



Big speech data analytics for contact centers

BISON

<http://bison-project.eu/>

European Horizon 2020 project No. 645323



Deliverable D8.2

Legal, ethical and societal issues of BISON

General framework

Due date: 30/06/2015

Submission date: 30/06/2015

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), Honza Cernocky (BUT), Javier Julian Ortega Reyes (COMC), Verena Hoffeld (EBOS), Luis Angel Galindo Sanchez (TME).

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

Summary

This Deliverable outlines a general framework aimed at identifying the main legal, ethical and societal issues connected with the development and use of BISON results and technologies and provides a first knowledge base and indications to BISON technical partners.

It constitutes a living document and will be articulated in four versions: besides the present, due in M6, the following ones are due in M12 (D8.3), M24 (D8.4) and M36 (D8.5). This will make it possible to support the technical teams throughout the project, from a general outline up to guidelines and a legal and ethical code for BISON.

This and the following versions of the Deliverable will focus on

- the procedures that will be implemented for data collection, storage, protection, retention and destruction, confirming that they comply with national and EU legislation;
- the planned/implemented informed consent procedures and their feasibility in massive CC data collection;
- ethical approvals for the planned collection and the planned analyses of personal data, if updates or new approvals as compared to the approvals submitted in M3 are needed
- potential dual use and malevolent/criminal/terrorist abuse of the BISON results outside the project and risk-mitigation and prevention strategies;

D8.2 is drafted at the initial stages of BISON design and development and will be enriched and integrated in its subsequent versions through a constant interaction with the technical partners: technical and legal tasks will continually build upon each other's results.

Table of Contents

Summary.....	2
1. Introduction.....	5
2. Legal and Ethical framework of data processing in the BISON perspective	5
2.1 The EU and international legal framework: an outline	5
2.2 Principles for the lawful processing of personal data	7
2.3 The relevant roles: data controller, data processor, data subject.....	12
2.4 Information and consent	13
2.5 Security measures	15
2.6 Data processing for scientific purposes	16
2.7 Data transfer from-and outside the EU and cloud services	17
2.8 Speech as biometric data	18
2.9 Big data: the lawful management of huge data sets	19
3. From the DPD to the General Data Protection Regulation – a general outline.....	20
3.1 The status of EU data protection legislation	20
3.2. A comparison between Directive 95/46/EC and the GDPR	22
3.3 New GDPR provisions in the BISON perspective.....	25
4. BISON data processing procedures	31
4.1 Lawful data processing procedures in contact centers (ante BISON).....	31
4.2 Data processing procedures in BISON project activities.....	38
4.2.1 Legal requirements for anonymisation	38
4.2.2 BISON general dataflow.....	41
4.2.3 Anonymisation procedures in BISON (annotation).....	43
4.3 Law-abidingness of BISON results	47
4.3.1 Information, consent and data collection	47
4.3.2 BISON data processing procedures	49
5. Legal aspects of BISON 2.1 Scenarios: a first schematization	54
5.1 Operation Scenarios.....	54
5.2 Operation & Quality Scenarios.....	55
5.3 Clients’ Scenarios	58
5.4 Law Regulation Scenarios	58
6. Beyond the law: ethical and societal issues	60
6.1 Ethics in BISON research	60
6.2 Key issues	61
6.3 Ethics at the CC partners	62
6.4 Big data ethics	63
7. Dual Use	65

7.1 Transfer outside the EU	65
7.2 Potential dual use of BISON results	67
7.2.1 Dual use and data.....	68
7.2.2 Dual use and the BISON system (technologies, algorithms)	68
7.3 Risk-mitigation strategies	69
8. Prevention of possible abuse/misuse.....	70
8.1 Possible malevolent/criminal/terrorist abuse/misuse of BISON results	70
8.2 Risk assessment	71
8.3 Prevention measures	71
References	74
List of acronyms	75

1. Introduction

This Deliverable is articulated in 8 Sections.

Section 2 provides the indispensable knowledge base for our technical partners needed to understand the legal and ethical foundations, principles and rules on which to found the design and development of BISON and the implementation of CC procedures for data processing.

Section 3 contains a general outline for this delicate transition stage from the EU Data Protection Directive still in force and the upcoming EU General Data Protection Regulation. Present and future rules are put in comparison and the relevant implications for BISON are identified.

Section 4 focusses on BISON data processing procedures. These are analysed from three different perspectives: a) lawful data processing procedures at partner contact centers; b) data processing procedures in BISON project activities, with particular attention to anonymisation; c) law-abidingness of BISON results, with particular reference to information, consent and the different stages of the data processing cycle.

Section 5 builds a first strong link between WP2 ‘User requirements and feedback’ and WP8. Starting from the real-life Scenarios developed in D2.1 ‘Initial user requirements’, it singles out the most relevant ones and identifies possible legal issues to be considered. This Section, in particular, will undergo development and deeper analysis in the following Deliverables, based on the partners’ feedback.

Section 6 gives a first set of inputs on ethical and societal issues, which may go beyond the legal and ethical framework as set at EU and national level and examined in the previous Sections.

Section 7 analyses potential dual use implications that may be present even in a civilian project such as BISON and will present possible risk mitigation strategies.

Section 8 discusses possible malevolent/criminal/terrorist abuse/misuse of the BISON results outside the project and identifies possible prevention strategies.

2. Legal and Ethical framework of data processing in the BISON perspective

2.1 The EU and international legal framework: an outline

Ethically dealing with individuals’ personal data means also, and in the first instance, assuring compliance with EU and national data protection regulation.

Data protection is a ‘third generation’ **fundamental human right**, entrenched by **Article 16** of the **Treaty on the Functioning of the European Union**¹, and by **Article 8** of the **Charter of**

¹See Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union 2012/C 326/01, on <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012E/TXT>

Fundamental Rights of the European Union², among other freedom rights such as the more ‘traditional’ right to liberty and security, freedom of expression, information, association, education, etc. The three paragraphs of Article 8 constitute the core, and the sense, of the personal data protection regulation, which, at the European level, is more thoroughly laid down by **Directive 95/46/EC** (hereinafter, the **Data Protection Directive**, DPD).

The DPD, brought into force by all EU Member States’ national law, contains a number of key principles for the fair and lawful processing of personal data, together with the technical framework and the security measures designed to guarantee that all personal data are safe from unforeseen, unintended or malevolent access, discovery and use, during the entire data processing period.

Beside this, and chronologically before, at international level the right to data protection was first recognized by **Council of Europe Convention 108**³ opened for signature on 28 January 1981. The Convention was the first legally binding international instrument in the data protection field. It draws inspiration directly from the European Convention on Human Rights and Fundamental Freedoms and has been signed by all the 47 members of the Council of Europe plus Uruguay.

The fundamental right to the protection of personal data under Article 8 of the Charter is not, however, an absolute right, but must be considered in relation to its function in society. Therefore, some limitations may be imposed on the exercise of this right, as long as these limitations are provided for by law and, respecting the essence of data protection, are necessary and genuinely meet objectives of general interest recognised by the EU and/or the need to protect the rights and freedoms of others.

Among the rights that are likely to come into conflict with the right to data protection, there is the freedom of art and science: the general restrictions for the use of personal data may be diminished as a consequence of the special value of science to society expressly recognized by the European data protection law (see § 2.6 below).

Despite this balancing of different fundamental rights and freedoms with the data protection right, it is precisely in the research field that ethical issues arise as cornerstone for the lawful and fair processing of personal data. Thus, while some of the limits imposed by the law to the processing of personal data fall, or are greatly diminished, when facing with freedom of scientific research, the common ethical rules and principles governing the research activity act as boundaries for scientific research itself. Ethical principles like *informed consent*, *confidentiality* and ‘*avoiding harm to do good*’⁴, which are maybe more clear and immediately comprehensible when referred to medical research involving human beings, are still valid and applicable when personal data are in dispute (see in particular §§ 2.2, 2.4 and 2.5 below).

The same rules are to be taken in consideration with even more attention when the processing involves large amounts of personal data and/or sensitive data (see §§ 2.4, 2.8 and 2.9). In particular, people should be given the possibility to manage the flow of their information across massive, third-

²Charter of fundamental rights of the European Union, 2000/C 364/01 http://www.europarl.europa.eu/charter/pdf/text_en.pdf

³Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, <http://conventions.coe.int/treaty/en/Treaties/Html/108.htm>

⁴ M. Israel & I. Hay, *Research Ethics for Social Scientists*, 2006, Sage Publications Ltd.

party analytical systems, so that data subjects can have a transparent view of how their data will be used – or sold.

2.2 Principles for the lawful processing of personal data

2.2.1. Basic concepts

The Convention 108, the DPD and the consistent national rules which have progressively come into force in all Member States pay a special attention to the collection of data, and to the principles applying in particular to this first phase of data processing, so that it is important to preliminary clarify some basic concepts concerning personal data protection, as defined by the DPD.

Personal data consist of ‘any information relating to an identified or identifiable natural person (*‘data subject’*)’, where ‘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’.

This means that where the data do not refer, directly or indirectly, to a natural person (to an ‘individual’, for Convention 108), because the link between the data subject and the data themselves never existed or is somehow broken and cannot be rebuilt in any way (such as with anonymized data), we are not processing *personal* data at all.

In the context of the BISON project, it is important to highlight that while the voice may also be considered a factor related to the ‘physical identity’ of the data subject, it actually becomes a personal datum only when, alone or in relation with other data and/or information, it makes it possible to identify the subject.

For the BISON project activities, speech data are fully anonymised, thus the DPD does not apply.

Data controller is ‘the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data’.

In the context of the BISON project, a data controller may be a contact center (CC) which processes the personal data of its own customers (natural persons).

Data processor is ‘a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller’. It acts in force of a contract or of an agreement with the data controller.

In the context of the BISON project, a data processor may be a contact center (CC) which processes the personal data of its Clients’ customers (natural persons), following the Clients’ instructions.

Its Clients are in turn data controllers with reference to the processing of their own customers’ personal data.

Processing is defined as ‘any operation or set of operations which is performed upon personal data,

*whether or not by automatic means*⁵, where ‘any operation’ has to be intended literally.

Every action that involves personal data is ‘processing’, and the non-exhaustive list provided by the DPD includes all the following operations: collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Such operations may be performed by the data controller itself and/or by the data processor, in force of a contract or of an agreement between them (see 2.3 below).

As to the collection of personal data, which represents the very first processing operation, the DPD (and, before, Convention 108 at Article 5) sets out some basic principles (Article 6), to be regarded as milestones for the lawful processing of personal data. All subsequent data protection legislation must comply with these principles and they must be kept into account when interpreting such legislation.

2.2.2. Lawful processing

The processing of personal data may constitute an interference with the right to respect the data subject’s private life. However, as already seen before, this right has to be examined and reconciled with other private or public legitimate interests. Both Convention 108 and the DPD refer to the principle of lawful processing of personal data, stating that **personal data** must be **obtained** and **processed lawfully**, but neither of them contains a definition of what exactly is lawful.

According to the European Court of Human Rights (ECHR) jurisprudence and the EU Charter, a data processing is lawful when:

- a) made in accordance with an existing (domestic) law ‘*accessible to the persons concerned and foreseeable as to its effects*’⁶, so that the individual may easily know the rules and consequently modulate his/her behaviour;
- b) pursuing a legitimate aim, that is the private or public interest to be balanced with the data protection right;
- c) is necessary in a democratic society, so as to justify the interference of the processing with the data protection right of individuals, and anyway complies with the principle of proportionality (see also 2.2.4 below);
- d) in any case, it respects the essence of the right to data protection.

2.2.3. Purpose specification

According to the DPD, data must be **collected** for **explicit** and **legitimate purposes** and **used accordingly**.

⁵ Convention 108 was primarily about *automatic processing*, which includes the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination. The DPD, instead, expressly refers to any operation performed upon personal data, whether or not by automatic means.

⁶ ECHR, *Amann v. Switzerland*, No. 27798/95, 16 February 2000, par. 50; see also ECHR, *Kopp v. Switzerland*, No. 23224/94, 25 March 1998, par. 55 and ECHR, *Iordachi and Others v. Moldova*, No. 25198/02, 10 February 2009, par. 50.

This implies that the **processing purposes** must **always be clearly declared**, primarily to the data subject, who has to be specifically informed of all elements related to the processing, **before the processing itself is started**.

Such elements are stated in Article 10 of the DPD – briefly:

- identity of data controller and representative, if any⁷,
- purposes of the processing for which the data are intended,
- possible recipients or categories of recipients of data,
- whether it is obligatory or voluntary to provide personal data and what are the consequences of failure to reply,
- rights granted to the data subject (e.g. right of access and to rectify the data).

On the contrary, any processing for undefined purposes is not compliant with data protection law, and the consent given in such cases is not deemed valid. The same applies when the data subject has been asked for just one consent in view of a plurality of purposes.

A controller must not use the data collected for a certain purpose to pursue a different one, also at a different time (i.e. after the declared purpose has been achieved): further use of personal data for other purposes needs an additional legal basis if the new purpose of processing is incompatible with the original one.

The concept of compatibility, however, is not defined and is left open to interpretation on a case-by-case basis. Generally speaking, it can be considered as ‘not incompatible’ any purpose that the data subject was reasonably able to predict as compatible with the data processing purposes according to the information received at the moment his/her data were collected.

Furthermore, the data collected must be strictly consistent with the declared purposes, so that it is unlawful to collect more data than necessary (but see § 2.6 below, also on compatibility of purposes).

Any transfer of data to third parties is also a *new* purpose needing an additional legal basis (see also § 2.7).

If personal data needed to be processed for the purposes of the BISON project – which is presently not foreseen – CCs would have to get a specific consent by their Clients’ customers.

Although only anonymous data will be processed, CC partners have duly and transparently informed their Clients about data processing in BISON with individual letters explaining the goal of the project and the activities that will be performed.

2.2.4. Relevancy of data

Personal data collected must also be **relevant** and **not excessive** in relation to the purposes for which they are processed.

⁷ If the data controller is not established in an EU Member State and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community, it must designate a representative established in the territory of that Member State.

Thus, only data necessary to achieve the declared aim of the processing operations may be collected, and the controller must strictly limit the collection of personal data to those data, which are directly relevant for the specific purpose(s) pursued.

In the BISON context, this could mean that data controllers (and contact centers when acting as data processors and collecting data on behalf of them) are strictly bound by the declared purposes both as concerns the quality and quantity of the personal data to be collected.

Only data which are related and proportionate to the specific purposes may be collected and processed: any wider collection may result in law infringements (and possibly also in contract infringements for the data processors towards their Clients)

2.2.5. Accuracy of data

Personal data must be **accurate** and **up to date**. Whenever the data controller, or processor, or person in charge of the personal data processing, knows that pieces of information on a given data subject are wrong, or have been changed (for example, because the data subject him/herself asks for updating), the personal data must be consequentially corrected.

Nonetheless, the impact of this principle has to be considered in relation to other needs. In some cases data accuracy is irrelevant because the data processing purposes have already been achieved, and data were up to date and correct when collected: this is the case, for example, of data collected for billing purposes, when the bills have already been issued and then only stored for administrative or fiscal needs.

In some cases, it is even not allowed to correct data, as they represent historical facts (i.e. reports, official documents, etc.), while in other cases it is necessary in order to avoid possible damages to the data subject (i.e. credit history data).

2.2.6. Limited retention

Another fundamental principle states that **data may be retained only for the period** they are **necessary** for the **achievement of the specific purposes** for which they are being processed, and then erased.

Both Article 5 of Convention 108 and Article 6 of the DPD actually point out that the data which identify individuals must not be retained longer than necessary.

Despite this, it is **possible to continue processing** personal data beyond the originally declared purposes if personal **data** are **anonymised**, so that they cannot in any way be linked back to an individual. The anonymisation process may be regarded to as the last authorized operation of the processing of personal data, before they cease being *personal* data to become simply *data*.

Another option is **pseudonymisation**: in theory, personal data are still ‘personal’, because they may be reconciled to an individual, but in practice identifying elements are separated from data, so that it is difficult to rebuild an identity without the key. In other words, the link to an identity still exists in form of the pseudonym plus the decryption key: re-identification is possible with the key, while is very difficult without it.

Pseudonymisation is not explicitly mentioned by Convention 108 or the DPD, but the Explanatory Report to Convention 108 states that:

- in Article 2 of the Convention, ‘**Identifiable persons**’ means a person who can be easily identified: it **does not cover identification** of persons by means of **very sophisticated methods**’ (§ 28), and
- in Article 5, ‘the requirement appearing under litterae concerning the time-limits for the storage of data in their name-linked form does not mean that data should after some time be irrevocably separated from the name of the person to whom they relate, but only that it should **not be possible to link readily the data and the identifiers**’ (§ 42).

Both these paragraphs refer to pseudonymisation, which actually seems to serve the declared purpose to enable the identification of data subjects for no longer than is strictly necessary.

Anonymisation is a central issue for BISON, because whenever data are fully and effectively anonymized, the EU Data protection Directive and any national and international rule or regulation on data protection become fully irrelevant, as no personal (i.e. identifying) data would be processed.

Consequently, any ethical principle or legal rule in force at European, national or local level, including the need for ethical approvals, notifications and/or authorisations by DPAs would not be applicable either.

Then, it is allowed under data protection law to retain data for future scientific, historical or statistical use, thanks to a specific exemption provided by the DPD⁸ (see 2.6 below). Such extended use of personal data must, however, be accompanied by special safeguards under national law.

2.2.7. Fair processing

The processing of personal data is **fair** when the **data subject** is **adequately informed** about how his/her data will be used and he/she **has the power to effectively act** on his/her own personal data, to modify them, get information on the process, etc. This is possible only when the data processing is transparent and the data subject is in the condition to know and fully understand (and agree) what happened to his/her personal data.

Therefore, the fairness principle is substantially a matter of transparency to the data subject, and is strictly related to the duty of giving him/her a complete information, to receive a valid (informed) consent and to guarantee, during all the processing period, his/her rights to maintain control over the data (i.e. access, modification, obtaining information, etc.).

2.2.8. Accountability

According to the principle of accountability, controllers have to implement all measures needed to promote and safeguard data protection in their processing activities.

Controllers are responsible for the compliance of their processing operations with data protection

⁸ Article 6: ‘Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use’.

law, whether or not performed directly by them or by a processor on their behalf, and should be **able** at any time – when requested – to **demonstrate compliance** with **data protection provisions** (to data subjects, to the general public and to supervisory authorities).

The DPD does not expressly refer to an accountability principle, but it could be descended both from Art. 6, when it says that *‘It shall be for the controller to ensure that paragraph 1 is complied with’*, and from Art. 17 on the security of processing, when it says that it is up to the controllers to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, and unauthorized disclosure or access.

However, above all this, the accountability principle is an Article 29 Working Party⁹ development: according to its Opinion 3/2010 *‘Controllers should also ensure that the practical measures implemented to comply with data protection principles are effective. In case of larger, more complex or high risk data processing, the effectiveness of the measures adopted should be verified regularly. There are different ways to assess the effectiveness (or ineffectiveness) of the measures: monitoring, internal and external audits, etc.’*, and it is also stated that *‘in assessing sanctions related to data protection violations, data protection authorities could give weight to the implementation (or lack of it) of measures and their verification’*¹⁰.

When acting in an operational context after project end, bigBISON in its commercial version will possibly involve ‘larger’ and ‘more complex’ data processing. Therefore, data controllers and processors acting on their behalf should be enabled (and encouraged) to regularly perform a regular verification of the effectiveness of the practical measures adopted to comply with data protection principles.

2.3 The relevant roles: data controller, data processor, data subject

The concepts of data controller and data processor, together with their interactions, play a crucial role in the application of the DPD, since they determine who shall be responsible for complying with data protection rules, and how data subjects may exercise their rights. The concept of data controller is also essential to identify the applicable national law and the exercise of the supervisory tasks of the DPA.

As seen above, the (natural or legal) person who determines the processing of personal data and takes any related decision (e.g. how to process, what kind of data, what type of means to be used for the processing, where, etc.) on other people’s data is a **controller** under data protection law.

It may be possible that several persons take these decisions together, to pursue a common purpose, and in this case they all are **joint controllers**. However, it is very important to highlight that only the controller (even if it is a joint controller) has this original (in the meaning of non derivative) **power** to

⁹ The Article 29 Working Party is composed of representatives of the national DPAs, the European Data Protection Supervisor (EDPS) and the European Commission. It is a very important platform for cooperation, and its main tasks are to provide expert advice from the national level to the European Commission on data protection matters, to promote the uniform application of the DPD, and to advise the Commission on any European Community law that affects the right to protection of personal data (see <https://secure.edps.europa.eu/EDPSWEB/edps/Cooperation/Art29>).

¹⁰ Article 29 Working Party, Opinion 3/2010 on the principle of accountability, WP 173, Brussels, 13 July 2010, at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf.

decide every aspect of the **processing** of personal data.

A **processor** is a legally separate entity that processes personal data on behalf of a controller, in force of a written agreement between them (e.g. tax adviser or telemarketing company). A division or a branch of the same company acting as controller cannot be considered as ‘processor’, even if it is clearly structured and quite independent, for the legal separation is an essential requirement.

The activities entrusted to a processor may be limited to a very specific task or context, or may be quite general and comprehensive. However, in order to solve any doubt on the ‘tag’ to be attributed to a person in relation with its role in data processing, it is always fundamental to make reference to the nature and the source of the power exercised: a controller simply *decides* to start a personal data processing and doing so becomes a controller, whilst a processor *derives* any power and range of permitted activities from the controller.

In BISON, partners which provide data do not all play the same role in data processing:

- Telefónica Móviles is the only one which operates as data controller, as it processes its own customers’ data
- Ebos and ComData, instead, only act as data processors on behalf of their clients, which, in turn, act as data controllers.

Therefore, the partners’ duties and responsibilities must be considered separately, since only data controllers are directly bound by the obligations foreseen by the DPD and by national rules and regulations, (e.g. as concerns information, consent and authorisations by DPA). Data providers, in turn, are bound by the controller’s instructions.

In connection with the different source of controllers’ and processors’ powers is that whenever **the processor acts irrespectively** of, or simply **exceeding**, the **instructions given by the controller** for the **processing** of data, thus taking autonomously any of the decisions which are up to the controller, the **processor becomes controller itself**. Consequently, the processor in breach of its duties directly assumes all the obligations foreseen by the DPD and by national rules and regulations on personal data processing, as this solution provides the best protection for the data subject’s interests¹¹.

Opposite to the controller and the processors stands the **data subject**, that is the natural person to whom personal data are related. Effective protection of personal data means effective protection of the data subject’s rights, so this figure represents a valid interpretation key for doubtful or unclear expressions in data protection law, if any.

2.4 Information and consent

In order to grant to the data subject an effective protection of his/her rights, the data controller is primarily required to provide an **information notice** to every data subject, either orally or in writing, whenever personal data are collected either from the same data subject or from third parties.

Such information must specify, in a concise and user-friendly manner:

¹¹ See Article 29 Working Party (2010), Opinion 1/2010 on the concepts of ‘controller’ and ‘processor’, WP 169, Brussels, 16 February 2010 at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf.

-
- what **purpose(s)** and **mechanisms** apply to the processing;
 - whether the data subject is **obliged** to provide the data **or not**;
 - what **consequences** may result from the **failure to provide the data**;
 - **who** the data may be **communicated** to **or** if data shall be **disseminated**;
 - what **rights** are granted to the **data subject**;
 - who is the data controller (and the data processor, if any), and how to contact them.

According to the information given in this document, the data subject should be totally conscious of the data processing before its beginning, and may therefore accept such use of his/her personal data or reject it.

The data subject's informed **consent** is a mandatory pre-requirement to lawfully process personal data, and there are limited exceptions to this rule.

One of these is the exception for scientific purposes (see below § 2.6), as foreseen by art. 6 DPD. Thus, also when the data subject has given his/her informed consent for purposes other than the scientific ones, nonetheless his/her personal data may be processed for such purposes, provided that the national data protection rules has implemented the Article 6 exception.

Should anonymisation not be practicable to achieve the project's goals, the use of personal data retained by BISON's partners shall be subject to the DPD and applicable national legislation.

This means that the data controller must have included scientific or, at least, industrial research among the purposes of data processing declared in the **information** given to the data subject, and must have in some way declared that data would be communicated to specific categories of third parties, in which also research partners may fall into as recipients.

When a partner acts as data processor, it has to check whether such disclosure is authorized by the agreement signed with its data controller. If there are no provisions of this kind, a new authorization has to be asked to the data controller.

Personal data may be processed only if the data subject has freely, specifically and unambiguously given his/her consent after being adequately informed.

In particular, *specific* in this context has to be read in relation to the different kinds of processing of data and/or different operations to be performed on them (and the data subject must be asked again for consent for further processing operations which could not reasonably have been foreseen when the initial consent was given)-

Free means that the data subject must be in condition to exercise a real choice, without risk of deception, intimidation, coercion or significant negative consequences if he/she does not provide his/her consent. The concepts of freedom and 'real choice' in relation to the data subject's consent also involve that, for example, the unique consent given to a multitude of different purposes is not deemed valid.

Given these requirements, it is necessary that BISON's partners – in case they were required to process personal data - preliminary carried out the following check:

- a) when acting as data controller, to verify whether data subjects have been given the informed

consent, and if not, to ask for it, when possible, in written form;

- b) when acting as data processor, to verify if the contract or agreement made with the data controller allows them to process data for purposes other than the performance of the contract and in particular for purposes compatible with BISON activities, as well as to communicate personal data to other BISON partners. In turn, the data controller must have previously obtained the data subjects' informed consent.

As to case *a)* above, the written form is not a requirement foreseen by the DPD for the validity of the data subject's consent. However, it is possible that the data collected consist both of common personal data (i.e., name, surname, age, address, etc.) and of sensitive ones. Every Member State is allowed, under Article 8 of the DPD, to '*prohibit the processing of 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*' (the so-called 'sensitive data').

This provision, however, does not apply when '*the data subject has given his explicit consent to the processing of those data*', and every Member State may require different formalities for the consent to be explicit, so it is **highly recommended** in any case to have or obtain it in a **written form**, to be able to provide adequate evidence of the consent.

2.5 Security measures

It is up to the controllers to provide technical and organizational measures to protect personal data, during all the processing period, against the risks related to the **integrity** of data (i.e., accidental or unlawful destruction, accidental loss, alteration, etc.), and **confidentiality** (i.e., 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.

Besides the controller, the processor too is charged with the obligation to prevent any event that may cause unlawful/unauthorized interference with the data processing operations, in accordance with the instructions received by the controller. The security obligation is, therefore, somehow shared between the controller and the processor, and affects also any other subject involved in the processing of personal data, who must strictly follow the instructions received for processing itself, and must also be the first party to take action if needed by the concrete circumstances.

The level of data security requested by law is determined by a plurality of elements, related to the:

- **nature** of collected data (sensitive data must have a higher level of protection than common personal data),
- the **concrete availability in the market** – as 'state of the art' – of security measures and remedies that suit the specific data processing features, and
- the **cost** of them, which, anyway, must be not disproportionate with the necessity of protecting personal data.

However, security measures are not only technical remedies, but also organisational rules that should be severely observed by all the subjects involved in data processing, as the latter are complementary with the former. It is surely of great importance to outline a clear distribution of responsibilities and

competences in matters of data processing, to ensure that authorisations to access personal data have been assigned by the competent person, that every access is automatically checked and authorized. It is even more important to keep in mind that any technical rule may easily become ineffective without, for example, the regular provision of information to all employees – even through data security training and education – about data security rules and their obligations under data protection law, especially regarding their obligations of confidentiality.

Thus, the quality of the complex of security measures requested is the result of a case-by-case evaluation, which must be performed before starting new personal data processing operations and then implemented and adapted, when needed, during the whole data processing period, with regard to the technical solutions, and the human factor, too.

2.6 Data processing for scientific purposes

An important exception to the principle of purpose specification (and therefore to the information and consent obligation seen in § 2.4 above) is provided by Article 6 of the DPD, which states that *‘Further processing of data for historical, statistical or scientific purposes shall not be considered as incompatible [with the original purposes] provided that Member States provide appropriate safeguards’*.

This means that if **personal data** are **obtained** for **one purpose** and then **re-used** for **research**, the research is **not**, generally speaking, an **incompatible purpose**.

The DPD and Convention 108 both permit the retention of personal data for scientific research once they are no longer needed for the initial purpose of their collection. Furthermore, the subsequent use of personal data for scientific research shall not be considered an incompatible purpose. National law is charged with the task of developing more detailed provisions, including the necessary safeguards, to reconcile the interest in scientific research with the right to data protection.

Thus, it may be useful to draw out a definition of what does the **DPD** mean with **‘scientific research’**. Article 179 (and following) of the Treaty on the Functioning of the European Union declares one of the objectives of the Union that of *‘strengthening its scientific and technological bases by achieving a European research area in which researchers, scientific knowledge and technology circulate freely, and encouraging it to become more competitive, including in its industry [...]’*, encouraging, for this purpose, *‘undertakings [...], research centres and universities in their research and technological development activities of high quality’*.

In the field of data protection, this meaning of scientific research is recalled by the Proposal for the General Data Protection Regulation, which, at Whereas no. 126, affirms that *‘scientific research for the purposes of this Regulation should include fundamental research, applied research, and privately funded research and in addition should take into account the Union’s objective under Article 179(1) of the Treaty on the Functioning of the European Union of achieving a European Research Area’*.

Therefore, according to these provisions and explanations, and considering that they all have to be evaluated in same social, cultural and juridical context, it is possible to conclude that ‘scientific’ is not limited, for example, either to research with health-related or biological subject, or to public funded or purely academic research.

The BISON project may be considered scientific research under the definitions quoted above. The Article 6 provision allows the processing of personal data originally collected for purposes other than scientific research, provided that the national data protection rules of project partners acting as data controllers have a regulation about such purposes.

Furthermore, **research data are not subject** to the principle of **limited retention**, so they can be kept indefinitely. Research data are also exempt from the subject access right, provided, in addition, the results are not made available in a form that identifies any individual. All other data protection principles still apply, including the duty to process personal data fairly and lawfully.

Clearly, this exemption becomes particularly relevant if any personal data are used for research, while if this only uses anonymised data, then there is no processing of personal data under the DPD, and the DPD does not apply to that research.

2.7 Data transfer from-and outside the EU and cloud services

Under Article 1 of the DPD the **flow of personal data is free between EU Member States**, just as, for the establishment and functioning of an internal European market, Article 7a of the EU Treaty grants the free movement of goods, persons, services and capital. Moreover, Article 12 of Convention 108 establishes that the transfer of personal data to another Contracting Party to Convention 108 must be free from restrictions.

On the other hand, the fundamental rights of individuals must be safeguarded too, so the DPD, while harmonizing the level of protection of the rights and freedoms of individuals with regard to the processing of personal data in all EU Member States, also poses some **restrictions** to the **export of personal data to third countries not ensuring an adequate level of data protection**.

Adequacy of data protection in a third country means that the main principles of data protection as seen above have been effectively implemented in the national law of that country. This requirement might be evaluated by the European Commission or by the domestic law of each Member State. At the moment, one of the most important decisions on adequacy taken by the EU Commission is actually a set of rules, known as *Safe Harbour Privacy Principles* (or simply ‘Safe Harbour’), elaborated between the EU and the US and mainly addressed to US business companies.

Therefore, if there is no specific consent to the data transfer outside the EU given by the data subject (given in accordance to what explained above in § 2.4)¹², and if the level of data protection of the recipient has not been already found ‘adequate’, the controller may be required to subject the intended data flow to examination by its national DPA before exporting personal data. It also has to demonstrate the existence of a legal basis for that data transfer, and that the recipient sets up enough security and organizational measures to grant adequate protection of the personal data (e.g., through contractual clauses, binding corporate rules).

¹² According to Article 29 Working Party it is undoubtful that the general rules on the legal significance of the consent also apply to Article 26 of the directive: part. Article 29 Working Party (2005), Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995, WP 114, Brussels, 25 November 2005.

Even if in **BISON none of the partners plan or are supposed to transfer personal data outside the EU**, it is nonetheless important to supply a brief but exhaustive framework on this issue, which becomes a little more complex when the ‘transfer’ of personal data consists of the whole of processing operation deriving from having personal data stored by one (ore more) **cloud computer services’ provider**.

Among other problems that may arise (related to lack of control over the data, and insufficient information regarding the processing operation itself), Article 29 Working Party faced the relevant data protection legislation, enunciating that ‘*The **applicable** legislation is the **law of the country in which the controller contracting the cloud computing services is established**, rather than the place in which the cloud computing providers are located*’, and that ‘*Should the controller be established in various Member States, processing the data as part of its activities in these countries, the applicable law shall be that of each of the Member States in which this processing occurs*’¹³. The same Opinion also clarifies the role and responsibility of the cloud client and provider, considered, respectively, as controller and processor.

2.8 Speech as biometric data

Biometrics refers to technologies that measure and analyse physical characteristics, for authentication or identification purposes. As to the voice, it may concern the analysis of the tone, pitch, cadence and frequency of a person’s voice, aimed to determine if a certain person is who he/she declares to be.

From a data protection perspective, biometric technologies are closely linked to certain **physical, physiological, behavioural or even psychological** characteristics of an individual, and some of them can be used to reveal sensitive data. Biometric data may also allow for automated tracking, tracing or profiling of persons and, as such, their potential impact on the privacy and the right to data protection of individuals is high¹⁴. Moreover, biometric data are **irrevocable**: a breach concerning biometric data threatens the further safe use of biometrics as identifier and the right to data protection of the concerned persons for which there is no possibility to mitigate the effects of the breach.

Voice biometric authentication systems are based on measurements and comparisons of the biological characteristics of the individual with others previously checked and recorded in a database by a mechanism called *enrolment*. Every spoken word (of a predefined speech used as sample) is converted, by a chain of mathematical operations, into a person’s voice print (also called ‘iVector’ in the R&D community), which is stored in the database. This shall be further interrogated to determine if a speaker is the person he/she claims to be, by comparing the stored voice print with the speaker’s, or even to determine which speaker, in a group of known speakers, most closely matches the unknown speaker (and in this case we must more properly refer to *identification* systems, instead of authentication’s).

¹³ Article 29 Working Party (2012), Opinion 05/2012 on Cloud Computing, WP196 Brussels, 1 July 2012, at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf

¹⁴ See for an outlook Article 29 Working Party (2012), Opinion 3/2012 on developments in biometric technologies, WP193 Brussels, 27 April 2012, at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf

The processing of biometric data is not only subject to the express consent of the data subject, but also depends on the authorization by DPAs¹⁵ and is anyway submitted to severe rules on security measures that must be adopted to protect data (e.g., biometric information must always be stored in encrypted form, decryption keys must only be accessible on a need to know basis, the system should be designed in a way that allows to revoke the identity link, either in order to renew it or to permanently delete it if the consent of the data subject is revoked, etc.¹⁶).

2.9 Big data: the lawful management of huge data sets

One of the most comprehensive definition available is probably that referring to big data as ‘*high-volume, high-velocity and high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight and decision making*’¹⁷. It normally refers, in first instance, to a huge mass of data that comes from a great variety of different sources and cannot be managed or analysed through conventional ‘local’ techniques standing on a single server or desktop computer.

BISON deals with big data because of the large amount of data collected, not of the sources. Possible issues generally related to big data which may apply to BISON include:

- big data analytics can involve **repurposing** personal data. If an organisation has collected personal data for one purpose and then decides to start analysing it for completely different purposes (or to make it available for others to do so) then it needs to make its users aware of this and a specific user consent is needed. This is particularly important if the organisation is planning to use the data for a purpose that is not apparent to the individual because it is not obviously connected with their use of a service (see in particular § 2.2.3 above on the ‘compatibility’ with declared purposes);
- a key aspect of big data is that they may in themselves **contrast** with the principle of **data minimisation** and **relevancy**. Collecting and processing big data might in principle raise questions, such as whether they may be excessive, or simply all relevant. The challenge for organisations is to focus on what they expect to learn or be able to do by processing big data before the beginning of processing operations, thus verifying that these serve the purpose(s) they are to be collected for, and, at the same time, that they are relevant and not excessive in

¹⁵ All data controllers must notify their national DPA before they start processing personal data, unless this obligation is not imposed by national law (Article 18 DPD). However, it is up to every Member State to provide simplifications and/or exemptions from notification when the processing of data does not appear to present any particular risk for the rights and the freedoms of the data subject, so that in many States a notification duty is imposed only for some categories of sensitive data and a few others, which may, however, include biometrics. Member States may also require a prior checking, to be carried out by the DPA, before undertaking data processing operations that may involve particular risks. What types of processing operations involve particular risks is an issue to be determined by each Member State. Again, biometric data processing is likely to be considered as a high level of risk processing for the abovementioned potential impact on the rights of individuals.

¹⁶These examples of security measures (that may significantly change in relation to the specific context and processing of data) are taken from the cited Article 29 Working Party Opinion 3/2012 on developments in biometric technologies.

¹⁷ Gartner IT Glossary, at <http://www.gartner.com/it-glossary/big-data>.

relation to such aim(s).

Both these issues are not immediately relevant for BISON, because all data used during the project are anonymized, so that they cannot longer considered as personal data.

In a possible future perspective, great attention has been paid by all BISON's partners to the data subjects from the very first step of data collection. In particular, focus has been put onto:

- providing adequate and punctual information;
- keeping into account the possible repurposing of the data for scientific research, while keeping in mind the notion of scientific research explained in § 2.6 above;
- taking care that the data are treated in respect to the relevancy and proportionality principles – for instance adopting anonymisation techniques and ultimately focusing on the legal duty to be fair, which involves taking account of the users' perspective and expectations.

At present, big data issues are extensively debated by politicians and researchers, for the huge potentialities of analytics technologies, their benefits and their potential threats to the protection of personal data and fundamental rights of individuals. Some authors deem it may be time to think, or re-think, of ethics for big data¹⁸, whose principles may serve as guidelines for controllers and other subjects involved in the processing of personal data.

However, the current data protection principles are inherently flexible. Big data are, still, data, and their large amount, or great capability of giving structured information about an individual, as well as the risks related with storage and fair processing, does not necessarily mean that basic data protection principles no longer fit for the purpose, or that a new data protection paradigm is necessarily required.

3. From the DPD to the General Data Protection Regulation – a general outline

3.1 The status of EU data protection legislation

As anticipated in D8.1¹⁹, a Proposal for a General Data Protection Regulation (GDPR) is currently being discussed and may soon be published in its final version and become applicable immediately after or even during the BISON project.

On 24th June 2015, just a few days ago, the first meeting between the European Parliament, the Council and the Commission (the so-said Data Protection Regulation Trilogue) took place to the purpose of reaching an agreement on the GDPR by the end of the year.

As stressed by Jan-Philipp Albrecht, representative for the EU Parliament for the Data Protection Reform, there are more points in common than points that divide the three Institutions: the European

¹⁸ Richards, Neil M. and King, Jonathan H., Big Data Ethics (May 19, 2014). Wake Forest Law Review, 2014. Available at SSRN: <http://ssrn.com/abstract=2384174>.

¹⁹ Deliverable 8.1 'Ethical approvals for the data' (M03), par. 6.

Parliament, the Commission, and the Council all agree on a number of critical elements that form the foundations of this reform.

The press conference²⁰ has actually confirmed some key principles:

- there will be a single set of rules, valid for all Europe;
- reinforced rights will be introduced to put people back in control over their data;
- the same rules will apply to companies from the EU and outside the EU;
- a strong and effective one-stop shop mechanism will be introduced to ‘simplify the lives of companies and citizens’;
- the 1995 Data Protection Directive is to be regarded to as the minimum level of data protection needed to guarantee in the reform.

Some issues, such as explicit consent and incompatible further processing, will need further thorough discussion between the competent Institutions.

EU Commissioner Věra Jourová explicitly affirmed that she is ‘confident that we can now deliver our new data protection rules to the European Union by the end of this year’.

We will keep the evolution of the GDPR constantly monitored and updated will be provided in the subsequent WP8 Deliverables.

The GDPR will substitute the EU Data Protection Directive and national laws currently in force, being directly applicable in the Member States’ legal systems²¹.

The GDPR aims at providing legal certainty and transparency for economic operators and ensuring individuals throughout Europe the same level of legally enforceable rights and obligations, as well as the same responsibilities for controllers and processors.

Different levels of protection in the various Member States are an obstacle for cross-border economic activities and the GDPR meets the need for a consistent and homogeneous application of the rules. This is important in particular in a context such as BISON’s where – in perspective, albeit not during the project’s lifetime – big biometric data may need to be processed.

The legal research in such a transition phase is far from easy, as rules may change at any time and possible modifications to the GDPR are presently not fully predictable. While we cannot ground our work on the upcoming rules as made public in their draft version up until now, we will keep a constant eye on any forthcoming news on this topic.

The objectives and principles of Directive 95/46/EC, however, are the level below which the GDPR shall not move – and above all are still in force, and will be in force for the next few years. We will therefore take them as the starting point and basic reference, while at the same time keeping a careful eye on the Proposal.

²⁰See http://europa.eu/rapid/press-release_STATEMENT-15-5257_en.htm.

²¹ European Commission - Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

Here we outline a general framework with the relevant points and will update and integrate it in the subsequent WP8 Deliverables, on the basis of the project's needs and of the evolution of the Proposal, until its final version will be published and the deadlines for adoption will be fixed.

3.2. A comparison between Directive 95/46/EC and the GDPR

This Section has been drafted based on the last available official version of the GDPR²² and has kept into account the subsequent official press releases and institutional discussions on the topic.

General scope

Directive 95/46/EC – It applies to the processing of personal data wholly or partly by automatic means, and to the processing other than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system. Exceptions: data processing concerning public security, defence, household activities, etc.

GDPR – Same general scope. New exception: data processing by EU institutions, bodies, offices and agencies.

What it means for BISON – If BISON is used by an EU entity falling in the exception, the GDPR does not apply and future specific regulation shall be taken into account.

Notification

Directive 95/46/EC – A general obligation to notify the supervisory authority is foreseen: the controller or his representative, if any, must notify the supervisory authority before carrying out any wholly or partly automatic processing operation or set of such operations intended to serve a single purpose or several related purposes. Simplifications or exemptions may be foreseen at national level in specific cases.

GDPR – The indiscriminate general notification obligation should be abolished, and replaced by effective procedures and mechanisms which will focus instead on processing operations which are likely to present specific risks to the rights and freedoms of data subjects. A data protection impact assessment should be carried out by the controller or processor prior to the processing.

What it means for BISON – The abolition of the notification will provide a substantial simplification of BISON procedures for CCs without at the same time reducing the level of protection of the data subjects. Both data controllers and data processors should actually perform a data protection impact assessment before carrying out processing operations, which may imply potential risks; such assessment should include in particular the envisaged measures, safeguards and mechanisms for ensuring the protection of personal data and for demonstrating the compliance with the GDPR. The Regulation points out that this assessment should in particular apply to newly

²² European Commission Com (2012) final, 2012/001 (COD), of 25.1.2012, available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

established large scale filing systems, which are intended to process large amounts of personal data and affect a large number of data subjects. This is the case of BISON, which – after project lifetime, in a commercial context - will imply the processing of big speech data.

Territorial scope

Directive 95/46/EC – The Directive applies to the processing

- a) carried out in the context of the activities of an establishment of the controller in a Member State,
- b) by a controller not established in the Member State, but in a place where its national law applies by virtue of international public law;
- c) by a controller not established in the EU who, to process personal data, uses equipment, automated or otherwise, situated in said Member State, unless such equipment is used only for purposes of transit through the Community.

In the circumstances of paragraph 1 (c), the controller must designate a representative established in that Member State.

GDPR – It applies to the processing of personal data:

- a) in the context of the activities of an establishment of a controller or a processor in the EU;
- b) of data subjects residing in the Union by a controller not established in the EU, where the processing activities are related to:
 - i. the offering of goods or services to such data subjects in the Union; or
 - ii. the monitoring of their behaviour.

It applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies by virtue of public international law.

<u>What it means for BISON</u> – If a CC established outside the EU acting as data controller uses BISON to offer goods or services to EU residents or to monitor their behaviour, it must comply with the EU Data Protection Regulation. If a CC established in the EU (data processor) processes data on behalf of a non-EU client (data controller) for the same purposes, it must comply with the Data Protection Regulation.

Conditions for consent

Directive 95/46/EC – The data subject's consent is defined: it is specified that it must be free, informed, explicit and unambiguous, and that it is one of the requirements for lawful data processing.

GDPR – Art. 7 specifies conditions for consent. The controller bears the burden of proof for the data subject's consent to the processing of his/her personal data for specified purposes. If the data subject's consent is to be given in the context of a written declaration, which also concerns another matter, the requirement to give consent must be presented distinguishable in its appearance from this other matter. The data subject shall have the right to withdraw his/her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

Consent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller (e.g. where the data subject is in a situation of dependence, such as in the case of an employee-employer's relationship).

What it means for BISON – CCs acting as data controllers should comply with art. 7 as concerns lawful consent. CCs acting as data processors should check that their Clients acting as data controllers have obtained a lawful consent in compliance with art. 7. BISON procedures should thus: a) make it possible to have a valid proof of lawful consent, b) allow the data subject to withdraw his/her consent at any time and which c) check in real time that the person to be called has not withdrawn his/her consent.

Direct marketing

Directive 95/46/EC – The data subject has the right to object, on request and free of charge, to the processing of his/her personal data for direct marketing, or to be informed before such data are disclosed for the first time to third parties or used on their behalf for the purposes of direct marketing, and to be expressly offered the right to object free of charge to such disclosures or uses.

GDPR – Same principle, in addition: the right shall be explicitly offered to the data subject in an intelligible manner and shall be clearly distinguishable from other information.

What it means for BISON – The information on the right to object to personal data processing for direct marketing purposes shall be explicitly and clearly made available, distinct from other information.

Security measures

Directive 95/46/EC – The data controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. The processor shall provide sufficient guarantees on technical security measures and organizational measures. The contract or legal act between controller and processor must specify that data processors must comply with security measures as set by data protection law as applicable in their own Member State.

GDPR – It is foreseen by law that not only the data controller but also the data processor must implement such appropriate technical and organizational measures. The measures shall be adopted following an evaluation of the risks.

What it means for BISON – As the new provisions are based on similar principles as the DPD, they should not imply a particular impact on the BISON procedures. There would be a simplified adoption of security measures, which will be based on one single set of rules and no longer on State law, which may set different security levels. BISON procedures should ensure GDPR abiding security measures when used by any CC (data controller or data processor). BISON should also comply with future implementing acts by the Commission specifying security measures requirements (e.g. to prevent unauthorised access to personal data, unauthorised disclosure,

reading, copying, modification, erasure or removal; ensure the verification of the lawfulness of personal data processing). Data processors and controllers should in addition carry out a preliminary risk evaluation. If done properly, this will guide them in setting up the most appropriate security measures.

Transfer of personal data to non-EU countries

Directive 95/46/EC – Personal data transfers outside the EU are only allowed if the third country in question ensures an adequate level of protection. Where the Commission finds that a third country does not ensure an adequate level of protection, Member States shall take measures to prevent any transfer of data to the third country in question.

Transfers of data to a country not offering an adequate level of protection may take place in specific cases, such as:

- with the consent of the data subject, or
- if the transfer is necessary for the performance of a contract between the data subject and the controller, or
- for the conclusion or performance of a contract made in the interest of the data subject between the controller and a third party, or
- if data are taken from a register which, according to applicable laws or regulations, is intended to provide information to the public and which is open to consultation.

GDPR – It is based substantially on the same principles. In addition, the rules on data transfer apply to personal data transfers to international organisations. The Commission may decide that not only a third country but also a processing sector within that country does not offer an adequate level of protection. In such case, personal data transfer shall be prohibited unless appropriate safeguards, standard data protection clauses or binding corporate rules are adopted.

As to data from public registers, the transfer shall not involve all personal data or entire categories of personal data. When the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

What it means for BISON – As the new provisions are based on similar principles as the DPD, they should not imply a particular operational impact on the BISON procedures. BISON should be developed and used keeping in consideration the limits set by the GDPR on data transfer to third countries and international organisations and enabling CCs who use it to comply with the applicable rules. Attention should be paid in particular to the Commission decisions on what countries *and processing sectors* within a certain country do not offer an adequate level of protection.

3.3 New GDPR provisions in the BISON perspective

Identification of the data subject – actions by controllers

If the personal data processed by the controller do not allow the identification of a natural person, the controller shall not be obliged to acquire additional information to identify the data subject for the sole purpose of complying with the GDPR.

What it means for BISON - No special functionalities need to be foreseen in BISON to enable the identification of natural persons from non-identifying data processed by the system.

Data protection policies

The controller must have transparent and easily accessible policies on data procession and data subjects' rights. It must provide information in a clear, intelligible form, in plain language.

What it means for BISON – Data subjects should be enabled to receive transparent, clear information on how BISON processes their personal data and have easy access to it.

Strengthening of data subject's control rights on data

Right to be forgotten and erasure of personal data have been strengthened.

What it means for BISON – BISON must enable data controllers and processors to perform a law-abiding personal data erasure, e.g. when data are no longer necessary, when the data subject has withdrawn consent or objects to processing, when processing is not compliant with the GDPR.

Data portability

The right to data portability has been introduced. Data subjects should be enabled to transfer personal data to a new online service provider.

What it means for BISON – Data controllers should be able:

- a) to extract a copy of all personal data to be processed with BISON in an electronic and structured format to be handed to data subjects upon their request;
- b) to allow data subjects to transmit their personal data and any other information provided by them and retained by an automated processing system into another one, in an electronic format.

Responsibilities of data controllers

New responsibilities and tasks have been imposed on data controllers.

What it means for BISON – Data controllers should adopt policies and implement appropriate measures to ensure and be able to demonstrate law-abiding personal data processing. E.g. keep documentation, implement data security requirements, perform a data protection impact assessment, comply with prior authorisation or prior consultation requirements; designate a data protection officer. They must implement mechanisms to verify the effectiveness of such measures, also by way of independent internal or external auditors.

Documentation of processing

A requirement to keep adequate documentation on processing activities has been imposed on both data controllers and data processors.

What it means for BISON – Data controllers and processors shall maintain documentation of all processing operations under their responsibility (e.g. name and contact details of controller and data protection officer, if any; purposes of processing; description of categories of data subjects and of categories of personal data relating to them; recipients or categories of recipients of personal data; transfers of data to third countries; time limits for erasure of the different categories of data; description of measures implemented by data controllers for lawful processing).

Data protection by design and by default

New obligations have been imposed on the controller arising from the principles of data protection by design and by default. Based on the state of the art and cost of implementation, appropriate technical and organisational measures to implement such principles should be adopted.

What it means for BISON – BISON shall by design implement mechanisms to enable data controllers to ensure that the principles of necessity and data retention are ensured. In particular, such mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals.

Data processors

The role and tasks of the data processor have been defined more clearly and stronger responsibilities have been foreseen.

What it means for BISON – BISON should enable CCs operating as data processors on behalf of a controller to provide sufficient guarantees to implement appropriate technical security and organisational measures and procedures to ensure compliance with GDPR and protection of data subjects' rights.

Processing by a processor shall be governed by a contract or other binding legal act with the controller, stipulating in particular that the processor shall:

- a) act only on instructions from the controller, in particular, where data transfer is prohibited;
- b) employ only staff committed to confidentiality or under a statutory obligation of confidentiality;
- c) take all required security measures;
- d) enlist another processor only with the prior permission of the controller;
- e) create in agreement with the controller the necessary technical and organisational requirements to respond to requests for exercising the data subject's rights;
- f) assist the controller in ensuring compliance with the obligations on security, notification of data breach to supervisory authorities, communication of data breach to the data subject,

impact assessment and prior authorisation;

- g) hand over all results to the controller after the end of the processing and not process the personal data otherwise;
- h) make available to the controller and the supervisory authority all information necessary to control compliance with GDPR obligations.

Data processors shall document in writing the controller's instructions and their own obligations.

Processors should not process personal data other than as instructed by the controller, otherwise they shall be considered to be a controller in respect of that processing and shall be subject to the rules on joint controllers, including all obligations imposed on controllers by the law.

Notification of personal data breaches

An obligation to notify personal data breaches to the supervisory authority has been introduced, building on the personal data breach notification in Article 4(3) of Directive 2002/58/EC, known as e-privacy Directive.

What it means for BISON – In case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 24 hours after having become aware of it, notify such breach to the supervisory authority. If not made within 24 hours a justification is needed.

The processor shall alert and inform the controller immediately after the establishment of a personal data breach.

The controller shall document any personal data breaches, including the facts surrounding the breach, its effects and the remedial action taken. This documentation must enable the supervisory authority to verify compliance with the GDPR.

If a data breach occurred in BISON, it should be possible for the data controller to detect it and take appropriate action as soon as possible.

Communication of personal data breaches

After having notified the data breach to the supervisory authority, a further obligation has been imposed on data controllers. In case a personal data breach may adversely affect the protection of the personal data or privacy of the data subject, the controller shall also communicate the personal data breach to the data subject without undue delay.

What it means for BISON – CCs which are data controllers shall adopt a procedure to communicate personal data breaches.

The communication shall not be required if the controller demonstrates to the satisfaction of the supervisory authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the personal data breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

Impact assessment

If processing implies specific risks to the rights and freedoms of data subjects owing to its nature, scope or purposes, the controller or the processor shall carry out an assessment of the impact on data protection of the envisaged processing operations.

What it means for BISON – Some BISON processing operations may present specific risks; the controller or the processor should therefore carry out an impact assessment.

Risky processing which may in particular concern BISON include.

- *a systematic and extensive evaluation of personal aspects; analysis or prediction of economic situation, location, health, personal preferences, reliability or behaviour of a person, on the basis of automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual;*
- *information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale;*
- *biometric data in large scale filing systems;*
- *other processing operations for which the consultation of the supervisory authority is required.*

The controller should seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of the processing operations.

Prior authorisation and prior consultation

In specific cases, the data controller and the data processor must request an authorisation from the supervisory authority prior to the processing of personal data.

What it means for BISON – In its actual business use, BISON may imply the transfer of personal data to non-EU countries. To this purpose, the controller or the processor should obtain an authorisation from the supervisory authority before processing personal data, in order to ensure the compliance of such processing with the GDPR and, in particular, to minimize the risks involved in the transfer of personal data to a third country or an international organisation.

The controller or the processor should consult the supervisory authority before processing personal data to ensure compliance with the GDPR and to mitigate the risks for the data subjects where:

- an impact assessment indicates that processing may present a high degree of specific risks; or
- the supervisory authority deems it necessary to carry out a prior consultation on processing likely to present specific risks.

If the supervisory authority deems that the intended processing does not comply with the GDPR, in particular where risks are insufficiently identified or mitigated, it may prohibit the intended processing and make appropriate proposals to remedy such incompliance.

The supervisory authority shall publish a list of the processing operations subject to prior

consultation; BISON partners should keep updated on this issue.

Designation of the Data Protection Officer (DPO)

The GDPR introduces a mandatory data protection officer for the public sector; as concerns the private sector, it is foreseen for large enterprises or whenever the core activities of the controller or processor consist of processing operations requiring regular and systematic monitoring²³.

What it means for BISON – The GDPR foresees a new figure, to be appointed in specific cases, which may involve BISON CC users, in case:

- processing is carried out by an enterprise employing 250 persons or more; or
- the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.

In other cases, appointing a DPO is a faculty, which may be exercised either by individual controllers or processors or by associations and other bodies representing categories of controllers or processors (e.g. contact centers).

DPOs should have specific professional qualities, in particular an expert knowledge of data protection law and specific practices and abilities to fulfil their tasks, which are focussed on monitoring the correct application of the GDPR and internal policies of the data controller and processor.

²³ This provision is based on Article 18(2) of Directive 95/46/EC, which provided the possibility for Member States to introduce such requirement instead of a general obligation to notify DPAs.

4. BISON data processing procedures

BISON shall be adopted by contact centers as an automated tool, which will enable them to accurately and effectively process big speech data and provide better services to customers on the basis of the outcome of such data processing.

BISON will therefore be part of new operational procedures by CC. These will necessarily start from CCs ante-BISON ‘traditional’ working procedures, which need to be law-abiding in the first place.

BISON, in addition, will provide further processing possibilities not available before and enable users to process large quantities of data over a short time, thus potentially making data processing more invasive for data subjects’ rights.

To provide a possibly complete general framework to guide BISON technical partners in developing a law-abiding system and CC partners in adopting correct procedures, we have focused on three points of view:

- 1) personal data processing ante BISON (traditional data processing by CCs);
- 2) data processing in the BISON project;
- 3) law-abidingness of BISON results (BISON in action in a real-life commercial context).

4.1 Lawful data processing procedures in contact centers (ante BISON)

BISON will have to be rationally integrated in its users’ (contact centers) daily procedures. Therefore, we need not only focus on the legal implications of the development and use of BISON results by themselves but in the context of consolidated business practices, so that the whole process of data processing, from the original recording up to its final destruction are compliant with applicable rules and regulations. For this reason, in the following we analyse the individual cases of BISON CC partners.

A. ComData

Adoption of key data protection principles

In order to fulfil the key data protection principles, ComData keeps its processes within the Czech Data Protection Law that imposes several obligations²⁴.

The administrator may process personal data only with the consent of the data subject. Without such consent, the administrator can process personal data only:

- a) if it is necessary to comply with a legal obligation of the controller, or
- b) if the processing is necessary for the performance of a contract to which the data subject is party, or

²⁴ ZÁKON ze dne 4. dubna 2000 o ochraně osobních údajů (Law of 4 April 2000, on the protection of personal data), available at <http://www.cz-museums.cz/UserFiles/File/Legislativa/zakon-101-2000.pdf> (in Czech language).

-
- c) for negotiations on the conclusion or alteration of a contract on a proposal from the data subject.

It has to be specified the purpose for which the personal data will be processed. Personal data may only be collected for - and processed only in accordance with - the purpose for which they have been collected.

Personal information may be processed for any other purpose only within the limits of the provisions of § 3 para. 6 of the Czech Data Protection Law (e.g. processing by intelligence services, by the Czech police for crime prevention, the Ministry of Finance, for national security purposes, etc.), or unless the data subject has given prior approval.

Information and consent

At the beginning of any interaction with the customers, the operator asks if they have time and if they agree with a recorded and monitored call. In case of a positive answer, the operator continues with the interaction, if not the call is ended.

Besides this, the operator also asks some security questions (date of birth, address, complete name, ID number) in order to assure that the conversation is being held with the correct person.

The explicit authorization from the customer is contained in the recording.

Anonymisation

In the normal transactions with customers, anonymisation is not foreseen, all recordings must be kept complete in order something is necessary to clarify with the client.

Therefore, no process of anonymisation is performed.

Security measures

In order to protect personal data ComData adopts the following process.

Recordings are stored in the company's internal repositories that are not accessible from the Internet or from a local network.

Access to them is possible only through a special application with the appropriate authority, communication is encrypted by SSL, and user access rights for exports are logged.

Recordings are stored in data warehouses, which are accessible only from specified IP addresses in inner network and stored for one year or other period that is contractually specified by the client.

Outside the internal network, VPN Firewall built on Fortigate is used to access recordings

Data transfer between controller and processor (from clients to ComData) and processing procedures by the processor

This process is adapted based on the requirements of each client. Sometimes clients are stricter in terms of the processes, while sometimes the requested data transfer is less complex.

In the following, we mention the current processes set with the clients.

Data transferred by e-mail

ComData gets the database from its clients via normal e-mail as encrypted files. The next step is to merge the received files, adjust them and move them to an excel file so they can be allocated to the company's system.

Entrance into the Helpdesk is a requirement to set up the database. It checks duplicities and black lists. These are the lists which contain the phone numbers of customers who already asked not to be called anymore and that ComData cannot process under any circumstance. Such data are removed from the Database and allocated in a special part of the system, which prevents any call to them. Then the system informs ComData that it can start using the database for calling. The database is uploaded to the application, which handles the database.

The clients as data controllers assure that they provide only personal data that ComData is allowed to use for the purposes that were agreed in the contract.

Data in the Client application

ComData stores personal data in a client's application where it has to log in. Every employee uses its own login, which contains a user name and unique passport credential, in compliance with applicable law.

An operator who handles calls only creates a contact card with all needed information such as name, surname, etc.

Data storage system

The Client stores data on a so-called FTP-based data storage system. It has been chosen as the option with highest security about data protection. There is a special data storage system allocated in ComData server where the client specifically allocates the data. It is a very secure option because is protected by the company's firewall and only accessible in compliance with strict security permissions.

On the basis of the detailed database, if necessary, ComData adjusts the operator card to make sure that everything is consistent when uploading the database. ComData adds the requirement to deploy the database to its system; this is basically referred to the request to the internal IT department to get ready to use the database.

It is also possible to select inefficient data from the database. 'Inefficient data' refers to all the data that ComData is not able to process, such as for example, non-existing numbers, faxes, no one answering the phone, etc.

Just by the act of simple calling, the operator marks in the card the status of the contact and ComData stores the result of the call.

The entire call is stored for the period foreseen in the contract. The Client, both during the calls or after their termination, has an overview of the conditions of its database.

Once the database has been completed, in other words after all the usable numbers have been called, or when the campaign ends based on the deadline set by the client, ComData puts the processed data back to the FTP server, where the client can download this new version. However, this function is not requested by all clients.

B. Ebos

Adoption of key data protection principles

Ebos acts as data processor and as such strictly follows its clients' (data controllers) written instructions.

It processes data for the sole purpose of the services described in the General Agreements, Services Orders, Work Orders and the Temporary Missions of its Clients, complying with applicable national and EU data protection and privacy rules and respecting principles of correctness.

Processing of customers' personal data is strictly limited to those needed to achieve the purpose of the customers' call, either to call back, send a letter or an e-mail. Existing data are verified and updated or corrected as needed.

Outbound call time is restricted to 10.00 a.m. until 8.00 p.m., excluding lunch time.

Prior to being connected to an operator, the customer is informed that the call will be recorded and he/she is given the opportunity to object.

During the call, before processing any personal data, the operator explains the reason why personal data are needed and asks for the customer's consent.

Personal data which are collected, updated or corrected during a call are directly inserted into the clients' CRM system which is controlled by the client and stored **on clients' server**.

No personal data are ever stored on Ebos servers.

All Ebos employees sign an addendum to their contract advising them on data privacy & personal data protection rules.

In its role as data processor, Ebos does not control the retention or destruction of customers' personal data.

Personal data are retained in the Client data base as long as needed for business purposes and destroyed by a routine set by the Clients (data collectors) according to national rules and regulations. Appropriate technical and organisational measures are implemented to ensure the protection of all data.

Information and consent

Customers calling Ebos are connected to an IVR (Interactive Voice Response) system, where they will first be given a language choice and then before being connected to an operator they will:

- a) hear a message informing them that his call will be recorded for quality control purposes; if the customer does not agree to the recording he/she is given the opportunity to press 1, which **hinders** the recording.
- b) during the call prior to collecting, updating or correcting personal information, the operator explains why personal data are needed and asks for the customer's explicit consent.

Anonymisation

In its normal business activities, Ebos does not proceed to anonymisation of personal data, all data are owned and controlled by its clients.

Ebos does not store any personal data in any of its own systems.

Personal data are retained in clients' databases as long as it is needed for business purposes and destroyed by a routine set by the Clients (data controllers) according to the local regulations.

Security measures

Ebos protects data against accidental loss, falsification, unauthorised disclosure or access to them on its premises.

Unauthorized persons are prevented from accessing the facilities used for data processing.

All entries are closed and equipped with an electronic access card reader. Buildings can only be accessed by authorized staff having an access card. In case of loss or theft of cards these are deactivated.

People not provided with an access card have to go to the main entrance, which is equipped with a camera.

Data are protected from being read, copied, amended or moved by any unauthorised person.

Ebos computer systems can only be accessed with a personal login-in and password and are protected against external access by a firewall.

Passwords have to be changed regularly.

Access to CRM systems is also protected with a login set by the client and a personal password.

Login-ins are communicated to each collaborator after having successfully passed the initial training phase and are not to be shared with any other employee.

Authorized persons using a CRM system can only access data that are within their competence.

When an employee leaves the company for any reason, his/her account is blocked. If an employee forgets his/her password, he/she will be asked to enter a new password following his/her request.

Operators must lock their workstation when leaving the workplace.

Data processing systems are protected from being used by unauthorized persons using data transmission facilities. USB stick ports are blocked.

All data including sensitive data are protected in the same way.

All operators sign a contract addendum advising them on security measures.

Call recordings are stored on an FPT server in a highly secured Data Center.

Access to the FTP server is password protected and only possible for administrators.

All data are duplicated; it means that they are stored simultaneously on two different servers.

Ebos Luxembourg does not perform a formal previous risk analysis.

Data transfer between controller and processor (from clients to Ebos) and processing procedures by the processor

Collection and recording of speech data:

Ebos is in the process of migrating to VoIP technology, which implies that:

- calls for the BISON project activities are recorded via a single telephone exchange located at Ebos Belgium;
- when calling in the customer is informed that his/her call will be recorded, prior to being connected to an operator;
- calls are only recorded if the customer has not objected prior to being connected to an operator as described above;
- recordings (Wav files) are automatically renamed according to Call ID, the relevant number and the operators' name;
- the renamed Wav files are sorted into different folders (by client) and stored on an FTP server at a highly secured Data Center in Belgium (not Ebos owned).

Access to the FTP server is password protected.

Storage, retention and destruction of personal data

Incoming and outgoing call recordings are stored in a highly secured Data Center (not Ebos owned), located in Belgium.

Via the FTP client 'Filezilla', administrators and supervisors at Ebos have access to the audio files stored on the FTP server. Supervisors have only access to the client project in their responsibility

As per local regulation, recorded calls are destroyed as a routine after 6 months, except for those which have been monitored by a supervisor. Monitored calls are kept for 1 year.

C. Telefónica

Adoption of key data protection principles

Telefónica is both data processor and data controller. Telefónica, in general, has no consent to communicate personal data to third parties. Therefore, in most of the cases, it processes personal data as data controller.

However, the Spanish Data Protection Law, Ley Orgánica 15/1999²⁵ (LOPD) allows a third party to process data as long as the third party has a legal relationship with the data controller and has a signed contract with the same compliance as described in art. 12 of LOPD and imposing security measures that apply in charge of processing. In these cases, this is transparent to the customer and consent is not required.

In order to fulfil the key data protection principles Telefónica keeps its processes within the respective national law, LOPD, which says it is obliged to specify the purpose for which the personal data will

²⁵ Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (Organic Law 15/1999 of 13 December, for the protection of personal data), available at <http://www.boe.es/buscar/doc.php?id=BOE-A-1999-23750>.

be processed. Data are used for commercial purposes, billing and for the performance the contract. These data follow the art. 4 of LOPD on ‘Quality of data’.

Telefónica also collaborates with the Spanish Data Protection Agency (Agencia Española de Protección de Datos, or AEPD) to interpret the law.

Information and consent

Telefónica informs the customer at the beginning of the call that the call may be recorded. This information is enough to obtain the consent. At the beginning of the call, the agent also asks some personal data (Name, Surname and ID card) to identify the customer.

At the end of the call, for specific cases like churn, new acquisitions, etc. the agent asks for a further customer’s consent.

For those that are already customers. Customers sign the contract which contains the general conditions, or ‘Condiciones Generales’.

For customers calling to Telefónica’s call center. Customers are informed at the beginning of the call, that the call could be recorded. This is the consent of the customer based on Spanish law. These data are processed internally (no third parties are involved).

For customers called. Telefónica only calls customers, who have given the consent to be contacted for commercial purposes and only to offer telco products, which are part of its core business.

For data subjects who are not yet Telefónica’s customers. Telefónica calls only in case it had previously obtained the consent to contact the customer, aligned with LOPD procedures.

Anonymisation

Anonymisation is not usually foreseen; Telefónica normally records the complete call, as it is needed for its business purposes (e.g. possible contestations by the client), in compliance with the law.

Security measures

All the recordings are stored in Telefónica’s internal repositories and data warehouses. Both infrastructures are included in the disaster recovery procedures for Telefónica’s data.

In order to protect personal data the procedure is as follows:

- recordings are stored in company’s internal repositories that are not accessible from the Internet or a local network;
- access to them is possible only through a special application with the appropriate authority;
- communication is encrypted by SSL;
- under the company’s security policy, different levels for user access rights are defined,
- the access of the different people is audited, checking who is accessing to specific data.

Further details on Telefónica’s security procedures are covered by non-disclosure and confidentiality obligations; however, it should be mentioned that it is submitted to external audits which ensure the procedures.

Data collection and transfer between departments (TME/TID)

At this moment, Telefónica does not transfer data from the recording platform to the datawarehouse.

When a department is interested to have access to recorded data, it has to justify why it is requesting such access. If said justification is accepted, the organization ensures a secured access for specific persons, following our security policy, to the repository where data are stored. Files only can be heard in this repository: they will be neither moved, not edited.

As concerns data collection and transfer between TME and TID, special contracts have been signed for the BISON project to correctly regulate data processing and anonymisation.

4.2 Data processing procedures in BISON project activities

In order to mitigate any possible risks to data subjects in project activities, the BISON project partners have agreed to only process fully anonymized data during project lifetime.

It should be highlighted that anonymisation is also relevant with reference to ante-BISON CC activities and in the perspective actual commercial use of BISON, as data controllers and processors should anonymise data whenever the goals of processing can be achieved without the use of identifying data, in compliance with the necessity principle set by EU law.

This Section will first provide a general framework on applicable EU rules on anonymisation and then focus on how BISON shall implement them in its general architecture and annotation activities.

4.2.1 Legal requirements for anonymisation

The **Data Protection Directive** does **not apply** to **data** rendered **anonymous** in such a way that the data subject is no longer identifiable. The concept of ‘personal data’ necessarily implies the possibility to identify – directly or indirectly – a natural person. The Directive does **not set any prescriptive standard**, it does not describe the de-identification process, but only its outcome, that is a reasonably impossible re-identification.

The concrete application of the general principle set by the Data Protection Directive, however, is far from easy: on the one side, it is difficult to create a truly anonymous dataset and at the same time to retain as much information as needed for a specific task. On the other side, irreversibly preventing identification requires data controllers to consider all the means which may ‘likely reasonably’ be used for identification, either by the controller or by a third party.

It should be mentioned that also the **e-Privacy Directive** imposes anonymisation in certain cases. As concerns traffic data relating to subscribers processed within electronic communications networks to establish connections and to transmit information, it foresees that, when used for marketing communications services or value added services (which is the case of BISON), **personal data** should be **erased** or **made anonymous after** the provision of the **service**.

Besides, it imposes the providers of a public communication network or publicly available electronic communication service to **erase** or **made anonymous data no longer needed** to transmit a communication.

In the BISON project, these latter provisions may in particular be of interest for CC partners.

A further reference point for BISON partners is **Article 29 Working Party (WP) Opinion on Anonymisation Techniques**²⁶. It describes the main techniques used to anonymise personal data and discusses in specific some of them, explaining their principles, strengths and weaknesses, possible mistakes and failures. Below a synthesis of the most relevant elements is provided.

The criteria on which Art. 29 bases its opinion on robustness focus on the possibility of:

- singling out an individual;
- linking records relating to an individual;
- inferring information concerning an individual.

As concerns the lawfulness of the anonymisation process, the Working Party starts from the assumption that personal data must have been collected and processed in compliance with applicable legislation.

Anonymisation is considered as ‘further processing’, which needs to comply with the compatibility assessment (e.g. data shall not be further processed for purposes incompatible with the purposes specified at the moment of their first collection) and with the basic principles set by art. 7 of the DPD.

According to the Working Party, **anonymisation** should be considered as an **instance of further processing compatible with the original purposes**, but **only** upon condition that the anonymisation process **reliably produces anonymised information**.

Although removing directly identifying elements in itself may not be enough to ensure the impossibility of re-identification, it should also be remembered the principle set by Convention 108: **identification with very sophisticated methods may not be relevant**, as it should not be possible to identify a person *readily*²⁷. Additional measures may often be needed to prevent identification. Such measures should be adopted in consideration of the context and purposes of the processing for which anonymised data will be used.

As observed by **Article 29** also in its **Opinion 03/2013 on purpose limitation**, ‘**anonymisation** is increasingly **difficult to achieve** with the advance of modern computer technology and the ubiquitous availability of information. Full anonymisation would also require, for instance, that any reasonable possibility of establishing a link with data from other sources with a view to re-identification be excluded. However, re-identification of individuals is an increasingly common and present threat. In practice, there is a very significant grey area, where a data controller may believe a dataset is anonymised, but a motivated third party will still be able to identify at least some of the individuals from the information released.

²⁶ Article 29 Data Protection Working Party – Opinion 05/2014 on Anonymisation Techniques adopted on 10 April 2014, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf

²⁷ See par. 2.2.6 on Convention 108, art. 2 par. 28 and art. 5, par. 42.

Addressing and regularly revisiting the risk of re-identification, including identifying residual risks, therefore remains an important element of any solid approach in this area.²⁸

De-identification is only the **first step**; the **second** one implies the application of **adequate safeguards**, whose strength should be proportionate to the adverse impact to the data subject of a possible re-identification. Examples of such safeguards may include, for instance, encryption, restrictions of access, etc.

As mentioned above, it is difficult to assess in advance whether re-identification may or may not be possible, since it depends on how readily and how directly the link between the data and the identifiers is structured.

Controllers should consider the concrete means that would be necessary to reverse the anonymisation process, their cost and know-how needed, as well as the likelihood and severity of implementing such means.

Data controllers should conduct a **data protection impact assessment** to decide what data may be made available for reuse and at what level of anonymisation and aggregation. An impact assessment should ideally be completed before disclosing information and making it available for reuse.

Whenever controllers release anonymised datasets for use, the risk assessment should include re-identifiability tests (e.g. penetration tests).

Data controllers should keep into account that the **risk of re-identification changes over time**, with the evolution of technology. Once rare and sophisticated analytics techniques are now commonly available at low or no costs.

Data controllers should therefore perform **periodic reviews** of their **policies** on the release of data and of **anonymisation techniques**, in consideration of current and possible future threats.

As concerns **data processors**, who may process anonymised datasets communicated to them by data controllers, they will be acting lawfully without needing to consider data protection requirements if they are not able to directly or indirectly identify the data subjects of the original dataset.

Before deciding if and how to use the anonymous data received by the data controller for their own purposes, they should in any case take account of the anonymisation techniques adopted by the data controller. Data **processors may** actually be held **liable** for **possible consequences** derived from their **own data processing**. If there is a risk of identification of the data subjects, the processing should be performed in compliance with data protection law.

The use of anonymised data may actually present some residual **risks**:

- in case of **pseudonymisation** (i.e. non-full anonymisation), data protection rules apply, as personal data are still being processed;
- full anonymisation may **deprive data subjects of safeguards otherwise foreseen** in relation to the use of their data (e.g. the prohibition to store information of any type, as foreseen by the e-Privacy directive on terminal equipment without the user's consent);
- in case of fully anonymised data, there may still be an **impact on data subjects**, especially as concerns **profiling**. Although the Data Protection Directive does not apply, individuals are

²⁸ Article 29 Data Protection Working Party – Opinion 03/2013 on Purpose limitation, adopted on 2 April 2013, available at http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf.

still protected by the European Convention on Human Rights and the EU Charter of Fundamental Rights; the use of **anonymised datasets** may lead to a loss of protection, e.g. in case such data are used, in combination with other data, to **make decisions which produce effects on individuals**, even if indirectly.

Different anonymisation techniques may be used, which may imply a different level of risk. Art. 29 Opinion outlines the risks of singling out, linking or inference, with respect to some of the most used techniques (e.g. pseudonymisation, noise addition, substitution, etc.).

As a concluding remark, as stressed also by Art. 29, anonymisation can protect privacy and personal data rights; however, this can only be achieved if anonymisation techniques are engineered and applied properly: context and objectives of the process must be clearly set to achieve the desired anonymisation level.

4.2.2 BISON general dataflow

In this Section we discuss the BISON dataflow, highlighting where and how anonymisation takes place.

Owing to the different internal organisation of BISON partner CCs, small differences in the dataflow may occur, and are discussed below. Different data flows apply in different BISON stages; therefore, we will discuss them separately.

A. First stage of BISON project research

In the initial stage of the BISON project, data flow is performed according to the diagram in Figure 1. The starting point is the audio file (Wav) of the call: of course, the call contains personal data.

The call is examined by a supervisor (a ComData, Ebos or Telefónica employee/collaborator, also called Master Annotator in CC's internal lexicon), who is the only authorised person to access personal data, with the specific purpose of intercepting any personal data in the audio call and manually removing them by 'silencing'. This latter is a practice by which the personal datum is physically overlapped with a silence, an audio beep, or alike. The result is a new audio file which contains no personal data: therefore, from this point in the data flow (red cross in the diagram), data can be considered fully anonymised.

The anonymised call is then processed by the annotator. It is a person who annotates the call according to the technical specifications defined by Phonexia: the resulting annotated file is either made available to the BISON partners of interest (Figure 1 – case of Ebos and ComData) and used for extracting statistics and features, exploited in their turn to improve the audio recognisers, or (Figure 2 – case of TME) processed internally, delivering to TID – another BISON partner – only the result.

Figure 1 – Ebos and ComData

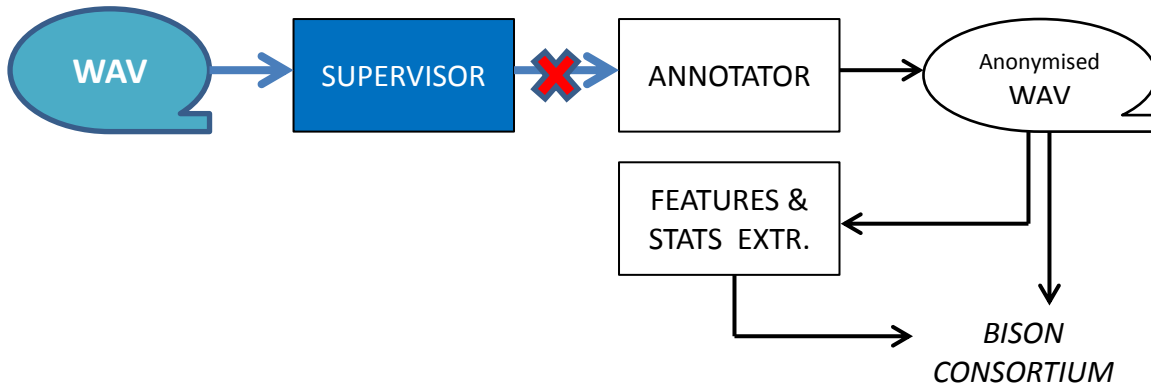
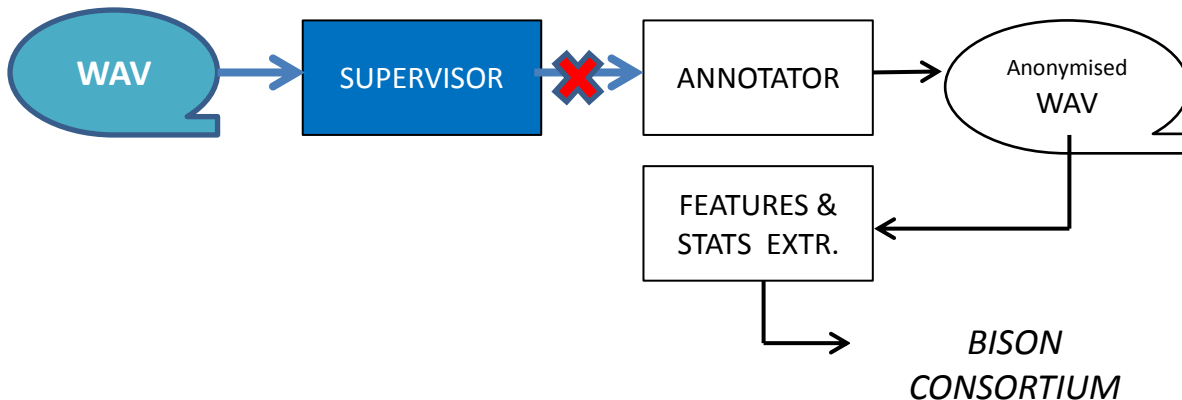


Figure 2 – TME/TID



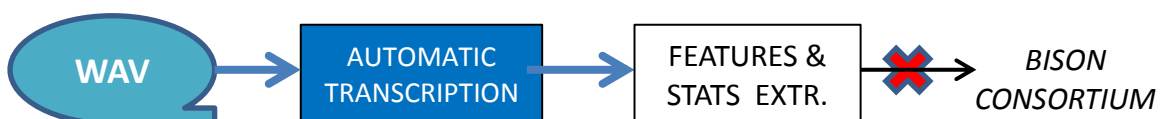
B. Second stage of BISON project research

Since BISON aims at handling huge amounts of speech data, the manual annotation of personal data by the supervisor, as synthesized above, cannot be maintained: therefore, automatic transcription – for all the supported languages – will be used, changing the point where anonymisation occurs.

The new dataflow is shown in Figure 2: again, the starting point is the audio file of the call, which contains personal data. The file is now subject to automatic transcription: unlike the first-stage procedure, there is no human supervisor silencing any personal data by hand.

Although the automatic transcriber might be able to intercept many terms and items automatically, the result of such ‘partial anonymisation’ cannot be considered 100% sure: thus, the result of this process should be considered as still containing (possibly a small amount of) personal data.

The next step is the extraction of statistics: results are just aggregated figures, no longer containing any personal data (see the red cross in the diagram). These data are made available to the BISON consortium, for improving the recognisers with all languages and huge data amounts.



C. After the BISON project (2015-2017) – Business operation

When bigBISON will be fully operational in a business context, Figure 2 will still apply: however, the extraction of statistics will be performed in each CC by the CC itself, so that no personal data will be ever delivered outside.

4.2.3 Anonymisation procedures in BISON (annotation)

ComData

- The Master Annotator retrieves recordings (Wav file) from internal Comdata server.
- The Master Annotator separates calls from stereo recording to two mono channels.
- The parts containing personal data are silenced using the ‘Audacity’ tool and file is renamed according to agreed convention.
- The anonymised Wav files are then saved in the annotators files to be annotated (each annotator has his own file and has only access to this file, while the Master Annotator can access all.
- The Master Annotator checks the annotation, corrects it if identifies minor issues, asks annotators to correct them and sends the file to Phonexia.

The process in detail is as follows:

Description of anonymisation of sensitive data from the call:

- 1) Selection of records
- 2) Listening to records (both channels - client and operator)
- 3) Identification of personal information in individual channels (e.g. address, social security number, account number, card number, telephone number, e-mail address, date of birth, etc.)
- 4) Personal information is covered with other audio signal (silence or beep) - records are not shortened but sensitive data are replaced by another signal

The annotation of personal data is performed as follows:

- 1) Symbols ‘//’ are used for designation of personal information in a record (e.g. operator’s surname – e.g. Vendula // Otáhalová)
- 2) Segment with sensitive information that has been replaced by an audio signal (anonymisation) is annotated using a predetermined mark (eg. ..., ‘X:’ or ‘%%’).

Ebos

The Master Annotator (MA) Verena Hoffeld is responsible for selection and anonymisation of speech data selected for BISON activity

Master Annotator checks and corrects transcribed/annotated speech data.

Furthermore, MA is responsible for the deletion of original call recording selected for the BISON project.

The Master Annotator has access to the calls stored on the FTP server and copies selected calls via 'Filezilla' to a specific 'Bison' folder on his PC.

The process can be outlined as follows:

- The Master Annotator retrieves the recordings (Wav files) from the secured central data center and copies them to the Ebos server in Luxembourg.
- The Master Annotator sorts the calls by length and makes a selection (ideally 4-6 min).
- The Master Annotator listens to the calls to check their quality, eliminating those having too much crosstalk.
- The Master Annotator *deletes any personal data* by silencing them via the 'Audacity' tool: the output file is renamed according to an agreed convention.
- The anonymized audio Wav files are saved in the annotators' files to be annotated (each annotator has his/her own file and has only access to this file – only the Master Annotator can access all).
- The Master Annotator checks the annotation, corrects any minor issues if necessary (or asks the annotator to do so) and sends the final annotated file to Phonexia.
- The original copy of the Wav file is deleted from Ebos Lux SA as a monthly routine.

Calls are selected by amount of speech data (5- max 15 minutes of speech) and saved temporarily in a folder on the Master Annotator's PC desktop.

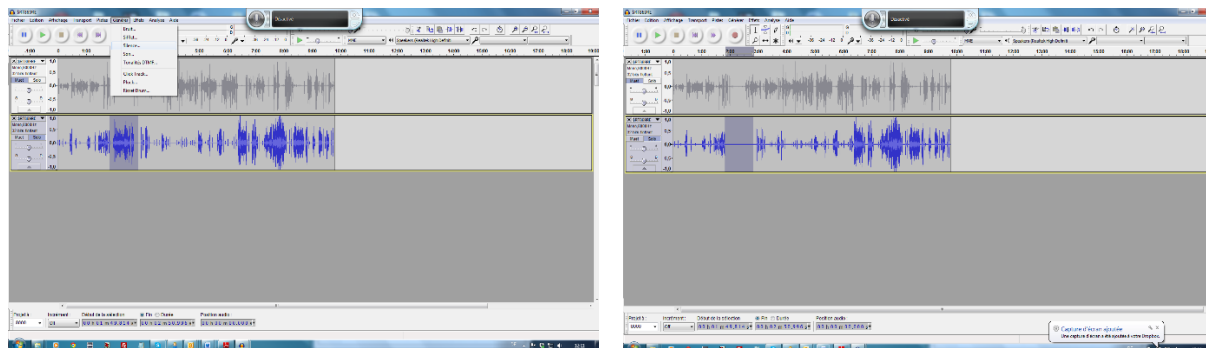
The MA listens to the selected Wav files to spot personal data and proceeds to anonymisation of all data enabling the identification of a data subject.

To proceed on anonymisation of the customers' personal data and metadata Ebos MA uses the tool 'Audacity'. This tool allows to work on recordings (Wav files) by either masking speech signals with a strong sound signal or by replacing the selected part of speech signals containing personal data *by full silence*. The recordings are not shortened.

For BISON purposes, all parts containing personal data are replaced by full silence; this means no more speech signals can be detected.

As documented below, the parts containing personal data are marked and replaced by silence.

AUDACITY SCREENSHOTS



The Wav file is then exported by the master annotator from ‘Audacity’ to the ‘annotator’ folders for further processing, meaning transcription & annotation.

When exporting the Wav file, the original Call ID (containing date and time of call, the name of the operator, the number called or calling) is replaced by a new identification number as agreed with BISON Partner Phonexia (e.g. fr 0001) consisting of the language of the speakers and a number (range starts at 0000). Thanks to this de-identification, it is impossible to link the call to the original call saved on the FTP server or data saved in clients’ data base.

The fully anonymised (Operator & Caller personal data) Wav files are stored on a local Ebos server, in ‘annotator’ folders for further processing, meaning transcription and annotation of the calls.

Annotators have only access to their own folder; the Master Annotator/local IT administrator can access all annotator files & folders.

Double security: in case an annotator still finds personal data, having been accidentally overheard by the MA, he/she marks the segment and informs the MA who will replace the data by silence as described above.

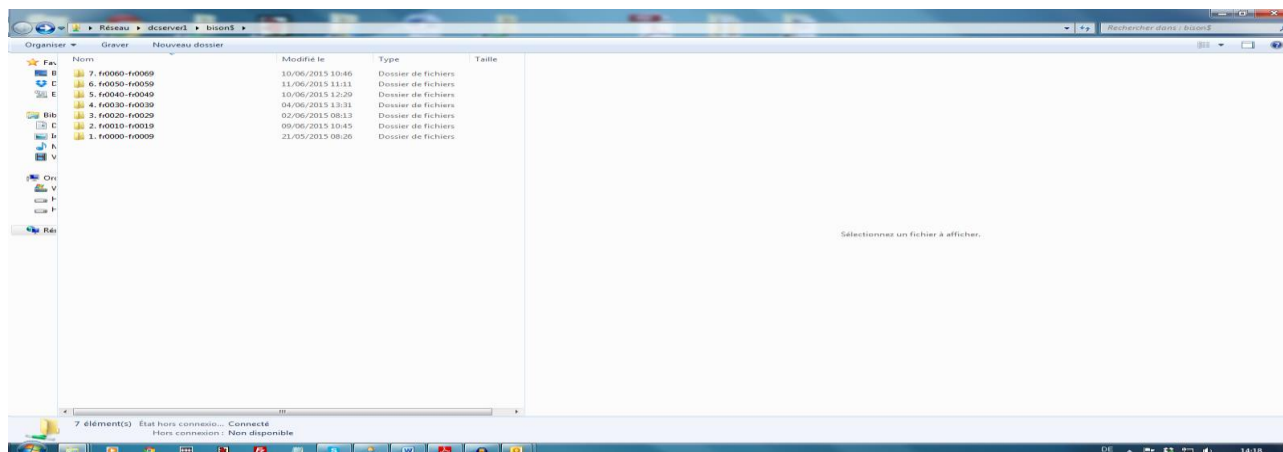
The MA annotator checks and corrects the completed annotation files on a daily basis.

The MA transfers the corrected files (transcription files + Wav files) to a password protected FTP server created for the BISON purposes on Ebos server in Luxembourg, which can only be accessed by the local IT administrator, the Master Annotator and BISON Partner Phonexia.

Phonexia has been provided with instructions on how to access to this FTP server and can retrieve the anonymised files directly from Ebos server for further BISON processing activities.

The files are classed in batches as per agreed file naming convention e.g.: 1. fr0001-fr0009

FILES ON SERVER SCREENSHOT



Telefónica

For the BISON project, Telefónica deletes the personal data of all the calls delivered to the project and then annotates them.

The process is as follows:

- Telefónica gets the audio files in Wav format with the recorded call;

-
- It anonymizes the recorder call deleting all the personal data and creating a new Wav file anonymized;
 - the anonymized Wav files are passed to the annotators who annotates the data inside the call;
 - the Master Annotator will check everything is right and act following the guidelines defined by Bison.

4.2.4. File destruction in BISON

ComData

The file destruction at ComData is always agreed upon with the client and is regulated in writing in the contracts.

The main conditions are set as follows:

- Time for keeping the recordings – the most common period is one year (anyway it can be longer or shorter based on the client's request). After the set period, the system erases recordings automatically. Then there is no way how to find them any longer. They are erased forever.
- Time and process for giving data back to the client – these are also agreed upon with the client; the most common way foresees the use of an encrypted – firewall secure server, but they can be also delivered in a CD-ROM or DVD ROM.
- Approved people that will have access to the information – only selected approved people may access the data, e.g. the IT department, the Project Manager, etc.

As a concluding remark, we can affirm that the File destruction is performed according to the needs of each single client and based on its requirements.

Ebos

After having fully anonymised the selected calls and having saved them on the 'BISON' FTP server in local Ebos network, the Master Annotator permanently deletes the original calls, which had been previously saved on her PC.

Telefónica

All the recordings are destroyed after a month the call was done.

For BISON, original calls will follow the same process. Destruction procedure implies the erasure of the audios from the repository where they were recorded.

However, once the call it is anonymized, it can be used for the whole project duration.

4.3 Law-abidingness of BISON results

At present, BISON is at its design and development stage and smallBISON is still to be achieved. Therefore, we hereby envisage what issues should be considered at this stage in order to achieve results which comply with applicable rules, in particular but not exclusively with data protection law.

4.3.1 Information, consent and data collection

Contact centers acting as data controllers – Personal data are usually collected directly from their own final customers (natural persons). CCs have the legal obligation to provide **information** on data processing and get explicit **consent** by the data subject before the first recording of the data.

In order to be valid, the consent should be referred to specific purposes and activities, such as for example:

- a) improving the CC service to the customer;
- b) commercial purposes (e.g. marketing, direct selling, statistics, etc.);
- c) profiling;
- d) geolocation;
- e) communication of data to third parties (e.g. partner companies) who may use them for commercial purposes;
- f) transfer of data to non-EU countries.

If such different purposes - instead of being separate and requiring separate consents - were all put together in one single meta-purpose, a single approval by the data subject may be deemed as an invalid, not freely given, consent.

The practice of imposing *de facto* the ‘commercial’ consent to the data subject together with the signature of a contract made with the data controller may also not be deemed a valid consent.

If not only common but also sensitive data are to be processed, the consent should also make specific reference to them.

It should also be remembered that consent is not the only legal ground to process personal data; for instance, consent is not required when processing personal data is needed:

- for the performance of a contract to which the data subject is party, or
- to take steps at the request of the data subject prior to entering into a contract, or
- to comply with a legal obligation, etc.

At present, conditions for consent differ in the various Member States, ranging from a general requirement of the written form to implicit acceptance.

The GDPR has strengthened the data subject’s consent, which should:

- be given explicitly by any appropriate method;
- enable a freely given specific and informed indication of the data subject’s wishes;
- consist either by a statement or by a clear affirmative action;

-
- ensure that the data subject is aware that it is giving its consent to the processing of personal data.

Silence or inactivity should therefore not constitute consent.

Consent is not valid if the individual has no genuine and free choice and is subsequently not able to refuse or withdraw consent without detriment.

If the data subject's consent is given in the context of a written declaration which also concerns another matter, the requirement to give consent must be presented *distinguishable in its appearance* from this other matter.

The data subject shall have the right to withdraw his/her consent at any time.

The controller bears the burden of proving that a valid consent has been given.

The first information and consent are usually provided on a one-to-one basis, for instance when a contract is signed between the data subject and the data controller or when the data subject first registers at the controller's web site to request services, information or to have access to resources, etc. Personal data are not gathered in a massive way.

In a second moment, the data controller may need to use the personal data for further purposes not originally present in the information or not first accepted by the data subject (e.g. profiling), also to be able to process them with BISON. The telephone operator at the CC will therefore have to provide a new information notice or an integration to the original one and get the data subject's explicit consent.

Contact centers acting as data processors – Personal data are collected from their clients, who in turn act as data controllers. The burden of responsibility to provide the information and get the consent lies with the controller, while the processor is bound to act in compliance with the instructions received by the data controller.

Data providers may also, in a second moment, need to use personal data for further purposes not originally present in the information or not first accepted by the data subject (e.g. profiling), following the requests of their Client. In this case, they will also have to provide a new information notice or an integration to the original one and get the data subject's explicit consent.

Numbers from telephone directories

If a CC intends to collect data taken from telephone directories and not from Clients' (or own) databases to use them for commercial purposes, it should do it in compliance with applicable 'opt out' rules.

Example: in Italy, a CC may call a telephone number from the telephone directory for commercial/marketing/direct sale, etc. purposes unless it is inserted in the 'Public Register of Oppositions'. The lists of numbers of the Public Register are periodically updated and available for sale²⁹. A number inserted in the Public Register may however be lawfully contacted if the controller or processor has otherwise got the owner of the line's consent to receive commercial calls (e.g. in the context of a contract).

²⁹ Further information on Italian telemarketing rules for operators is available at the following link: <http://www.registrodelleopposizioni.it/en/operators/operators-home>.

Tips for BISON Guidelines

Data protection information notice should have the content foreseen by law.

Informed consent has to be obtained before the first recording of data.

Consent should be explicit, not implicit.

Consent should refer to specific, defined purposes.

Data may only be processed for a specific purpose if the data subject has given his/her consent.

Controller and provider should be able to give evidence of the data subject's consent.

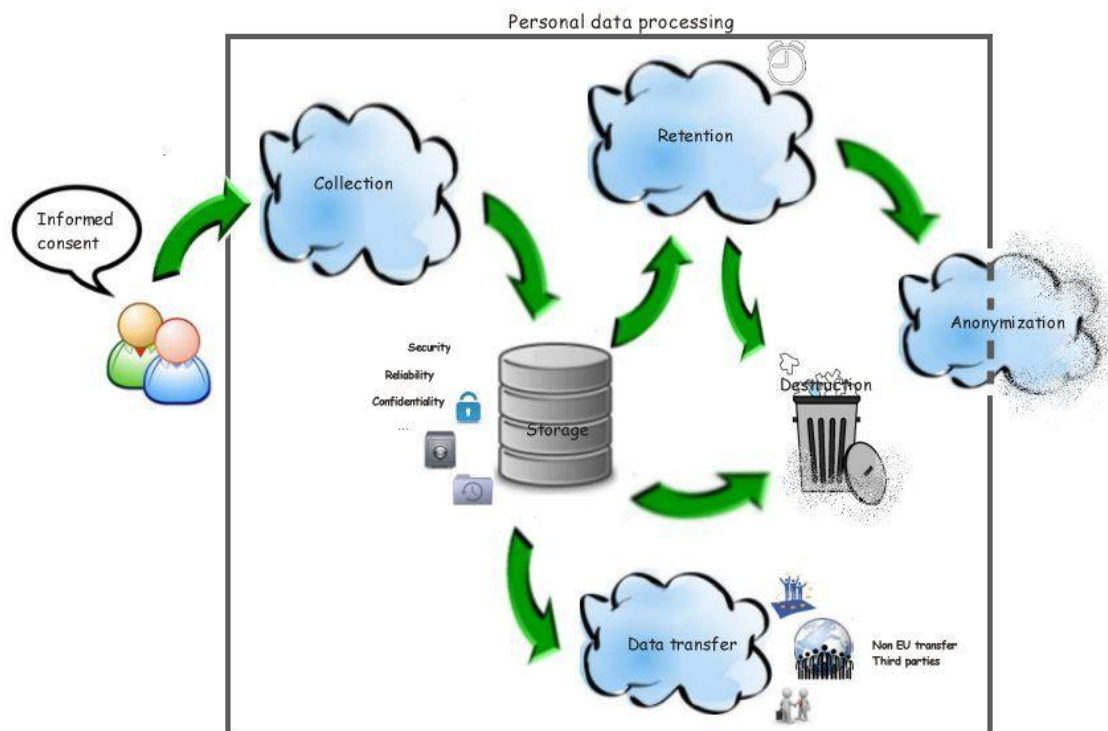
Only data strictly necessary to achieve a specific purpose may be processed.

If consent has been withdrawn with reference to a specific purpose, from that moment onwards the personal data can no longer be lawfully processed.

CCs should be compliant with possible 'opt out' rules concerning the use of telephone numbers inserted in telephone directories and should keep the list of callable numbers constantly updated.

4.3.2 BISON data processing procedures

The picture exemplifies a correct data processing procedure, ranging through all the stages of a personal datum's lifecycle. Below some further notes and tips on the stages following informed consent and collection will be provided. Where applicable, a distinction has been made between the rules in force as set by the Data Protection Directive and the upcoming rules of the General Data Protection Regulation, with reference to its publicly available draft.



Storage

Personal data should be stored in compliance with national and EU data security rules.

Before the entry into force of the GDPR, each CC, either acting as data controller or processor, should comply with its own national rules.

With the enactment of the GDPR, it should carry out a risk evaluation and implement appropriate technical and organizational measures, to achieve an appropriate level of security, in consideration of the risks implied by the processing and the nature of data, taking into account the state of the art and costs of such implementation.

Tips for BISON Guidelines

Both data controllers *and* data processors should adopt security measures.

While the Data Protection Directive is still in force

At present, as long as the DPD and related national implementation laws are in force, reference should be made to national rules of the Member State of the subject adopting such measures.

A verification should first be made on the existence and characteristics of possible ‘minimum’ security measures imposed by national law, which should in any case be adopted, irrespectively of the type of processing or of the nature of the data.

Data controllers and processors should be able to document and give evidence of the security measures adopted.

Duties and connected responsibilities of data controllers and processors in case of damages to third parties connected with inadequate security measures should be carefully checked and prevention measures should be adopted.

For data processors: should security measures not be adequately detailed in the controller’s instructions, all measures foreseen by the law should in any case be adopted. It would not be sufficient to simply adhere to the instructions in order to avoid possible responsibilities.

Further security measures beyond the minimum ones foreseen by national law should also be adopted. These may not be fully identified and described in the law; in this case, data controllers and processors should make reference to the aim of minimizing risks on data, such as:

- a) their destruction or loss, whether by accident or not,
- b) unauthorized access or
- c) processing operations that are either unlawful or inconsistent with the purposes for which the data have been collected.

Such suitable *ex ante* security measures should keep in consideration technological innovations, the nature and the specific features of the processing, a risk analysis and a cost/benefit analysis.

After the entry into force of the GDPR

Data processors and controllers should perform a preliminary risk evaluation.

Data processors and data controllers should implement appropriate technical and organisational security measures. These are not detailed in the GDPR.

Constant monitoring of the legal evolution is advisable: the Commission shall adopt delegated acts

for the purpose of further specifying the criteria and conditions for said technical and organisational measures, including the determination of what constitutes the state of the art, for specific sectors and in specific data processing situations, in particular taking account of developments in technology and solutions for privacy by design and data protection by default.

The Commission may also adopt, where necessary, implementing acts for specifying the requirements of technical and organisational measures to different situations, in particular to:

- a) prevent any unauthorised access to personal data;
- b) prevent any unauthorised disclosure, reading, copying, modification, erasure or removal of personal data;
- c) ensure the verification of the lawfulness of processing operations.

Data Retention and Destruction

Personal data may only be retained for the period allowed by law.

The GDPR strengthens the data subject's 'right to be forgotten', that is to request and obtain from the controller the erasure of his/her personal data and the abstention from further dissemination of such data, especially as concerns personal data made available while the data subject was a child. Such request is based upon conditions set by the law, i.e. when:

- personal data are no longer necessary in relation to the purposes for which they had been collected and processed, or
- the data subject withdraws his/her consent, or
- the storage period consented to has expired, and where there is no other legal ground for the processing of the data, or
- the data subject objects to the processing, or
- the processing does not comply with the GDPR for other reasons.

Tips for BISON Guidelines

The concept of 'processing' should be clearly understood: even data stored as files in an old backup or printed and archived in a repository are still being processed in legal terms, even if left untouched.

Retention limitations set by data protection law should be implemented also in consideration of possible retention obligations to keep data for a longer time as set by other laws, for example for accounting purposes or to manage possible legal disputes.

The information to the data subject should explicitly indicate the period for which the personal data will be stored and retained.

Databases containing personal data should be structured so as to enable the constant control over the data retained, in consideration of possible different levels of consent given by customers for different purposes (e.g. only for the performance of the contract, for marketing purposes, etc.) and of possible actions by the data subject (e.g. withdrawal of consent, objection to processing).

Possible requests by data subjects, such as withdrawal of consent or erasure of data should be forwarded to all subjects to whom personal data may have been communicated (e.g. data controller's

commercial partners).

Action should also be taken in case data have been made public, such as taking all reasonable steps, including technical measures, to inform third parties who are processing such data of the erasure request. Erasure should include links and all available copies.

Mechanisms should be adopted to ensure that the time limits for erasure and/or for a periodic review are observed.

Erasing data means not simply deleting them from the server where they are stored but actually destroying them so that they cannot in any case be recovered, even using special recovery tools. The use of software for the secure and final destruction of data, which for instance overwrites the memory cells 'n' times, may be advisable.

Transfer to third parties

Personal data may only be communicated to third parties, different from the data processor, if the data subject has given his/her previous specific consent.

Tips for BISON Guidelines

The information notice to the data subject should indicate the recipients or categories of recipients of the personal data.

If a data controller intends to transfer data to a third party – such as a commercial partner – it has to get a specific informed consent by the data subject, unless it is the case of a lawful request by a competent public authority.

Getting an all-purpose consent which may include the performance of the contract, the acceptance to receive commercial offers by the data controller *and* the transfer of data to its commercial partners may not be deemed valid and should be split so as to get separate specific consents.

Transfer outside EU

Personal data may only be transferred outside the EU upon specific conditions set by the law.

Tips for BISON Guidelines

While data controllers may well be aware of certain non-EU transfers, as in case of the transfer to a non-EU based Contact Center, more delicate may be the use of certain software or IT services which may imply the storage of data in servers located outside the EU (e.g. cloud services, folder sharing tools such as Dropbox, etc.). It is advisable to read carefully all conditions before signing an IT service contract which may involve non-EU data transfers.

While the Data Protection Directive is still in force

Data controllers should abide by national laws which allow the transfer to third countries ensuring an adequate level of protection. Each Member State assesses the adequacy of such protection level.

Where a third country does not offer an adequate level of protection, data controllers should check the existence of specific conditions, such as:

-
- the data subject has given his/her unambiguous consent to the transfer; this implies that the transfer should be foreseen in the information notice;
 - the transfer is needed to perform a contract between data subject and controller;
 - the transfer is needed to make or perform a contract in the interest of the data subject;
 - the transfer is needed or required for important public interest grounds;
 - the transfer concerns data from a register which is by law intended to provide information to the public and which is open to consultation.

The data controller who needs to transfer data to a third country not offering an adequate level of protection may also be authorized if it provides adequate safeguards for the protection of the privacy of the data subject and the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses.

After the entry into force of the GDPR

Both data controllers *and* processors who intend to transfer data to third countries are bound by the limits of the GDPR, should be aware of them and keep constantly updated.

There are three different cases to be considered:

- a) Transfers are allowed without further authorization if the Commission decides that the third country, or a *processing sector* within that third country ensures an adequate level of protection.
- b) If according to the Commission a third country or a *processing sector* does not ensure an adequate level of protection, transfers are prohibited. Data processors and controllers should periodically check the lists of such countries and sectors published in the Official Journal of the European Union.
- c) If the Commission has not taken any decision on adequacy, transfer may be possible with the adoption of appropriate safeguards on the protection of personal data in a legally binding instrument, such as: i) binding corporate rules; ii) standard data protection clauses adopted by the Commission or by a supervisory authority; iii) contractual clauses between the data controller (or processor) and the recipient of the data, preliminarily authorised by a supervisory authority. In cases i) and ii), instead, no further authorization is required. If appropriate safeguards are not in a legally binding instrument, authorization is required.

Data controllers and processors may also transfer data to third countries with the adoption of binding corporate rules as set by supervisory authorities and in compliance with possible delegated acts to be agreed upon by the European Commission.

The information notice to the data subject should, where applicable, also specify whether the controller intends to transfer data to a third country or an international organisation and describe the level of protection afforded by that third country or international organisation by reference to an adequacy decision by the Commission.

5. Legal aspects of BISON 2.1 Scenarios: a first schematization

This Section is strongly connected with WP2 ‘User requirements and feedback’. Starting from the real-life Scenarios developed in D2.1 ‘Initial user requirements’, it singles out the most relevant ones and identifies possible legal issues to be considered.

D2.1 has addressed ‘User expectations and requirements’, outlining different Scenarios in which BISON may act: Operation Scenarios, Operation and Quality Scenarios, Clients’ Scenarios, Law Regulation Scenarios.

The legal aspects actually refer not only to the fourth scenario, but need to be considered also in all the other ones.

The following tables are aimed at providing a first schematization of the legal aspects implied by relevant Scenarios in order to provide partners with the knowledge tool to implement law-abiding scenarios.

This Section, in particular, will undergo development and deeper analysis in the following Deliverables, based on the partners’ feedback.

5.1 Operation Scenarios

User requirements that are directly connected to the performance of the operation and its improvement. Such requirements may support, reduce, improve or make more efficient processes that may or may not exist at call centers yet.

Scenario	Possible legal issues
Automation of call reason codes A functionality that automates the reason(s) for the customers calls and automatically exports them into client database. Each reason has a group of keywords which are used for the reason definition. The reason for the customers’ calls is detected by these keywords groups. This will need human supervision to update the structure of groups.	- Possible collection and processing of sensitive personal data. - Precise instructions to be given to the human supervisor. - Organizational procedures to be applied as part of security measures.
Reduction of calls from persons who are not entitled to act To reduce repeated inbound calls from people who are not the owners of the line or not allowed to obtain confidential information (for example, spouse is calling but the contract has been signed by the husband).	- Secure identification of the person entitled to make a contract/owner of the line. - Validity of the contract. - Disclosure of personal data to unauthorised persons. - Inaccuracy of personal data given by other people (different from the owner of the line).
Online control of agents Online control marks whether all necessary	- Privacy/data protection of operators. - Protection of operators against possible

information were told or not. Agent gets information if there is some information still missing. Agents know that the sale is correct.	unlawful monitoring performed with electronic tools.
Historical information about sales Collection of information from calls with sales and provision for CC customers. To identify groups with the highest appearance of sales.	- Customers' profiling.
Call me later If customer wants the agent to talk to someone else with more expertise, like husband or parents.	- Evidence of authorisation by owner of the line to talk with a third person (wife, son, etc.). - Need to be sure of the identity of the third person. - Legal relevance of what the third person may say, and possible inaccuracy of personal data collected. - Right of the third person to make contracts or change conditions of existing contracts with the company.
Service upgrade offer Detect clients with high possibility to upgrade the service, offer additional functionalities.	- Profiling of customers (e.g. income level). - Customers should have given consent to process data for commercial purposes.
Automatic notification of breakdown Notifications for IT to check if everything is ok when set up keywords are mentioned often in calls.	- IT limitation of access only to personal data strictly needed for the purpose. - Compliance with national rules possibly set on IT administrators (e.g. unmodifiable log of activities performed).

5.2 Operation & Quality Scenarios

User requirements that are connected with the Operation and also with the Quality side (for clients or clients' customers). Such requirements are correlated with the satisfaction from the clients and users.

Scenario	Possible legal issues
Customer's agreement with a contract To control a verbal agreement with a contract in the call to be sure that the sale is completely valid (for example check if the customer agreed with the contract by saying "YES" loudly and clearly).	- Validity of telephone contracts according to EU legislation. - Validity of clauses, which require specific/written approval or a signature. - Need to be sure of the meeting of offer and acceptance (e.g. in a single voice file).

	- Integrity and non-modifiability of speech recording. - Effective possibility for the data subject to exercise access/intervention rights.
Measuring Customer satisfaction and dissatisfaction Being able to extract calls from satisfied/dissatisfied customers and to analyse post call surveys (for training purposes and client information).	- Data subject's consent for such purposes is needed. - Choice of the data to be selected, complying with necessity and relevance principles.
Real time Customer satisfaction and dissatisfaction A real time alert to team leader if the system detects customer's satisfaction or dissatisfaction. Satisfaction is detected by keyword/phrases.	- Choice of personal data to be selected and related criteria. - Possible negative consequences on team members. Procedures to avoid automatic detrimental decisions involving workers.
Sales opportunity recognition Detect calls with sales Opportunity or Churn Threat to measure. To find out which words or phrases are most often used in sales calls and which in not sales calls to know, what can lead to discourage customers.	- Possible customer profiling.
Commitment detector for previous calls System will identify name of customer and check previous calls and if there was some promise (future call for example), using call ID and name of agent provides status of the promise / same for Shops / Mailing / automated messages. Tags to be found: You agreed to call me, you said me to call me, I have been in a shop, treated badly.	- Possibility of remote control of the worker. - Procedures to avoid automatic detrimental decisions involving workers.
Detection of argumentation To detect whether the agent asks questions to argue on sale or not by checking if agent used argumentation techniques. Very useful to train the agents.	- Possibility of remote control of the worker - Procedures to avoid automatic detrimental decisions involving workers.
Fine-tuning of marketing campaigns Marketing costs optimization by fine-tuning of marketing campaigns allowed by measuring how customers perceive the product. To measure how sales representatives adapt the script they receive from marketing.	- Customers' profiling. - Customer must have given commercial consent.
Repeated calls detector An alert for supervisor within 24 hours in case of repeat call.	- Possibility of remote control of the worker

Pre-determined probing questions To determine if the pre-determined probing questions were asked in the call.	- Possibility of remote control of the worker
Avoid forced sales To red flag calls where the agent insisted too much even if the customer refused several times.	- Possibility of remote control of the worker. - Procedures to avoid automatic detrimental decisions involving workers.
Congratulation message To send congratulation message to agents who made an excellent call - customer expresses satisfaction with service delivered by agent - agent made successful retention call - efficient sales based on key phrases / keywords /emotion/ length of call.	- Possibility of remote control of the worker.
Silence detection Hold time is measured and reported to supervisor. Supervisor gets an alert if the blank is too long.	- Possibility of remote control of the worker. - Procedures to avoid automatic detrimental decisions involving workers.
Native language detection Detect preferred language used by customer and automatically route him directly to same language setting next time he/she calls.	- Processing of sensitive personal data. - Profiling of customers.
Offer channel detection Detect channel where the customer received the offer. Tags to be found: I saw/watch the offer in the web/TV/newspaper/magazine; I received an email/twitter/Facebook message; My friend/mother/ father/ colleague/ brother/... told me; I saw it in a store; someone called me.	- Customers' profiling.
Technical support control Voice Recognition would allow us to control that all steps of technical check are strictly followed in the technical support area.	- Possibility of remote control of the worker. - Procedures to avoid automatic detrimental decisions involving workers.
Training needs To quickly determine the training needs of the agent to react. Based on the adherence to call script.	- Possibility of remote control of the worker.
Voice print To be used as a system to authenticate the person who is calling.	- Processing of sensitive personal data. - Biometric data.
Detection of emotions	- Possibility of remote control of the worker.

Identify % of calls with positive / negative emotions. Identify possible reasons and change of mood during the calls (customers that start calls with positive emotion and finish with negative one).	- Procedures to avoid automatic detrimental decisions involving workers. - Processing of sensitive personal data.
Agent's performance measuring To automate today's restricted call listening process which allows both measuring the real performance and enable a fairer evaluation of calls.	- Possibility of remote control of the worker.

5.3 Clients' Scenarios

User requirements that are connected to the clients; in many cases they are able to provide an added value to the clients, improving their internal processes and satisfaction from their customers.

Scenario	Legal Issues
Improved insight on customer churn To have a tool that records at 100% level the reasons mentioned by customers abandoning the service.	- Retention of personal data after the end of the contract.
Collecting / checking customer's data Control if SPOC (Single Point of Contact) information such as phone numbers, e-mail addresses, addresses were checked or collected/updated and spelled by agent.	- Updating or correction of the customer's personal data.

5.4 Law Regulation Scenarios

User requirements designed to provide higher security to the contact center, customers and clients, in compliance with applicable law and specific conditions.

Scenario	Legal Issues
Detection of calls with performed security check To check that agent asked all security questions he/she is supposed to ask.	- Secure identification of the customer. - Data necessity principle.
Ensuring compliance phrases required by the law Automatic recognition of phrases required by the	- Completeness of information. - Consistency with original information notice provided at data collection.

law included in the call script.	- Information and consent to record speech. - Evidence of consent by data subject. - Update of phrases based on the evolution of legal framework. - Possibility of remote control of the worker. - Procedures should be implemented to avoid automatic detrimental decisions involving workers.
----------------------------------	---

6. Beyond the law: ethical and societal issues

The automated processing of large amounts of biometric speech big data poses relevant issues also from the ethical and societal standpoints, in particular with respect to *social acceptance*.

Despite all technical and organisational measures that can be taken to preserve and enhance security, and the compliance with rules and regulations protecting users' rights which strongly constrain the admissible use of personal data, the sole idea of (large quantities of) data being handled by an automatic system - by definition outside the direct control of the final user - is often perceived as a sort of a threat.

This may be due to the 'loss of control' feeling it suggests, from the psychological viewpoint, possibly associated with a limited technical and legal knowledge.

Therefore, in this Section we provide a first outline of the main ethical and societal issues implied by BISON, both to ensure that it is fully law-abiding and also to contribute to its ethical functioning and social acceptance.

6.1 Ethics in BISON research

The BISON partners are engaged to carry out their activities not only in compliance with applicable rules and regulations at international, EU and national level but also with wider ethical principles. These latter include the highest standards of research integrity as set, *inter alia*, in the European Code of Conduct for Research Integrity.

On the one side, this includes rules that any researcher must respect, i.e. not to perform any misconduct, plagiarism, falsification, etc. This would apply to any research in general, of any kind, even when not directly involving any ethical issue.

On the other side, BISON research is conducted in a field, which may raise ethical issues as concerns the processing of personal data. In this case, as foreseen by the Grant Agreement, the partners should provide copies of:

- (a) any ethics committee opinion required under national law and
- (b) any notification or authorisation for activities raising ethical issues required under national law.

In D8.1 we have provided an explanation of the ethical issues of the BISON research, both as concerns University partners and industrial partners and have provided information on ethical approvals.

To avoid the raising of any ethical issues where not necessary, the BISON partners have expressly chosen not to process any personal data during project lifetime, as it has been deemed not strictly necessary to achieve the project results in terms of development, testing, implementation, etc.

All personal data coming from outside sources, i.e. CC partners' Clients' customers, will be anonymised before being used for BISON, in compliance with the necessity principle set by EU and national data protection laws.

In its actual commercial deployment, however, bigBISON may indeed have to process personal data, so as to enable users to provide a better service to customers and to make targeted offers. Its functioning shall therefore comply with ethical principles in the use of massive personal data.

6.2 Key issues

Ethical and societal key issues cover a wide variety of aspects, such as the following:

- what information levels should be provided, to whom, and in which circumstances;
- the perception by the general public and the special impact towards different kinds of groups (e.g. the elderly, people with disabilities, people of certain races or religious beliefs);
- on the negative side, whether socially-unwanted consequences might occur due to possible mishandling of biometric data, such as, for instance:
 - social exclusion and discrimination,
 - impact on the trust relationship between citizens and the government,
 - risk of erosion of civil liberties,
 - excessive control of the government over the individuals;
- on the positive side, desirable social consequences related to the deployment of the BISON system include:
 - *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;
 - *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;
 - *reduction of work stress and agents' control* – BISON strongly reduces the need for a call to be audited by a human supervisor, thus indirectly checking the agent's way of working; more transparent and uniform control procedures are introduced;
 - *improvement of the chances for home work* – thanks to the support for agent supervision also in distributed CCs, BISON could make it easier for CCs to accept home work, with a positive impact on workers' life, especially for women (reducing the need to commute, making life easier for mothers with kids, etc.);
 - *indirect improvement of job stability* – by strengthening the CCs competitiveness and improving work conditions, the volatility of agents' jobs should be expected to decrease.

More generally speaking, BISON will consider and analyse all socially important impacts of its introduction.

Based on the outcome of the research on legal, ethical and societal issues of WP8, a set of concrete guidelines and recommendations will be drafted for the full compliance of BISON with the legislation in force at EU and national level, as well as with ethical and societal principles from its design and development until its deployment and commercialisation stage.

6.3 Ethics at the CC partners

It is important to note that the ethical commitment of the CC partners is not limited to the mere compliance as required by law: in fact, the partners adhere to self-regulatory codes of ethics and respect the best practices identified for their commercial sector.

ComData

ComData adheres to the Code of Conduct, endorsed by the Direct Marketing and Mail Order Trade Association in Prague the 22th February 2005³⁰.

The Code of Ethics aims to:

- contribute to the protection of customer or consumer;
- protect the interests of association members against business entities with questionable business activities and access to the detriment of the whole industry;
- protect the good name of direct marketing, mail order and the reputation of the whole Association.

In the field of Telephone marketing, the Code includes a commitment for every service provider of telemarketing to always provide quality and telemarketing staff training and comply with all applicable laws.

For instance, according to the Code calls must always begin with the indication of the company and the name of the operator, it is forbidden to call families at night (between 9.00 p.m. and 7.00 a.m.), etc.

The Code also requires to ensure control of telemarketing operations, the accuracy and correctness of the telephone call, the accuracy of the data recorded on the results of telephone marketing.

It is also prohibited to conceal the telephone marketing purpose of the call, especially by pretending another purpose is being pursued or to begin the call with misleading words.

Telefónica Moviles

Telefónica has thoroughly communicated its ethical commitments in a public document called ‘Digital Manifesto’³¹.

In particular, in this document it is emphasized the importance for people to understand and participate in the use being made of their personal data.

³⁰ See <http://archiv.ihned.cz/c1-1005319-eticky-kodex-asociace-direct-marketingu-a-zasilkového-obchodu>

³¹ See <http://www.digitalmanifesto.telefonica.com/manifesto/>

Telefónica proposes three pillars of ‘digital confidence’ that should inform and shape the design of a new digital experience:

- put people in control of their personal data (transparency and control for digital citizens);
- keep people’s identities private;
- keep people’s data safe (safety and cyber-security).

Telefónica supports this approach and believes that these principles would definitely help to build common ground for a successful global digital economy while delivering significant benefits to individuals and to society.

Ebos

The Austrian Standard Plus has certified Ebos compliance with EN 15838 on 1th March 2013³². Although it is not expressly an ethical code, it may surely contribute to the adoption of correct and ethical procedures in personal data processing.

EN 15838 is a European standard describing the requirements for service provision for Customer Contact Centers. It was approved by CEN (European Committee for Standardization) on October 5, 2009.

Such standard includes areas such as management strategy and policy, processes, requirements for Contact Center agents, requirements for infrastructure and best practice guidelines for client organizations.

6.4 Big data ethics

The European Commission digital agenda for Europe highlights that data have become a ‘key asset for the economy and our societies similar to the classic categories of human and financial resources’.³³

While it is widely acknowledged that ‘big data’ may bring significant advantages to Europe’s economy, innovation and society, at the same time their invasive power sets new ethical challenges.

A balance between what is good and desirable and what is bad is stroke by the upcoming **EU legal framework on data protection**: higher responsibilities on data controllers and processors and more control powers to data subjects, as well as new rules taking into account the enormous technological innovation achieved since the 1995 Directive.

However, this may not be perceived as the final solution to all ethical issues. Such perception may in part have to do with the limited actual knowledge of the legal framework in force by large part of the population. Such ‘ignorance’ may somehow amplify the sense of risk and of helplessness of citizens before IT players processing their data – data subjects may actually have rights and control powers they are not fully aware of.

One first pillar for big data ethics may thus be **awareness building**. Correct information and teaching of data protection at different levels may contribute to this.

³² See <http://ebosluxembourg.apps-1and1.net/presentation/certification/>

³³ See <https://ec.europa.eu/digital-agenda/en/making-big-data-work-europe>.

Ethical behaviour and consequent trust may also be enhanced by the adoption of *guarantee tools*, such as labels and logos, which warn and ensure users that their privacy will be fully respected and that their personal data will be processed ethically.

On the other side of such lack of information, there is the **information overload**, which may actually lead to no-information, such as in the case of the recently introduced obligation of cookie banners on the home pages of web sites. The web user is forced to handle several cookie notices a day, possibly not even reading all of them. While the intention is strongly grounded from the legal and ethical standpoint, the desired result might not be fully achieved.

For BISON, such considerations may apply to formal information notices by CCs:

- ethical information notices should not only be complete but also user friendly, not overwhelming and not containing too technical ‘legalese’ terms;
- contact centers may also provide special information on big data analytics performed by BISON, explaining in understandable terms what the system is able to do and also the connected advantages for the user.

Websites and applications put the data subject before the choice between letting them process his/her personal data or not receiving the requested service. In legal and contractual terms, such procedure is correct – a company provides services and a user accepts the terms and conditions of the same service. However, such acceptance may lead to a possibly unperceived level of *invasiveness* on people’s lives, since big data analytics may profile users to a level of detail ever achieved before³⁴.

On the other hand, users of a search engine may receive links which are not necessarily the ‘most adequate’ answers, but the best ones for marketing purposes. Whether and to what extent this practice is ethical is debatable, but it is certainly allowed in the current legal framework.

Big data analytics has thus the potential to influence people and their choices. If used without the adherence not only with the law, but with wider ethical principles, this may bias the otherwise normal evolution of society and culture by way of an induced – and possibly conditioned – evolution.

In this context, the data protection law is an indispensable **defence tool** in protecting people and their data. The GDPR will have even stronger powers in this: non-EU data controllers (thus also US-based IT corporations), for instance, shall also be subject to EU law when offering goods and services to – or monitoring the behaviour of – European citizens.

One may ask him/herself if further and stricter regulation might help to achieve a higher and more effective level of protection. It may be difficult in any case to achieve full ethical behaviour by imposing it by law: the GDPR is already extremely detailed and imposes strict obligations.

The solution may perhaps be found in different incentives. Being ethical – that is, being correct even beyond the mere application of legal rules (i.e. not calling at night or lunchtime even if allowed) – may bring a significant advantage in competitive terms, since a user will be happier to receive services by an ethical CC rather than an un-ethical one.

³⁴ A case which is often cited concerns the pregnant teenager, whose status was known first to big data analytics systems than to her own family. See <http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/>

Summing up, the adoption of ethical codes, as adopted by BISON CC partners, turns out to be a crucial factor in this context, for the benefit both of customers/data subjects and CC themselves.

7. Dual Use

The term ‘dual use’ indicates ‘items, including software and technology, which can be used for both civilian and military purposes’³⁵.

Research activities may sometimes lead to results that have potential dual use – for example, a software used to guide at a distance a toy might be used to control a military drone.

In Horizon 2020³⁶, only research with an exclusive focus on civilian applications can be funded. However, this does not rule out the participation by military partners or the application of military technologies for civilian uses, provided that the research itself is clearly focused on civilian applications. From this viewpoint, it is worth highlighting that BISON only involves civilian partners.

The following sections will discuss whether BISON results may allow some form of ‘dual use’ and, if so, what strategies may be adopted to prevent or mitigate the risks associated with possible military applications of such results.

7.1 *Transfer outside the EU*

Dual use items are subject to special rules in case of their transfer outside the EU.

The reference legal source is Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items.

This legislation regulates the free movement of dual-use items *inside* the European Union, except for a few classes of products (i.e. Items of stealth technology, Items of the Community strategic control, Items of the Missile Technology Control Regime technology, Items of the Chemical Weapons Convention, Items of the Nuclear Suppliers’ Group technology)³⁷.

Instead, an authorisation shall be required for the export of dual-use items (including software and technology) outside the European Union.

This type of control is provided over materials, equipment and technology that may be used for the design, development, production or use of nuclear, chemical and biological weapons and their means of delivery – none of which match the BISON research field or its expected results.

³⁵ See Article 2(1) of Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items.

³⁶ See Article 19(2) of the Horizon 2020 Regulation (EU) No 1291/2013.

³⁷ See Article 22(1) and Annex IV of Council Regulation (EC) No 428/2009.

However, the Regulation also provides for controls relating to the transmission of software and technology by means of electronic media, fax or telephone to destinations outside the Community. In fact, the definition of ‘export’ also includes the *‘transmission of software or technology by electronic media, including by fax, telephone, electronic mail or any other electronic means to a destination outside the European Community; it includes making available in an electronic form such software and technology to legal and natural persons and partnerships outside the Community’*³⁸.

In this context,

- ‘Software’ means a collection of one or more ‘programmes’ or ‘microprogrammes’ fixed in any tangible medium of expression;
- ‘Programme’ means a sequence of instructions to carry out a process in, or convertible into, a form executable by an electronic computer;
- ‘Technology’ means specific information necessary for the ‘development’, ‘production’ or ‘use’ of goods. This information takes the form of ‘technical data’ or ‘technical assistance’. In turn, ‘Technical data’ may take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals and instructions written or recorded on other media or devices such as disk, tape, read-only memories³⁹.

The Regulation only applies to the software specially designed or modified for the ‘development’, ‘production’ or ‘use’ of goods specified in Annex I of the Regulation itself (better detailed below).

No control on ‘Software’ is required, instead, when it falls into one of the following categories:

A. generally available to the public by being:

1. sold from stock at retail selling points, without restriction, by means of:

- a) Over-the-counter transactions
- b) Mail order transactions
- c) Electronic transactions
- d) Telephone call transactions

2. designed for installation by the user without further substantial support by the supplier.

B. in the ‘public domain’

C. the minimum necessary ‘object code’ for the installation, operation, maintenance (checking) or repair of those items whose export has been authorised⁴⁰.

Controls on ‘technology’ transfer do not apply to information ‘in the public domain’, to ‘basic scientific research’ or to the minimum necessary information for patent applications⁴¹.

³⁸ See Article 2(2) of Council Regulation (EC) No 428/2009.

³⁹ See Annex I of Council Regulation (EC) No 428/2009.

⁴⁰ See Annex I, General Software Note (GSN), of Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual- use items.

⁴¹ See Annex I, General Technology Note (GTN), of Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual- use items.

The goods listed in Annex I of the Regulation include the following categories:

- 0) Nuclear materials, facilities and equipment
- 1) Special materials and related equipment
- 2) Materials processing
- 3) Electronics
- 4) Computers
- 5) Telecommunications and information security
- 6) Sensors and lasers
- 7) Navigation and avionics
- 8) Marine
- 9) Aerospace and propulsion

The BISON research does not fall into any of these, because categories 0-4 and 6-9 are out of scope, while the ‘Telecommunications and information security’ category actually applies to specific *‘Telecommunication systems and equipment, and specially designed components and accessories therefor’*, which might *‘employ functions of digital ‘signal processing’ to provide ‘voice coding’ [defined as the technique to take samples of human voice and then convert these samples into a digital signal, taking into account specific characteristics of human speech]’⁴²*.

In fact, while BISON makes indirectly use of voice sampling technologies for voice recording (see Deliverable 3.1 for more details), the BISON results are not meant to produce a telecommunication system, equipment, or related accessories.

7.2 Potential dual use of BISON results

BISON intends to develop a software package for speech analytics, a big data tool capable of analysing speech for contact centers. The targeted BISON output is tightly linked to existing CC infrastructures (such as call handling software, automatic customer dialers, etc.) and therefore hardly allows for direct military application.

Besides, BISON is primarily designed and intended for European Contact Center businesses. For example, the result returned from data processing is a set of information from which the CC agent can draw on to answer the customer’s questions. This is therefore closely related to the service offered to the customer. The system is structured exclusively for the data processing aimed at providing a better service to the customer and to make targeted commercial offers, with the exclusion of any other non-civilian purpose.

For this reason, any immediate direct use of this system for military purposes (e.g. incorporating it in a drone, robot or using it in a direct military action) it is not conceivable.

⁴² See Annex I, 5A001, of Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual- use items.

7.2.1 Dual use and data

BISON is aimed at processing data to the purpose of providing better services to Contact Centers and their clients.

Given the CC business focus, the data processing purposes will be only civilian, i.e. of a commercial nature. Even the automated processing of such data, when applicable, will have exclusively a civilian nature, being directly related to the CC business.

The possibility of managing big speech data from commercial CCs by the BISON system as the final result of the research does not in itself mean a possibility of use for military purposes.

7.2.2 Dual use and the BISON system (technologies, algorithms)

Components of Speech data mining techniques indeed do have a military use. Although not useable for direct military actions (attack or defence), they have been extensively used for military intelligence. In the 1970s, the first research program funding automatic speech recognition ‘SUR: (Speech Understanding Research) was funded by DARPA⁴³.

DARPA has continued to fund high-profile speech data mining programs until nowadays (for example GALE, EARS, TRANSTAC, etc.) and the core research partner of BISON – Brno University of Technology BUT Speech@FIT group, is proud to be one of the few European research groups funded by DARPA programs⁴⁴.

At the same time, BUT Speech@FIT is also funded by an IARPA⁴⁵ program ‘Babel’ that is highly relevant to BISON. The departments of defence are also very active in commercial procurement of speech data mining technologies, for both tactical applications (for example detecting persons planning an attack by their voices in the military action areas) or for military intelligence data interceptions. Phonexia is proud to have provided its technology to several DoDs, exclusively in the NATO countries.

The BISON project is benefitting from the component technology research done with military funding and for military customers and at the same time, the technologies developed for military customers and in current or future programs might benefit from the results of BISON – for example:

- BISON is building on know-how generated in the IARPA Babel program on the rapid development of speech recognition and keyword spotting for languages with missing, costly or unavailable resources;
- Although BISON is not directly building on the outcomes of DARPA RATS (speech data mining from very bad military channels), the work on robustness (mainly of speaker and language recognition) of this program is highly relevant for BISON.

⁴³ Defense Advanced Research Projects Agency (DARPA) is the research arm of U.S. Department of Defense, <http://www.darpa.mil/>

⁴⁴ Currently, BUT is funded by DARPA RATS program and is about to launch research in DARPA Lorelei program.

⁴⁵ Intelligence Advanced Research Projects Activity (IARPA), civilian intelligence counterpart of DARPA, www.iarpa.gov/

-
- Military customers are interested in the high-level information mining from speech; therefore, any technology developed in BISON is of great interest (although ‘business outcome’ is not really relevant, these customers are interested on planning terrorist actions, etc.).

7.3 Risk-mitigation strategies

The risks of dual use are two-fold:

- 1) Legitimate military use by partners’ customers in the BISON project (mainly of Phonexia). In this case, care will be taken that these customers *have no access* to the ultimate goal of the BISON project – namely, the contact center solutions and that the exact configurations (for example, interfacing with the telephony sub-system, user scenarios, details of business data mining, etc., are not shared with these customers). BISON consortium will also take care that no CC data gathered in the project are provided to these customers (however, the general rule of BISON is that no CC data are shipped outside of the consortium, which includes any type of third parties). On the other hand, we find it rather opportune to continue our cooperation with military and intelligence customers on the level of component speech data mining technologies, as this has historically proven to be advantageous⁴⁶.
- 2) Illegitimate use, for example by a terrorist group or an alien government service that usurps the HW and SW infrastructure of a CC that has purchased the technology based on the BISON project. In this case, the technology can be used for illegitimate purposes, but it would require a significant effort from their new users and would be rather delicate, since:
 - a. the input will definitely differ from a normal CC operation and the new owners of the technology will have to interface it to their source channels (for example telephone switch tapping);
 - b. in case BISON technology is intended for military intelligence, the acoustic characteristics of speech data mining will not match, therefore the users will obtain significantly worse results than with military-grade technology;
 - c. the companies delivering the solution (Phonexia and myForce) will control the licenses of the software and can interrupt its functionality by cancelling or not renewing the licenses.

More generally speaking, with a sufficient effort, any technology can potentially be reused (and possibly mis-used) for other purposes than originally developed: the key point is the effort required to perform such an adaptation, related with the quality of results. In the BISON case, the above strategies appear strong enough to make BISON very hardly mis-usable.

⁴⁶ We would like to remind that the Internet was once a military project funded by ARPA (predecessor of DARPA).

8. Prevention of possible abuse/misuse

Sometimes the results of research activities may have the potential for malevolent/criminal/terrorist abuse.

In particular, it may happen when research:

- involves information on/or the use of biological-, chemical-, nuclear/radiological-security sensitive materials and explosives, or the means of their delivery;
- involves the development of technologies or the creation of information that may have severe negative impacts on human rights standards (in particular, personal data and related issues);
- has other potential for terrorist or criminal abuse (e.g. infrastructural vulnerability studies, cyber-security related research).

This Section is dedicated to analyse the risks of possible abuse/misuse of BISON research and results.

8.1 Possible malevolent/criminal/terrorist abuse/misuse of BISON results

The possible misuse of BISON can be situated on two levels. For both levels, misuse actions may be performed by persons that do have legitimate access to the data or to the systems or by illegitimate use (for example, by computer hacking, or physical break-in the location where BISON hardware is installed).

1. During the BISON project
 - a) Risk of malevolent exploitation of *involuntary* leakage of personal data used for training, development and evaluation of algorithms by involuntary action, technical omission (for example, non-complete anonymization of a speech file) or negligence (for example, by wrong setting of access rights on computer file or directories).
 - b) Risk of *voluntary* leakage of data with the explicit aim to discredit or more widely affect the BISON project, or its partners, team members, or the European Commission.
2. After completion of the BISON project (i.e., when its results are deployed in the industry):
 - a) Risk of misuse by legitimate users of BISON results: for instance, commercial CCs could massively mine personal data from telephone calls (violating the process that normally takes care of deleting personal data).
 - b) Risk of misuse by employees or associates of commercial CCs (for example, to perform their own business goals by doing speech analytics and selling it through channels other than the CCs).
 - c) Risk of misuse by state agencies (taking possession of BISON and deploying it massively to spy citizens without necessary warrants or against applicable laws).

-
- d) Risk of misuse by criminal/terrorist groups (for example, by taking possession of BISON and using it to analyse telephone traffic of law enforcement agencies, deciding actions such as evasion, attacks, changing of strategies, etc. based on the results of this analysis).

With respect to all these issues, the most potentially critical profile for BISON concerns the processing of personal data, intended as a human right.

While the privacy issue will be addressed throughout the activities of BISON, first ‘risk assessment’ and ‘prevention measures’ concerning this topic are discussed below.

8.2 Risk assessment

During the development of BISON, only anonymous data (according to the procedures discussed in Section 4) will be processed. While the anonymization process *per se* implies some risks, its structure and the related organisation are conceived to minimise such risk. In particular:

- The BISON consortium only exploits highly skilled personnel in critical positions, selected with established, careful procedures that ensure that only reliable people have access to data and manage the process.
- The process structure inherently separates the most critical role (master annotator, a.k.a. supervisor) from other data handling roles (in particular, annotators in Section 4).

At a later stage, for the use of BISON results, the following considerations apply:

- the relatively high level of maturity required in non-trivial technical domains (such as speech data mining, machine learning and telephony integration) makes BISON much more difficult to misuse than weapons, chemicals, etc.
- speech data mining solutions are not usually commercialized as a ‘boxed’ software, but involve a high level of interaction between the supplier and user through configurations, modifications, customizations, after-sales support, updates, and other forms of consulting. This makes the use of BISON results more controllable, allowing the suppliers (Phonexia and MyForce) to take a corrective action in case of misuse.

The table at the end of this Section summarises some major risk categories, together with the related possible prevention measures. The topic will be further explored in the next WP8 Deliverables, in parallel with the development of the BISON research.

8.3 Prevention measures

The BISON system will be structured so as to select only the useful information to provide better services to customers of Contact Centers.

In particular, the following technological precautions are taken:

- Tight integration with the telephony and other CC infrastructures making it difficult to ‘decompose’ the BISON solution and use it for different unauthorized purposes.

-
- Strict license control over the components and also whole solutions, exercised always by the owner of the technology.
 - Selection of reliable business partners that will be responsible for the sales and support of the technology in different markets.
 - Careful information of the customer about what is legally doable and not doable with the BISON technology and clear instructions that its use and possible further local development must be obeying the local rules (i.e. transfer of liability).

To avoid also that in the implementation of the software some data can be taken out of context or employed for different purposes, the following security measures will be taken:

- Strict encryption of data files necessary for the operation of speech data mining sub-systems (especially the ones that are readable by humans, such as language models or pronunciation dictionaries).
- Strict isolation of data files that have been used for training the systems from the delivery to the customers – the data files are never shipped, what is included to the systems are models from which it is not possible to reconstruct the original content of training data or identities of speakers.

MAJOR RISK CATEGORIES – ASSESSMENT TABLE

Type of risk	Precautions
Unlawful processing of personal data	- Data are fully anonymised (Section 4)
Incomplete anonymization of a speech file due to involuntary flaw	- Two-level anonymization process (master annotator vs. annotators), with feedback in case annotators find some personal residue - Differentiation of roles of involved personnel
Incomplete anonymization of a speech file due to imperfect automatic tool	- Two-level anonymization process, with manual intervention to expunge any personal residue - Only highly skilled personnel in critical position
Data leakage	- Role-based access rights for files and involved personnel - Proper data handling procedures - Clear separation of duties in data management process - Strict encryption of data files - Isolation of data files used for training
Risk of misuse	- Tight integration of BISON technology into application context (to make it hard to separate and use it for different purposes) - Technology not usable “as is”, but only after proper configuration and customization (requires consulting) - License control - Selection of reliable business partners

References

EU and international Legislation

- Article 29 Data Protection Working Party (2014), Opinion 05/2014 on Anonymisation Techniques adopted on 10 April 2014. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf;
- Horizon 2020 Regulation (EU) No 1291/2013. Available at <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32013R1291>;
- Article 29 Data Protection Working Party (2013), Opinion 03/2013 on Purpose limitation, adopted on 2 April 2013. Available at http://idpc.gov.mt/dbfile.aspx/Opinion3_2013.pdf;
- Treaty on European Union and Treaty on the Functioning of the European Union 2012/C 326/01. Available at <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:12012E/TXT>;
- Article 29 Working Party (2012), Opinion 05/2012 on Cloud Computing, WP196 Brussels, 1 July 2012. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf;
- Article 29 Working Party (2012), Opinion 3/2012 on developments in biometric technologies, WP193 Brussels, 27 April 2012. Available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf;
- Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). European Commission Com (2012) final, 2012/001 (COD), of 25.1.2012. Available at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf;
- EU Charter of Fundamental Rights (2010/C 83/02). Available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.C_.2010.083.01.0389.01.ENG;
- Article 29 Working Party (2010), Opinion 3/2010 on the principle of accountability, WP 173, Brussels, 13 July 2010. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf;
- Article 29 Working Party (2010), Opinion 1/2010 on the concepts of ‘controller’ and ‘processor’, WP 169, Brussels, 16 February 2010. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf;
- Council Regulation (EC) No 428/2009 of 5 May 2009 setting up a Community regime for the control of exports, transfer, brokering and transit of dual-use items. Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF>;
- Article 29 Working Party (2005), Working document on a common interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995, WP 114, Brussels, 25 November 2005. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp114_en.pdf;
- UN Security Council Resolution 1540 (2004). Available at [http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1540\(2004\)](http://www.un.org/en/ga/search/view_doc.asp?symbol=S/RES/1540(2004));
- Council Common Position 2003/805/CFSP of 17 November 2003 on the universalisation and reinforcement of multilateral agreements in the field of non-proliferation of weapons of mass destruction and means of delivery. Available at https://www.consilium.europa.eu/uedocs/cmsUpload/l_30220031120en00340036.pdf;
- Charter of fundamental rights of the European Union 2000/C 364/01. Available at http://www.europarl.europa.eu/charter/pdf/text_en.pdf;

-
- 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>;
 - Chemical Weapons Convention (1993). Available at <http://www.opcw.org/chemical-weapons-convention>;
 - Council Regulation (EEC) No 2913/92 of 12 October 1992 establishing the Community Customs Code. Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1992R2913:20070101:en:PDF>;
 - Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981. Available at <http://conventions.coe.int/treaty/en/Treaties/Html/108.htm>;
 - Biological and Toxin Weapons Convention (1975). Available at [http://www.unog.ch/80256EE600585943/\(httpPages\)/04FBBDD6315AC720C1257180004B1B2F?OpenDocument](http://www.unog.ch/80256EE600585943/(httpPages)/04FBBDD6315AC720C1257180004B1B2F?OpenDocument);
 - Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction (1972). Available at <http://disarmament.un.org/treaties/t/bwc/text>;
 - Treaty on the Non-Proliferation of Nuclear Weapons (NPT) (1968). Available at <http://www.un.org/disarmament/WMD/Nuclear/NPTtext.shtml>.

Cited literature

- EU funded research. Available at http://ec.europa.eu/research/participants/data/ref/fp7/89797/improper-use_en.pdf;
- Responsible life sciences research for global health security: A guidance document. Available at http://whqlibdoc.who.int/hq/2010/WHO_HSE_GAR_BDP_2010.2_eng.pdf
- Biorisk management: Laboratory biosecurity guidance. Available at http://www.who.int/csr/resources/publications/biosafety/WHO_CDS_EPR_2006_6.pdf-
- M. Israel & I. Hay, Research Ethics for Social Scientists, 2006, Sage Publications Ltd.
- Richards, Neil M. and King, Jonathan H., Big Data Ethics (May 19, 2014). Wake Forest Law Review, 2014. Available at SSRN: <http://ssrn.com/abstract=2384174>.
- Gartner IT Glossary, at <http://www.gartner.com/it-glossary/big-data>.

List of acronyms

AEPD – Agencia Española de Protección de Datos (Spanish Data Protection Agency);

Call ID – Call identification;

CC – Contact Center;

Convention 108 – Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981;

CRM – Customer Relationship Management;

DARPA – Defense Advanced Research Projects Agency;

DoD – Department of Defence;

DPD – Data Protection Directive. 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;

ECHR – European Court of Human Rights;

FTP – File Transfer Protocol;

GDPR – General Data Protection Regulation. Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. European Commission Com (2012) final, 2012/001 (COD), of 25.1.2012.

IARPA – Intelligence Advanced Research Projects Activity;

IVR – Interactive Voice Response;

LOPD – Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (Spanish Data Protection Law);

MA – Master Annotator;

SPOC – Single Point of Contact;

SUR – Speech Understanding Research;

VoIP – Voice Over Internet Protocol;

Wav – Waveform Audio File Format.