to selected parts of a call-script (e.g. input buttons, screens, etc.) to configure the automatic fire of anonymisation triggers<br>▪ [Automatic anonymisation support] Anonymisation keywords/phrases can be added to the speech engine so that such parts are automatically flagged<br>▪ [Manual anonymisation support] Switching off a given privacy flag in the Recording Management Tool automatically triggers the application of the "immediately lower" security flag<br>▪ [Manual anonymisation support] If even the last privacy flag in the Recording Management Tool is switched off, custom security profiles, leading to custom "anonymisation levels", will apply (these can be configured only by the supervisors and the system administrator)<br>▪ [Export] Disabling the default export setting (which only allows anonymised files to be exported), thus enabling some non-totally-anonymised recordings to be exported, causes the automatic application of *anonymisation profiles* that restrict the access to anonymisation functions to selected power users<br>▪ [Export] When an enabled power user accesses the export function to export possibly-non-anonymised recordings, an *export level menu* will appear (with the lowest setting selected by default)<br>▪ [Export] The *export levels* also imply different restrictions on who can access the exported data (for instance, only users with an access level not lower than the user who exported the data could listen to the exported file) |
| Principle of Privacy by default | ▪ [Anonymisation] "Anonymise everything" is the default setting after software installation<br>▪ [Anonymisation] If the "Anonymise everything" flag is turned off (potentially allowing for non-totally-anonymised files to be produced), a new security setting is automatically activated which allows users to *listen only to anonymised recordings* (automatic protection)<br>▪ [Export] A system-wide default setting normally permits only anonymised data to be exported<br>▪ [Export] When an enabled power user accesses the export function to export possibly-non-anonymised recordings, the *export level menu* which appears is pre-set on the lowest setting by default |

| | |
|---|---|
| Principle of appropriateness of the security measures | ▪ [Secure communication] Web-based tools are secured via a Virtual Private Network<br>▪ [User rights] Role-based authentication mechanisms are put in place to control user access on a fine-grain and strict-necessity basis<br>▪ [User rights] User *restriction profiles* allow for maximum flexibility in granting each user/user group the exact amount of access rights required for the specific purpose, based on a very specific set of *restriction parameters*<br>▪ [User rights] Unlimited restriction profiles can be defined so as to tune the system to each possible desired configuration, following the customer's specific internal organisation and needs<br>▪ [User rights] Hierarchy of users make it possible to grant each user exactly the rights to do his job<br>▪ [Storage security] Original recordings (with personal data) are stored in a secure database<br>▪ [Export] Exporting non-totally anonymised recordings is only possible to selected power users and only after explicitly disabling the default export flag<br>▪ [Export] Manually increasing the *export level* of the export menu is only possible for users whose *anonymisation profile* explicitly allows for this action<br>▪ [Manual anonymisation support] The manager/administrator can decide that something else should be anonymised, in addition to the already-performed procedure (possibly to cope with a human fault or some system error)<br>▪ [Manual anonymisation support] An agent can manually start/stop anonymisation "on the fly" (possibly to cope with the customer saying unexpected personal data in a non-standard way) *only* if previously enabled by the manager/administrator<br>▪ [Logging] To strengthen the security level around the *Supervisor module*, any action of any user using such a module is automatically logged |
| Principle of least privilege | ▪ [User rights] Role-based authentication mechanisms are put in place to control user access on a fine-grain and strict-necessity basis<br>▪ [User rights] User *restriction profiles* allow for maximum flexibility in granting each user/user group the exact amount of access rights required for the specific purpose, based on a very specific set of *restriction parameters*<br>▪ [User rights] Even inside the supervisors/administrators groups, supervisors never get general, unrestricted access rights – the set of rights is always tuned to the specific task, e.g.:<br>o supervisors are not enabled to listen to anonymised parts of |

| | |
|---|---|
| | the recordings, or may be enabled only in selected cases like when the anonymisation was manually forced by the agent during a call, or conversely when the anonymisation was performed automatically, and so on<br>○ a supervisor may be unable to listen to anonymised parts of a recording even if he was the person who enabled the agent (who actually handled the call) to perform manual anonymisations<br>▪ [User rights] An agent only has the specific rights his supervisor/administrator has defined for him<br>▪ [User rights] Hierarchy of users make it possible to grant each user exactly the rights to do his job. |
| Principle of intentionality | ▪ [Anonymisation] The "Anonymise everything" and "listen only to anonymised recordings" flags must each be turned off explicitly<br>▪ [Export] Exporting non-totally anonymised recordings is only possible (to selected power users) only after explicitly disabling the default export flag<br>▪ [Export] When an enabled power user accesses the export function to export possibly-non-anonymised recordings, selecting an *export level* other than the lowest (default) requires an explicit user action<br>▪ [Export] Manually increasing the *export level* of the above menu generates appropriate warnings, asking for explicit confirmation of critical actions |

## 6.3 CC contracts analysis

A relevant part of the data needed for BISON training and development comes from partner CCs, as they have access to a wealth of speech recordings from their day to day business activities.

However, as we have discussed together with the partners, such information may not all be freely usable and a case by case analysis needs to be performed.

As concerns the BISON project, this issue has been solved, in that all personal data used during project lifetime will be fully anonymised. This decision has also been taken in consideration of the legal principle of necessity: personal data shall be processed only when strictly needed to achieve specific purposes. The BISON goals may be achieved also with anonymised speech recordings.

However, our legal and ethical support needs to be provided also keeping in mind that BISON will eventually be exploited after project end and thus we should act in perspective.

Speech is usually recorded by CCs based on contracts with clients, who entrust them specific activities (i.e. answering customers' request, making commercial offers, conducting surveys, etc.). Such contracts should comply with all applicable rules and regulations; as concerns data protection, in particular, they should specify the purposes for which customers' personal data may be processed by CCs and have to foresee the appointment of CCs as data processors, with specific instructions.

Contracts are often drafted by CC clients, especially in case of large corporations and possible amendments may require long and delicate negotiations.

Without having access to confidential information, we have checked the content of the most relevant contracts of partners EBOS and ComData[18] and they do not pose any specific legal issue with reference to the use of data in the BISON project, and in this context it should also be considered that no personal data will be involved.

This analysis has been useful to identify what may be the relevant issues to be discussed with Clients in future contracts, in case in the BISON post-project exploitation stage personal data needed to be processed for further training and development to allow the BISON system to get closer to the market.

We have provided partners with a short guideline on privacy issues in CC contracts, circulated in the form of internal working document: a summarisation of the basic issues is reported in Table 9 below.

We have also contributed to the drafting of an Addendum to a General Agreement between EBOS and an important Client, so that EBOS could be expressly authorised to process its Client's customers' personal data not only for the performance of the Agreement but also:

- for improving services to customers,
- for scientific, research and development purposes,
- for performing tasks within projects co-funded by the European Commission or other public bodies (e.g. Innovation Actions), such as the BISON project.

Drafting Addenda, whenever the Client agrees, may be a good solution in long-term relationships where activities are regulated by stable contracts, so that there is no need to negotiate a totally new agreement which may be complex, costly and possibly affect the relationship with the Client.

[18] As observed in D8.1, TME is in a different position than EBOS and ComData: as a CC and at the same time being a large corporation, it processes the data of its own customers and acts as data controller. On the contrary, the other partners process data on behalf of their Clients and act as data processors. In the table we have summarised the typical case of a CC operating on behalf of a Client, which is the case in object.

**Table 9 – Check list for data protection in CC contracts**

| Issue | What should be checked |
|---|---|
| Use of Client's customers' personal data for performance of contract with Client | Purposes for which the CC is allowed to process its Client's customers' personal data should not be limited to the performance of the contract, if they may be further used for other purposes, e.g. R&D purposes, EU-funded projects activities, improvement of BISON system, etc. |
| Communication of data to third parties | If there is the need to communicate personal data to parties other than the Client or public authorities, a provision should be inserted to allow it, with specific limitations (e.g. only to project partners, for R&D purposes, etc.). |
| Appointment as data processor | CCs should be clearly designated as data processors based on specific instructions.<br>Written instructions are an indispensable requirement for law-abidingness. |
| Security measures | CCs acting as processors should implement appropriate technical and organisational security measures, as defined by the national law of their own Member State (not of the controller).<br>Contract provisions on security measures should be checked, so that this principle is respected.<br>A written document should be drafted to provide evidence of the correct adoption of such measures. |
| Lawful processing of personal data | Where possible, it may be useful to ask for a written statement by the Client where it expressly declares that its customers' personal data have been lawfully recorded and processed and that EBOS/ComData shall not be held responsible when processing such data in compliance with applicable law, the contract, the appointment as data processor and the instructions. |

## 6.4 NDA

During the project lifetime, BISON partners need to exchange confidential information and this should be inspired to principles of lawfulness and correctness.

As concerns contact centers' data, in particular, audio, transcripts and anonymised metadata need to be handed to selected R&D partners in the consortium and this is based on a Non-disclosure agreement (NDA). These data shall not in any case be disclosed to the public. On this issue please see also Deliverable 3.1 § 3 "Contact Center Data".

NDAs between the partners were signed on 1st January 2015, to enable all to start project activities in a correct way.

We have examined these agreements *ex post* during the project, to check compliance with what had been promised in the DoW and to ensure adequacy in respect of the needs of the BISON project.

The signed agreements are deemed complete, correct and adequate for the purposes of the project.

For future collaborations between the partners, new agreements will need to be signed, taking into account:

- the type of confidential information to be exchanged,
- the duration of the confidentiality commitment,
- the purposes of the collaboration.

# 7. Ethical approvals for the data (update)

## 7.1 Ethical approvals issued by University Data Protection Officers

No change is to be reported since 31 March 2015. The analysis and content provided in D8.1 Section 3 is still fully valid and applicable.

## 7.2 Ethical approvals issued by Data Protection Authorities

No change is to be reported since 31 March 2015. The analysis and content provided in D8.1 Section 4 is still fully valid and applicable.

## 7.3 Ethical approvals and CC industrial partners

No change is to be reported since 31 March 2015. The analysis and content provided in D8.1 Section 5 is still fully valid and applicable.

# 8. Relevant updates on data protection

During the BISON project progress, we constantly monitor the evolution of rules, regulations and relevant case law to provide an adequate support to partners based on the current situation.

This Section reports the most relevant legal updates on data protection at European level.

## 8.1 Personal data transfers to the United States

On 6 October 2015 the Court of Justice of the European Union issued a ruling which confirmed the relevance of fundamental rights and personal data protection in the context of data transfers to non-EU countries. The Court set a very important principle: the United States do not offer an "adequate" level of protection of personal data.

The judgment follows the legal action started by Maximilian Schrems against the Irish Data Protection Commissioner[19]. Also considering Edward Snowden's revelations[20], Schrems claimed that the NSA violated citizens' privacy and that the US laws could not be considered adequate to protect the personal data coming from Europe.

The EU Court has declared that European Commission decision 2000/520/EC, which considered the "Safe Harbor" pact adequate, is invalid.

The "Safe Harbor" framework was meant to facilitate data transfers from the EU to the United States: it set a series of principles which U.S. companies could abide by in order to have the right to process personal data of European citizens in the U.S. respecting the protection level of the EU Directive and preventing accidental loss or unwanted disclosure.

The Principles were the following:

- notice – data subjects should be informed on the collection and use of their personal data;
- choice – everyone should be free to refuse the collection of his data and their transfer to third parties;
- onward transfer – personal data may only be transferred to organisations which comply with adequate principles;
- security – organisations should provide guarantees against the risk of data loss;
- data integrity – only relevant data should be collected;

[19] Case C362/14, full text of the decision can be found at http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=80732)

[20] Edward Snowden is an IT expert and former CIA employee, who supposedly copied confidential information from the United States National Security Agency (NSA) and publicly disclosed it without having been authorised. From this information there emerged that the NSA, telecommunication companies and national Governments apparently managed global surveillance programs.

- access – data subjects should have the right to access to their own data, correct or cancel them;
- enforcement – these rules should be effectively enforced.

The Court decision may have relevant consequences. In theory, each EU Member State may suspend the transfer of data towards US servers if it deems it opportune[21].

The Court has not allowed for a transitionary period, although it may have been useful and much discussion has followed.

It should be highlighted, however, that the Court decision does not mean that the transferring of personal data to the U.S. has become – in general – unlawful. What is no longer possible is to carry out such transfer based on the "Safe Harbor" framework.

Until specific decisions are taken by European competent bodies, the organisations which need to transfer data across the Atlantic may do so, albeit relying on different legal tools, e.g.:

- the explicit consent of the data subject, or
- Standard Contractual Clauses[22], or
- Binding Corporate Rules[23].

Although not of immediate relevance for the BISON project during its lifetime (as partners only process anonymous data and do not transfer them outside the EU), it should be taken in consideration in the future processing of clients' personal data by contact centers.

## 8.2 Evolution of the General Data Protection Regulation (GDPR)

In D8.1 § 6 and D8.2 § 3 we have outlined the ongoing process which will eventually lead to the abrogation of the Data Protection Directive and the entry into force of the General Data Protection Regulation (GDPR). The main possible changes and their impact on BISON have been highlighted.

[21] Following the Court ruling, the Italian Data Protection Authority (Garante per la protezione dei dati personali) has invalidated its Authorisation for the transfer of personal data to the United States. See http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/4472540

[22] The Commission has the power to decide that certain Standard Contractual Clauses provide adequate safeguards as concerns the protection of the privacy and fundamental rights and freedoms of individuals and the exercise of the corresponding rights. See http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm

[23] Binding Corporate Rules are internal rules (i.e. a Code of Conduct) adopted by multinational corporate groups which define their global policy on the international transfers of personal data within the same group to entities located in countries which do not provide an adequate level of protection. They make it possible to ensure an adequate level of protection and to avoid having to sign Standard Contractual Clauses for each data transfer within the group. Approval under the EU cooperation procedure is required. See http://ec.europa.eu/justice/data-protection/international-transfers/binding-corporate-rules/index_en.htm

Since the disclosure of the GDPR draft, there has been much debate at institutional level on the new rules and their suitability.

This last stage of discussions on the GDPR was performed jointly in the form of the so-said "Trilogue", involving the European Parliament, the European Commission and the European Council of Ministers.

On 15 December, an agreement was finally reached, based on the final negotiations of the Trilogue.

Following the political agreement reached in the Trilogue, the final texts should be formally adopted by the European Parliament and by the Council in early 2016.

The basic elements of innovation of the GDPR are:

- single set of rules across Europe;
- one single supervisory authority (one-stop-shop);
- rules applicable to companies based outside Europe that offer services in the EU;
- data protection by design;
- no more notifications to supervisory authorities;
- easier access to data by the data subject;
- right to data portability;
- clarified right to be forgotten;
- right to know when own personal data have been hacked.

The new rules should become applicable two years after the formal publication in the Official Journal of the European Union.

The Commission will work closely with Member State Data Protection Authorities to ensure a uniform application of the new rules.

During the two-year transition phase, the Commission will carry out information activities addressed both at citizens, to create awareness about their rights as data subjects, and at companies, as concerns their obligations.

Data Protection Authorities should work more closely together in the future, in particular with the aid of the one-stop shop mechanism aimed at solving cross-border data protection cases.

The next Deliverables will report on the further evolution of the GDPR and – after its formal publication – will analyse its content in detail.

# 9. References

This Section lists the relevant legal references mentioned in this Deliverable, with exact title and links. This aims at creating a knowledge base for partners, which may be consulted whenever needed, so as to allow cross-checking and further analysis for specific cases and scenarios.

## 9.1 European legislation

### EU Conventions

[Conv 108/1981] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data - European Treaty Series No. 108 – done at Strasbourg, the 28th day of January 1981. Available at http://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37

[Additional Protocol - Conv 108/1981] Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, done at Strasbourg, the 8th day of November 2001. Available at https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000001680080626

### EU Directives and Regulations

[Dir 2011/83/EU] Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights, amending Council Directive 93/13/EEC and Directive 1999/44/EC of the European Parliament and of the Council and repealing Council Directive 85/577/EEC and Directive 97/7/EC of the European Parliament and of the Council. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:304:0064:0088:en:PDF

[Dir 2009/24/EC] Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:111:0016:0022:EN:PDF

[Council Regulation 207/2009] Council Regulation (EC) No. 207/2009 of February 26, 2009, on the Community trademark (codified version). Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:078:0001:0042:en:PDF

[Dir 2008/95/EC] Directive 2008/95/EC of the European Parliament and of the Council of 22 October 2008 to approximate the laws of the Member States relating to trademarks. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:299:0025:0033:en:PDF

[Dir 2006/123/EC] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market. Available at http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0123&from=EN

[Dir 2006/114/EC] Directive 2006/114/EC of the European Parliament and of the Council of 12 December 2006 concerning misleading and comparative advertising. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:376:0021:0027:EN:PDF

[Dir 2002/58/EC] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

[Dir 2000/31/EC] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce'). Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000L0031:EN:HTML

[Dir 98/34/EC] Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1998L0034:20070101:EN:PDF

[Dir 97/66/EC] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML

[Dir 95/46/EC] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

**Recommendations of the Committee of Ministers to member States**

[Recommendation CM/Rec(2015)5] Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment. Available at https://wcd.coe.int/ViewDoc.jsp?id=2306625

**Opinions of Art. 29 Data Protection Working Party (DPWP)**

[Opinion 5/2014 DPWP] Opinion 5/2014 on anonymisation techniques – wp 216, adopted on 10 April 2014. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

[Opinion 3/2013 DPWP] Opinion 3/2013 on purpose limitation – wp 203, adopted on 2 April 2013. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

[Opinion 8/2010 DPWP] Opinion 8/2010 on applicable law – wp 179, adopted on 16 December 2010. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp179_en.pdf

[Opinion 1/2010 DPWP] Opinion 1/2010 on the concepts of "controller" and "processor" – wp 169, adopted on 16 February 2010. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

## 9.2 National legislation

### Czech legislation

[CZ 89/2012] Act No 89/2012, of 3 February 2012 - Civil Code. Available in the original language at http://www.zakonyprolidi.cz/cs/2012-89

[CZ 222/2009] Act no. 222/2009 Coll., of 17 June 2009 on the free movement of services. Available in the original language at http://www.zakonyprolidi.cz/cs/2009-222

[CZ 198/2009] Act no. 198/2009 Coll. of 23 April 2009 on equal treatment and legal means of protection against discrimination and amending certain laws (Anti-Discrimination Act). Available in the original language at http://www.zakonyprolidi.cz/cs/2009-198

[CZ 480/2004] Act. No. 480/2004 Coll. of 29 July 2004 on certain information society services and amending certain acts (Act on certain information society services). Available in the original language at http://www.zakonyprolidi.cz/cs/2004-480

[CZ 441/2003] Act No. 441/2003 Coll. of 12 March 2003 – Trademark law. Available in the original language at http://www.zakonyprolidi.cz/cs/2003-441

[CZ 121/2000] Act No. 121/2000 Coll. of 4 July 2000 on copyright, rights related to copyright and amending some laws (Copyright Act). Available in the original language at http://www.zakonyprolidi.cz/cs/2000-121

[CZ 101/2000] Act No. 101/2000 Coll., of 4 April 2000 on the Protection of Personal Data. Available in the original language at http://www.zakonyprolidi.cz/cs/2000-101

[CZ 40/1995] Act No. 40/1995 of 9 February 1995 on regulation of advertising. Available in the original language at http://www.zakonyprolidi.cz/cs/1995-40

[CZ 634/1992] Act. No. 634/1992 of 16 December 1992 – Consumer Protection Act. Available in the original language at http://www.zakonyprolidi.cz/cs/1992-634

### Italian Legislation

[IT 59/2010] Legislative Decree No. 59/2010 of 26 March 2010 on services in the internal market. Available in the original language at http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2010-03-26;59

[IT 145/2007] Legislative Decree No. 145/2007 of 2 August 2007 on misleading and comparative advertising. Available in the original language at http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2007;145

[IT 206/2005] Legislative Decree No. 206/2005 of 6 September 2005 – Consumer Code. Available in the original language at http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-09-06;206

[IT 30/2005] Legislative Decree No. 30/2005 of 10 February 2005 – Code of industrial property. Available in the original language at http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-02-10;30

[IT 259/2003] Legislative Decree No. 259/2003 of 1 August 2003 – Electronic Communications Code. Available in the original language at http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-08-01;259

[IT 196/2003] Legislative Decree No. 196/2003 of 30 June 2003– Personal Data Protection Code. Available in the original language at http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196 Available in english at http://194.242.234.211/documents/10160/2012405/DataProtectionCode-2003.pdf

[IT 70/2003] Legislative Decree No. 70/2003 of 9 April 2003 on electronic commerce. Available in the original language at http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-04-09;70!vig=

[IT 300/1970] Law No. 300/1970 of 20 May 1970 – Workers' Statute. Available in the original language at http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1970-05-20;300!vig=

[IT 633/1941] Law No. 633/1941 of 22 April 1941 on copyright and connected rights. Available in the original language at http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:1941-04-22;633!vig=

[IT 262/1942] Royal Decree 262/1942 of 16 March 1942 – Civil Code. Available in the original language at http://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:regio.decreto:1942-03-16;262

**Luxembourgish legislation**

[L 02/08/2002] Coordinated text of the Act of 2 August 2002 on the protection of individuals with regard to the processing of personal data amended by the Act of 31 July 2006, the Act of 22 December 2006, the Act of 27 July 2007, the Act of 28 July 2011. Available in the original language at http://www.legilux.public.lu/leg/a/archives/2002/0091/a091.pdf Available in english at http://www.cnpd.public.lu/fr/legislation/droit-lux/doc_loi02082002_en.pdf

**Spanish legislation**

[E 3/2014] Law No. 3/2014, of 27 March 2014 approving the revised text of the amending General Law for the protection of consumers and users and other laws complementary, approved by Royal

Decree 1/2007 of 16 November, 2007. Available in the original language at http://www.boe.es/diario_boe/txt.php?id=BOE-A-2014-3329

[E 29/2009] Law No. 29/2009, of 30 December 2009 approving the revised legal regime of unfair competition and advertising to improve the protection of consumers and users. Available in the original language at http://www.boe.es/diario_boe/txt.php?id=BOE-A-2009-21162

[E RD 1/2007] Royal Decree No. 1/2007, of 16 November 2007 approving the revised text of the General Law for the protection of consumers and users and other complementary laws. Available in the original language at http://www.boe.es/buscar/act.php?id=BOE-A-2007-20555

[E 15/99] Law No. 15/1999, of 13 December, 1999 on personal data protection. Available in the original language at http://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

[E RD 994/1999] Royal Decree No. 994/1999, of 11 June 1999 approving the regulation of security measures for automated files containing personal data. Available in the original language at http://www.boe.es/buscar/doc.php?id=BOE-A-1999-13967

[E RD 1/1996] Royal Decree No 1/1996, of 12 April 1996 approving the revised text of the Copyright Act, regulating, clarifying and harmonizing the applicable legal provisions on the subject. Available in the original language at http://www.boe.es/buscar/doc.php?id=BOE-A-1996-750

[E RD 1332/1994] Royal Decree No. 1332/1994, of 20 June 1994 establishing certain aspects of the Law No. 5/1992, of October 29, 1992 regulating the automated processing of personal data. Available in the original language at http://www.boe.es/buscar/doc.php?id=BOE-A-1994-14121

[E RD 428/1993] Royal Decree No. 428/1993, of 26 March 1993 approving the Statute of Agency for Data Protection. Available in the original language at http://boe.es/diario_boe/txt.php?id=BOE-A-1993-11252