BEAT

Biometrics Evaluation and Testing

http://www.beat-eu.org/

Funded under the 7th FP (Seventh Framework Programme)

Theme SEC-2011.5.1-1

[Evaluation of identification technologies, including Biometrics]

D9.2: Guidelines for Privacy and Data Protection

Due date: 30/06/2013 **Submission date**: 28/06/2013

Project start date: 01/03/2012 **Duration**: 48 months

WP Manager: Els Kindt **Revision**: 1.0

Author(s): E. Kindt (KU Leuven – ICRI-iMinds)

Project funded by the European Commission in the 7th Framework Programme (2008-2010)		
Dissemination Level		
PU	Public	Yes
RE	Restricted to a group specified by the consortium (includes Commission Services)	No
CO	Confidential, only for members of the consortium (includes Commission Services)	No

D9.2: Guidelines for Privacy and Data Protection

Abstract:

This Deliverable 9.2 explains the legal aspects relating to privacy and data protection of the use of biometric databases on the BEAT platform for parties and entities using the platform. It describes in particular the data protection requirements in the European Union and the issues that need to be addressed when the biometric community, including (academic) researchers and industrial partners, deploy the BEAT platform.

Analysis learned that it is in particular important to determine for each user of the BEAT platform which role (e.g. of controller(s), recipient and/or processor(s) (if any)) such user has in relation to the (biometric) data processed on the platform under the data protection legislation. Furthermore, each user, but especially the controller, shall need to determine the national data protection law(s) that is/are applicable. This is herein further explained. Once decided, the users need to accept to comply with the privacy and data protection legislation. This deliverable explains how this could be done.

The deliverable also explains some additional aspects and terms for the Terms of Use for the BEAT platform.

Content

Introduction

The BEAT platform developed in the BEAT project is aimed at providing a web-accessible online open source platform for the evaluation of biometric systems, more in particular for research, testing and attestation purposes, and will be made available to the public. In this objective, it is unique and fulfills a need which is apparent in the biometric community, both for (academic) researchers and industrial partners.

The platform also allows the upload, management and use of biometric databases for the same purposes. Biometric data, even if biometric data would only be used for research purposes, are however personal data. Partners of the BEAT consortium and users of the BEAT platform shall therefore be fully aware that the use of biometric data on the platform for research purposes requires specific attention under the current privacy and data protection legislation.

This second deliverable of Work Package 9 in the BEAT project provides for this reason guidelines to the users of the BEAT platform, in the first place in relation with privacy and data protection. It intends to explain the roles that users may have and the corresponding obligations when they are using the BEAT platform, whether using the platform by accessing it online over the Internet, or whether installing it in its own environment. A distinction will hereby be made between several types of users, Type I, Type II and Type III users, for which different use terms will apply, depending on the access and use that they will make of the platform. This report hereby aims at explaining the parties involved the various legal aspects relating to data protection of the use of biometric databases on the BEAT platform, while focusing on the explanation and proposed Privacy and Data Protection Terms of Use for the BEAT platform.

While the BEAT platform may be mainly used by parties established within the European Union, it is possible that parties from outside the European Union are also interested in using the platform. In this case, these parties will be advised to also respect the European privacy and data protection legislation as will be explained herein.

In addition to privacy and data protection issues, this deliverable will also address and explain some more general Terms of Use for the BEAT platform, needed once the platform will be operational and used by the public (research) community. The proposed Privacy and Data Protection Terms and the more general Terms of Use will be the basis for the later agreements with parties using the BEAT platform

The guidelines contained in this report are in the first place addressed to BEAT partners in their further development and use of the BEAT platform.[1] The content of this deliverable is at the same time also addressed to a wider public, in particular future users of the platform. For this reason, the guidelines and principles of data protection contained in this report and to be complied with are drawn up in a succinct and in an as much as possible comprehensible way. Underlying this deliverable 9.2, is the legal analysis that was made in deliverable 9.1, and which provides the background for this report.

[1] This report 9.2 is also based upon other reports and deliverables of the BEAT project, including but not limited to D2.1, D2.2, D2.3 and D7.1 and, in its final version, D7.5.

1. Summary of the Roles of Parties interacting with the BEAT Platform

In the preparatory deliverable D9.1, the roles of the parties using the BEAT platform were carefully described and analyzed. Because of the aim of the BEAT project to develop a platform for different use cases by several types of interested parties allowing for biometric evaluation and certification[2], *parties interacting with the platform will not all have the same role.* The roles of parties have to be reviewed in detail because it is important and required to determine the so-called 'controller(s)' and 'processor(s)' for every personal data processing operation based on the actual activities.

Uploading biometric data bases or *using* and accessing biometric databases on the BEAT testing platform, even if the databases would not be directly accessible (e.g., for the user, interacting only with the front-end) shall be considered personal data processing. Indeed, the simple retrieval of personal information or accessing such personal data is sufficient for the Directive 95/46/EC and the data protection laws (see below) to apply. [3]

The different roles of parties using the BEAT platform is relevant from the perspective of undertakings of those parties with regard to the use of the BEAT platform ('Terms of Use'), including use terms in relation with the (intellectual property) rights to the platform, and from the perspective of *responsibility for privacy and data protection in relation to the use of biometric databases* on the this platform ('Privacy and Data protection Terms of Use').

- Most parties will use the BEAT platform as it is set up and offered by others for specific purposes, without determining themselves which biometric data(bases) will be offered in combination with the BEAT platform. They typically will use the BEAT platform in participating in a contest or in pursuing their particular (research) interests without organizing the platform .

We will refer to these parties as 'Type I Users-recipients'.

These parties will in principle only have access to the *the front-end computing infrastructure* of the BEAT platform, for example online, at a particular website. While this front-end infrastructure allows these parties to use the BEAT platform for testing purposes, these parties will decide about which biometric databases will be available on the platform nor have direct access to any biometric database(s) uploaded on the platform.

[2] The ten use cases described in D2.1 for the BEAT the platform are 2.1 Benchmarking, 2.2. Security Attestation, 2.3 Evaluation, 2.4 Sensitivity, 2.5 Comparative Evaluation, 2.6 Biometric algorithm optimization, 2.7 Optimization, 2.8 Multimodal biometric system brokerage, 2.9 Quality assessment and 2.10 Educational Resource.

[3] The concept of processing of personal data refers to *any operation or set of operations* which is performed upon personal data, whether done by automatic means or otherwise. This includes the collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, transfer or otherwise making available, alignment or combination, blocking, erasure or destruction of personal data.

These users ('Type I users') will have to agree with a set of Terms of Use for the BEAT platform as well as with limited Privacy and Data Protection Terms of Use.

Type I users could be considered the *recipients* of personal data in the sense of privacy and data protection legislation as will be further explained *below*[4].

- Other parties will be engaged in the use of the BEAT platform in that they determine

  1) *which biometric data(bases) will be offered for use* with the BEAT platform and accessible for testing purposes ; and

  2) choose to deploy the BEAT platform for the testing in combination with the determined biometric database(s); and

  3) determine the use case(s) and the purpose(s) of the use of the biometric data on the BEAT platform.

We will refer to these parties as 'Type II Users – controllers'.

Type II Users will in principle have access to the *back-end computing infrastructure* of the BEAT platform. The back-end will allow *inter alia* the upload and administration of biometric databases for research. It will accommodate various biometric research and systems.[5]

These users will be proposed to agree (i) with (more elaborate) Terms of Use for Type II Users because they will receive extensive rights for using the BEAT platform, as well as (ii) with particular Privacy and Data Protection Terms of Use. They are responsible for the use of the databases in compliance with the governing privacy and data protection legislation. Type II Users will be the *controllers* in the sense of this legislation as will be further explained *below*[6].

A summary of the most important principles and obligations both general and under the governing privacy and data protection legislation will be given in the sections 2, 3 and 4. These principles and obligations will also be referred to in the Privacy and Data Protection Terms of Use suggested in this deliverable for Type II Users.

- Some entities or organizations could also be asked to prepare and support the use of the BEAT platform on behalf of Type II Users.

We will refer to these entities or bodies, operating the BEAT platform on behalf of some other party, 'Type III Users-processors'.

For example, in case Type II Users do not have the technical skills to operate the BEAT

[4] About this concept of recipient, see section 5.

[5] The interaction with the back-end infrastructure is described in the functional specifications and description in D2.1 often as activities of the 'administrator'.

[6] About this concept of controller, see section 2.

platform[7], they may decide to engage the services of another entity, body or organization to assist them in the setup of the back-end computing infrastructure and in operating the BEAT platform system on their behalf. These Type III Users hence will only provide support, including uploading the biometric databases determined by the Type II Users, further to the instructions of and acting on behalf of the Type II Users.

These users ('Type III Users') will under the current data protection legislation in essence have to conclude a written agreement with the Type II User of the BEAT platform, which will include particular privacy and data protection undertakings, with a focus on organizing and maintaining security and confidentiality of the data.

Type III Users have the role of *processors* of personal data in the sense of privacy and data protection legislation as will be further explained *below*[8].

We hence can summarize, as explained and based on the reasons above, the role of the parties interacting with the BEAT platform[9] as follows:

- Party only using the BEAT platform as it is set up and offered by others, without determining which biometric data(bases) will be offered in combination with the BEAT platform = **Type I User -** recipient
- Party determining 1) *which biometric data(bases) will be offered for use* with the BEAT platform and *2) choosing to deploy the BEAT platform* in combination with the determined biometric databases = **Type II User -** controller
- Party asked to prepare and support the use of the BEAT platform on behalf of Type II users = **Type III User -** processor

An extensive description and analysis of the different scenario's as described in D2.1. and relevant for Type I Users, Type II Users and Type III Users can be found in Annex C.

[7] Third party reviewers or entities organizing competitions could be such Type II Users which wish to engage another organization to operate the platform on their behalf.

[8] About this concept of processor, see section 6.

[9] The interaction of the parties with the BEAT platform is also described in the functional specifications and description in D2.1.**.** Based upon our analysis (see D 9.1), the terms 'users', 'administrators' and 'third parties' deployed in this report, however, do not fully coincide with the qualifications of 'controller' and 'processor' under the data protection legislation, implementing Directive 95/46/EC (see *below*).

2. Selection and Use of biometric databases on the BEAT platform : Privacy and Data Protection and Terms of Use for Type II Users-controllers

Type II users are the 'controllers' of the (biometric) data processing on the platform

Parties using the BEAT platform in combination with biometric data bases, need to assess whether they may be 'controller' in terms of the data protection legislation or not. The "controller" of a data processing is in principle responsible for the obligations imposed by the Directive 95/46/EC and the national data protection laws under the current data protection regulation in the European Union.

The controller is more specifically 'the natural or legal person, public authority, agency or any other body which *alone or with others determines the purposes and means of the processing personal data.'* This definition in Directive 95/46/EC is not much altered in the current Reform Proposal.

More than one entity may be the controller. To be the controller, a person or entity does not need to actually possess or 'own' the data. It is sufficient to have the authority or decision power to decide on the means and the purposes of the processing of particular personal data, in this case the biometric data(bases) which will be used in connection with the BEAT platform, or other personal data, such as logging data.

In addition, it is important to note that in order to determine which entity is controller 'an analysis of the factual elements or circumstances of the case' shall be made. 'One should look at the specific processing operations in question and understand who determines them, by replying in a first stage to the questions "why is this processing taking place? Who initiated it?".[10]

In view of the intended development and use the BEAT platform, and the determination of the entity/ies responsible for compliance with the obligations, the 'controller(s)' (and also of the 'processor(s)' (see *below*)) of the processing operations on the BEAT platform shall be determined.

From the description of the requirements in D2.1, it results that there are many use cases or scenarios for using the BEAT platform. Ten such use cases are described. The *roles of 'users', 'administrators' and 'third parties' mentioned in D2.1 for these use cases, however, do not fully map in a consistent way with the roles these parties have from a data protection point of view.*

[10] Article 29 Working Party, *Opinion 1/2010 on the concept of "controller" and "processor"* WP 169, p.8, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

- In these use cases where the 'administrator' 'decides about the purposes' of the processing, i.e. decides about using particular biometric databases by making a data (base) choice or selection and determining a particular use case and 'decides about the means', i.e. decides to use and/or make the BEAT platform available for the processing of the biometric data, one shall conclude that in such cases the 'administrator' should be considered the controller of the data processing for a particular use case. This could apply for example to the use case 2.1 Benchmarking (scenario a).

- The same decisions mentioned above, however, could also be taken by a in the use cases described so-called 'third party'[11], such as for the use cases 2.1 Benchmarking (scenario b) and 2.5 Comparative Evaluation. In these cases, the 'third party' will be the controller.

- The 'user' may also determine for biometric databases chosen by the user to use the BEAT platform and specify own data processing purposes (e.g., see and compare with use case 2.3 Evaluation described in D2.1 where the user could determine the specifications of an experiment see also the overview below use case 2.3 scenario b). The 'user' becomes in that case 'controller'. The user may in this case also appoint an 'administrator' for the setting up of the specific use, the latter acting as processor (see *below*).

  However, in the cases that the 'users' are only able to access the front-end computing infrastructure[12], for example for participation in a particular competition or testing set up by the administrator or a third party, users would in that case not have the role of controller(s). In that case, it would require that the administrator (or third party) takes the decisions about the setup of the platform, the tasks and its tool chain, i.e. the means of the processing and the purposes for doing so.

►►Type II Users shall check that in case the decisions about 'the means and purposes' are taken by the administrator (or third party) together with the user, *both may be considered (co)controllers*. In that case, both the administrator and the user should follow the Terms for the Type II User.

As mentioned, an extensive description of the different scenario's for Type II Users can be found in deliverable D2.1. A summary hereof is attached to this deliverable in Annex C.

BEAT partners, once the platform is being made available to interested parties outside the consortium for their use, and provided BEAT partners are not further involved in the use of the platform, will not be responsible for the processing of personal data on the platform, not as a controller and not as a processor. The BEAT platform is in that case comparable with any other data processing tool or platform, such as e.g. an ERP software program, allowing third

[11] 'Third party' as deployed in the description of the use cases in D2.1 should not be confused with the definition of 'third party' for data protection regulation purposes as described above.

[12] See D2.1, p. 9.

parties to process for example personnel data.[13] This may be different however, when particular databases would be provided with the platform or if one or more BEAT partners would be further involved in the interaction with the platform (e.g., for uploading databases decided by the users, or when administrating the platform for use[14]...).

Ownership or appropriate license rights ?

Type II users of the BEAT platform need to ensure that they are entitled and have the (legal) right to use one or more selected databases of their choice on the platform.

For this purpose, they need to ascertain whether they either are the (i) *owner* of the database(s) that are going to be deployed on the BEAT platform or (ii) *have obtained the license rights from the rightful owner(s)* of the data base to use the databases on the platform.

Such license rights should be established by a (preferably clear) license agreement or by another way of approval of use of the data base on the platform.

In case of *co-ownership*, e.g., of biometric databases established during a joint research project, the co-owners should agree about the right of the Type II user to use the database(s) on the platform.

Scope and content of the license agreement for biometric databases

Many license agreements for the use of (public) biometric research databases restrict the use of such databases to internal research purposes.

In case the Type II users are using the BEAT platform and connected biometric databases for other research than internal research purposes (e.g., for organizing a contest) , such license agreement[15] between the owner and the Type II user shall mention the (license) right that the biometric database(s) may also be made available pursuant the BEAT platform (and a chosen scenario) to other parties for testing and research purposes, who will have limited access thereto under conditions.

This is needed because the use of the database(s) on the BEAT platform could in that case not be considered as internal research and will in that case not be restricted to use for internal research.

Such license agreement may also need to mention any commercial use that may be made of the databases through the BEAT platform, if applicable.

[13] See also and compare for similar situations and arguments in relation with providers of cloud computing infrastructure: W. Kuan Hon, Ch. Millard and I. Walden, 'Who is responsible for 'personal data' in cloud computing? – The cloud of unknowing, Part 2, available at http://idpl.oxfordjournals.org/content/early/2011/12/06 /idpl.ipr025.full

[14] This is different from administrating the platform by one or more BEAT partners for purposes of licensing (only) the platform.

[15] Such license agreement shall hence not be restricted to the use of the biometric databases for internal research purposes.

Biometric data(bases) for testing and research purposes : primary purpose or secondary use ?

Type II users of the BEAT platform could decide to collect new datasets for use on the BEAT platform or to use already existing biometric data collections databases.

When new datasets are collected for use on the BEAT platform, the testing and research is the *primary* purpose of the data collection and the use of the data.

In case existing data collections are used, these databases can either exist for research purposes or not (e.g., a client database). In case existing databases are used which do not have research as their primary purpose, re-use of the data for research purposes may only be permitted if allowed and if specific conditions are respected pursuant applicable national data protection legislation. Such legislation often provide for provisions allowing to re-use data for research but usually impose additional safeguards and conditions, for example rendering the data anonymous or encoding the data. The purpose of the safeguards is typically to 'rule out' that the data will be used to support measures or decisions regarding any particular individual.[16]

Biometric data however can in principle not be 'anonymized' as it inherently refers to individuals. There is a lot of misunderstanding about this concept. 'Anonymized biometric data' is hence a 'contradictio in terminis'. What is possible, is the separate storage of biometric data (e.g., the samples) and any additional information about the biometric data (e.g., name, etc). This notion of 'functional separation' completed with additional safeguards is very important.[17]

As it further implies however that the data cannot be anonymized, the Data Protection Authority may have to be consulted to obtain prior authorization if needed (see also b*elow*).

For research databases, additional personal information about the individuals from whom the data are collected, is often limited, and mostly only kept by the party originally collecting the data. This will also render it very difficult to provide the individuals from whom the biometric data originate with information (see *below*).

In any case, Privacy by Design requires that any such additional personal information about the individuals from whom the data are collected shall at least be stored in a separate location, or even better, deleted if possible.

The biometric data used on the BEAT platform are 'personal data'

The Directive 95/46/EC which is the basis for the national data protection legislations in the EU Member States defines "personal data" as meaning "any information relating to an *identified or identifiable* natural person (data subject)".[18]

If the natural person to whom the information relates can be identified or identifiable, the data

[16] Article 29 Working Party, *Opinion 3/2013 on purpose limitation*, WP 203, p.28

[17] It implies that Type II users need to guarantee the security of the data , and take all other necessary technical and organisational measures to ensure functional separation. *Ibid.*, p. 30. See also below.

[18] Currently, the Directive does not mention biometric data as such.

will be considered personal data. As a result, the data protection provisions apply. Since biometric data are in principle used in many applications to identify or at least, because of unique characteristics, allow for identification[19], biometric data will in general and in principle be considered personal data and hence fall withing the scope of the Directive 95/46/EC.[20]

Most biometric data used for testing purposes are moreove often so-called 'raw data', i.e. the images of the fingerprint, face, etc. This type of biometric data facilitates the comparison with other data bases for identification, if intended.

If personal data would be in so-called public databases, this conclusion does in principle not change[21] (see also *below*). Whether the biometric databases uploaded on the BEAT platform would be 'private' or 'sequesterd' databases or 'public databases', freely available on for example the Internet, hence is not very relevant. This Directive, as implemented in national laws, imposes rights and obligations for the processing of personal data.

In the Reform proposal, the definitions of personal data and data subject include that direct or indirect identifiability shall be reviewed in view of the 'means reasonably likely to be used by the controller or by any other natural or legal person'. This in fact does not change much as this criterion was already used in the interpretation before.

The proposal also explicitly defines biometric data. Biometric data is therein defined as 'any data relating to the physical, physiological or behavioral characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data'.[22]

Although *in casu* it would *not* be the purpose of the BEAT platform to identify persons, but to use the data for research purposes only, this does not change the conclusion however that the biometric data used on the platform will in principle be considered personal data. The biometric data indeed is information relating to persons that at least can be identified, even if that were to be by a third party (for example, the 'original owner' of a research database, who collected the data).

Synthetically generating biometric data based upon a sample degradation model (see internal (administrative) use case 3.2, D2.1, pp. 30-31) will also imply the processing of biometric (personal) data if the degradation model would allow a link to particular original biometric data[23], on which the synthetically generated data could be based, and which would hence remain information relating to an identified or identifiable person. If the synthetically generated biometric data would not be based on particular original biometric data ('raw

[19] For example, fingerprint or faces, even without names or other additional personal data, in principle could allow identification of the data subjects concerned, by comparison of the biometric data with data in other databases, e.g., of epassports.

[20] Data or information on the BEAT platform which are no personal data, include for example the algorithm as such, uploaded by a user on the platform.

[21] See also EDPS, Turbine Opinion, 2011, p. 3.

[22] Article 4 (11) of the proposed General Data Protection Regulation. The Reform Proposal also contains provisions relating to biometric data processing (see below about the need for an impact assessment for the processing of biometric data).

[23] E.g., a particular fingerprint.

data'), but rather be compiled from at random, a collection of features of a large group of biometric raw data, it could be defended that such synthetically generated biometric data is no personal data since the information does not relate to an identified or identifiable natural person anymore.

National data protection legislation is applicable to the use of biometric databases

It is sometimes argued that biometric data used for research purposes, in particular the use of data for research that would be in the 'so called public domain', such as facial images on the internet, or 'public biometric databases', would not be governed by data protection regulation. This is not correct. Data protection legislation does in principle not make a difference for granting protection whether the data have been rendered public or not.

The national data protection legislations in European Member States are all based *on the EU Data Protection Directive 95/46/EC.*[24] This Directive 95/46/EC imposed upon Member States to implement the provisions set forth in this Directive, which all Member States have done.[25] Their legislations impose rights and obligations as determined in the *national* data protection legislation, but contain – largely - the principles and provisions as set forth in the EU Data Protection Directive 95/46/EC. Only the handling of (fully) manual files (which is clearly not the case in BEAT and for the BEAT platform) is not governed by the Directive 95/46/EC.

Some of the main principles and obligations for data controllers, which are also relevant for controllers of biometric data used on the BEAT platform, are hereunder mentioned and briefly summarized. Please note, however, that controllers *need to apply those national data protection provisions*[26] *which apply to the use of the databases* and the processing of other personal data on the BEAT platform.

To determine the *applicable national data protection law*, the Directive 95/46 states that the laws of the Member States where a controller *processes personal data in the context of the activities* of an establishment in that Member State, shall apply.[27] Most national data protection laws have adopted a similar provision. This means *that controllers are subject to the law(s) of the Member State where they process personal data in the context of the activities of an establishment of that controller in the Member State*.

[24] 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, *O.J.* L 281, 23.11.1995, pp. 31-50, available in English at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[25] Please note that Switzerland has also adopted data protection regulation based upon the Directive. The EU Commission has decided that the data protection legislation of Switzerland offers an adequate level of protection. This is relevant for transborder data flows for data from within the Union to Switzerland (see also below, Section 7, 7.7)

[26] BEAT partners and later 'users' and 'administrators' of the BEAT platform subject to their role as controllers (and processors) will find an English translation of the national data protection legislations in each of the EU Member States at the websites of the national DPAs.

[27] Article 4.1. Directive 95/46/EC.

►►To the extent that the BEAT platform will be available online, the place of the activities of the Type II Users- controller(s) setting up and using the platform will determine the applicable national laws.[28]

For example: Company Y (e.g., established in Germany) is conducting research activities at its R&D department established in France. The R&D department in France wishes to test and improve its biometric algorithm and decides to access and use the BEAT platform (which is made available online by a Swiss organisation). The R&D department of the Company Y is deciding (alone) about the type of deployment of the BEAT platform, the programming of the tasks and the toolchain for use in the BEAT platform. The R&D department of the Company Y also decides about the databases to be uploaded for the purposes of the tests. Since the use and processing of personal (biometric) data is carried out in the context of activities of the R&D departement established in France of Company Y, the activities are hence taking place in France and the French data protection legislation will apply. The R&D department and/or the Company Y[29] will be considered controller of the processing of the biometric and other personal data on the platform, and shall comply with the French data protection legislation.

Where a controller is established in a number of Member States and uses personal data for its activities in more than one of its establisments (e.g., France, but also Portugal, …) , the laws of *each of those Member States* will apply.

In addition, it shall be noted that the Directive gave the Member States in some areas a choice for the implementation, resulting in data protection laws in Member States which are sometimes *(slightly) different*.[30]

►►For these reasons, the Type II Users- controllers will have to determine and analyze the data processing rights and obligations *under the applicable national (data protection) laws* and apply such applicable national data protection laws.

[28] About the applicable law, see also Article 29 Data Protection Working Party, *Opinion 8/2010 on applicable law*, 16.12.2010, 33 p.

[29] If the R&D department is a mere establishment or branch of the Company Y without being a separate legal entity, the Company Y will be considered the controller. Even if established in Germany, Company Y will have to comply with the French data protection legislation since the activities in which context the biometric data are processed, take place in France.

[30] Some Member States may also have national laws which are more stringent than the provisions of the Directive, since the Directive imposes only a minimum protection and does not forbid Member States to provide a higher level of protection.

3. Type II Users: Main Privacy and Data Protection Principles and Terms of Use

Hereunder are the most important data protection principles for controllers mentioned of which four are briefly discussed in this section. All of these most important data protection principles are listed and summarized in Annex A. This report and Annex intend to give to BEAT users only a general and non-exhaustive overview of the data protection principles when processing biometric data on the BEAT platform for research purposes.[31] For an extensive overview, the applicable data protection legislation needs to be consulted.

Type II Users-Controllers need consent or another legal basis for the legitimate processing of the biometric data(bases) on the BEAT platform

Type II Users, being the controller, *must verify* for uploading and the use of biometric databases on the BEAT platform (and any other processing of personal data) whether such use and processing is based and *covered by one of the legal grounds mentioned in the (national) applicable data protection legislation(s)*.[32] The use by the Type II User of biometric data collected by a third party outside the EU (e.g., biometric research data bases of U.S. governmental agencies) also needs to comply with this principle. Once such databases are used for activities of the controller within the EU, a valid consent, if any, or an other legitimate basis is required for the use of such data on the BEAT platform.

In research projects, parties collecting or using personal data often rely for personal data processing on the *consent* of volunteers providing their personal data. Such consent needs to fulfill particular conditions, in particular that such consent is informed, free and specific. A specific form is usually drafted for the purpose of obtaining such consent.

►►For the use of biometric data on the BEAT platform, Type II Users-controller(s) could possibly rely on the consent of the data subject that their biometric data are used for test and research purposes when deciding to upload one or more databases on the platform, if all conditions are fulfilled.

As mentioned, the consent is defined and subject to conditions. Consent shall be specific, informed and free. How specific such consent should be, is debated.[33] To the extent that the BEAT platform uses data bases of biometric data for which use the data subjects (i) who *were volunteers* (ii) have given their *specific and informed consent* for use of their *biometric data for research purposes* by the collecting research company or institution *and third parties*, and such in conformity with national data protection law(s), one could defend that this is sufficient as legal basis, as long as there is no significant imbalance in the relation between the data

[31] They are summarized in seven topics for an easy recapitulation.
[32] See also *above* about how to determine the applicable national data protection legislation(s).
[33] See also, about consent, Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent (WP187),* 13.7.2011, 38 p.

subject and the controller.[34] It is hereby also important to take the reasonable expectations of the data subject[35], from whom the data were collected for research purposes, are respected. However, it could also be contested to the extent the consent probably did not make an explicit reference to a platform such as BEAT and the data subjects hence could not foresee such use.

►►In case specific biometric data would be collected for use on the BEAT platform, it is *recommended* that the Type II User-controller informs and foresees in the consent form for the data subjects that the consent allows use of the biometric data on a common testing and evaluation platform, such as the BEAT platform, made available online to a closed group of users or to the public, and that may be used for several use cases, whereby the data may be used, directly or indirectly, by several actors, worldwide, even in countries not providing an adequate level of data protection.

It is further important to realize that, subject to further research, biometric data is considered by some as so-called '*sensitive data*'[36] while this is disputed by others.[37] In particular, some consider that the processing of biometric data involves health related personal data (e.g., iris may reveal certain diseases) and data revealing racial or ethnic origin (e.g., facial images indicate race or ethnic origin). This is increased in case samples are stored and used. Biometric databases for research often contain samples rather than templates.[38] The risk that such samples contain sensitive information therefore increases.[39]

►►In case of the collection of biometric data, the collection may include sensitive data and additional obligations will apply.

For example: Some national laws of the Member States may allow lifting the prohibition of the processing of the sensitive data with the (*written*) consent of the individual while other national laws may not. If applicable, the Type II BEAT User-controller should take this into account.

---

[34] See the proposed art. 7.4 of the Reform Proposal.

[35] See about this aspect, e.g., also Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation (WP203), 2*.4.2013, 70 p.

[36] Sensitive data is information on racial or ethnic origin, political opinion, religious or philosophical beliefs, trade-union membership, health or sexual life (see Art. 8 Directive). See also the Court of Justice, on a reference for a preliminary ruling, which has stated in 2003 that 'data concerning health' as set forth in the Directive 95/46/EC shall be given *a wide interpretation* : ECJ, C-101/01, *Bodil Lindqvist*, 6.11.2003, *ECR* 2003, p. I-12971, § 50.

[37] About this discussion, see also Article 29 Data Protection Working Party, *Advice paper on special categories of data ("sensitive data")*, 20.4.2011, p. 10: '*Some* DPAs are also in favour of including biometric data and the creation of personal profiles' and (p. 15 Conclusions): 'Regarding new categories, the *majority* of the Working Party supports including genetic data and biometric data' (emphasis added).

[38] We refer to the terms and vocabulary as discussed and developed by international standardization groups, in particular ISO/IEC JTC 1/SC 37 and adopted in 2012: ISO/IEC 2382-37:2012 Information technology - Vocabulary - Part 37: Biometrics, 13.12.2012, 28 p.

[39] See also E. Kindt, *The Processing of Biometric Data. A Comparative Legal Analysis with a focus on the Proportionality Principle and Recommendations for a Legal Framework*, doctoral thesis, Leuven, 2012, KU Leuven Law Library, 760 p., also available in other university libraries and soon published with SpringerLink.

Information to the data subjects, unless exemptions apply for use of data for research

The Directive 95/46/EC states that whether the data is collected directly from the data subject or from a third party, the data subject *must be informed* of 1) the identity of the controller and his representative, if any; and 2) the purposes of the processing. If it is necessary to guarantee fair processing towards the data subject (having regard to the specific circumstances in which the data are collected), additional information must be given, including 3) people or organizations or categories of recipients[40] who will be given the data; 4) whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply; and 5) about the data subject's right to access his or her file and right to rectify his or her data that is erroneous or incomplete.

If personal data has not been obtained from the data subject, the data subject must be informed in addition 6) about *the categories of data concerned* by the processing.[41]

However, *exceptions* to this information obligation to the data subject may exist in Member States, subject to national law, in particular for processing for statistical purposes or for the purposes of historical or scientific research if providing this information is impossible or involves a disproportionate effort, and subject to the implementation of adequate safeguards (e.g., rendering the data anonymous).

►►The Type II BEAT User-controller should take this information obligation into account.

In case of the use of 'public' databases, collected by and available from other research institutions, it may be that the information of the data subjects from whom the biometric data was collected, is impossible or involves a disproportionate effort for the Type II BEAT User-controller for the use on the BEAT platform. In this case, the Type II BEAT User-Controller may be exempt from the information obligation. National legislation should be checked.

►►The Type II BEAT User-controller may also have to respect the right to object to be included in a biometric database (see Annex A).

[40] A "recipient" is defined in the Directive as any natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not.

[41] The above information must be given to the data subject as soon as possible, in principle *when the data is collected*. If the data is not directly obtained from the data subject, the information must be given when the data is recorded or if disclosure to a third party is envisaged, not later than the time when the data is disclosed for the first time.

Type II Users-Controllers need to have the use of the databases on the BEAT platform notified - Prior checking in specific situations

Most Member States have a procedure in place which obliges the controller of an automated filing system to make a *notification* to the local Data Protection Authority (DPA) *prior to* carrying out any processing operation. The purpose of the notification and related provisions is mainly to ensure transparency and provide information to the public. As a result, the notified processing is mentioned in a public register kept by the DPA. Any modifications to existing processing operations usually also need to be notified.

However, the Member States have the possibility, with regard to certain categories of processing operations, to provide for a simplification for such notification (e.g., in France) or for an exemption from notification (e.g., if a data protection officer is appointed (for example, in Germany).

This notification obligation is however under review and would no longer apply subject to adoption of the current version of the Reform proposal. The obligation, however, would be replaced according to the proposal by an obligation of the controller to keep similar detailed documentation.

►►Type II BEAT Users-Controllers currently still need to review the existing notification procedures in their countries and according to national applicable privacy and data protection legislaton.

In addition, the Directive provides that there may be situations where further investigation by the supervisory authority or by the data protection official is both relevant and desirable. In that case, *prior checking* with the supervisory authority is mandatory (Article 20 of the Directive).

In case biometric data are saved in for example a central database, the Working Party recommends that the Member States require prior checking by a legislative measure.

For example: The data protection legislation in France imposes prior authorization for biometric data processing operations other than for the government unless the processing would qualify under one of the Unique Authorizations issued by the French DPA. The use of biometric data for research on a platform such as BEAT, has to our knowledge, not been the subject of such a Unique Authorization.

►►The biometric data used on the BEAT platform is in principle kept in the form of databases. For this reason, the Type II BEAT Users-Controllers for the platform shall review

under the applicable national data protection laws whether a notification is sufficient for the use of the data bases on the platform for research purposes or whether prior authorization is required. In the latter case, often specific delays are stipulated for review of the request and the reply by the DPA.

To conclude, it means that the Type II BEAT Users-Controllers would hence need to notify/request prior authorization, unless such notification/authorization would already have been obtained for the use of biometric data for research purposes by the Type II BEAT Users-Controller in the sense and to the extent as the use on the BEAT platform.

Type I1 Users-Controllers shall implement all necessary technical and organisational security measures

Type II BEAT Users-Controllers shall ensure, in addition, that the data are protected by implementing all necessary technical and organisational security measures (see also Annex A below).

Upon the use of biometric data for research, however, specific attention shall be given to ensuring that the data will not be used to support measures or decision regarding particular individuals or in a way which may be affecting such individuals (e.g., (identity) theft of biometrics).

For this purpose, functional separation is very important and implies that Type II users need not only to guarantee the security of the data, but shall also take all other necessary technical and organisational measures to ensure functional separation.[42] It implies further taking specific additional security measures, such as encryption, making sure that the data enabling the linking of information to a data subject, if any, are encoded or encrypted and *stored separately*, and restriction of access to the data only on a need-to-know basis.[43]

Furthermore : Type 1I Users-Controllers outside the EU and the data protection legislation effective in the Union

In section 2, the territorial scope of the data protection legislation in the EU Member States was clarified. Type II Users-Controllers established in the EU and which process personal data in the course of their *activities on EU territory* fall under the Directive 95/46/EC. This means that for any entity or body being Type II User, which uses the BEAT platform and uses and processes (biometric) data in the course of its activities in one or more EU Member States, the EU data protection regulation will apply.

[42] Article 29 Working Party, *Opinion 3/2013 on purpose limitation*, WP 203, p.30.
[43] *Ibid.*, p. 32.

In addition, in the current regulation, the use of *any equipment* (except for transit purposes) in the EU for the processing of personal data, is sufficient for the EU data protection regulation to apply. The BEAT platform could in our view be considered such equipment in the EU if it would be hosted or offered online by an entity in the EU.

►►Therefore, Type II Users *from outside the EU shall also obey the EU data protection rights and obligations in such case when the using of the BEAT platform* could fall under the current data protection regulation, for example, when relying on a processor established and with activities in the EU which is hosting and operating the platform. To confirm this, it is recommended that the entity licensing the platform (licensor) clearly stipulates such in the contractual terms for using the BEAT platform.

Note on current reform proposals: In the current proposal of Regulation, the use of equipement on the territory of the Union is no longer the criterion for non-EU controllers for application of the data protection regulation but rather whether services or goods are offered to data subjects in the Union or behaviour is monitored (art. 3 Reform proposal). This creates for the BEAT platform uncertainty as to whether non-EU Type II Users-controllers will be subject to the data protection legislation. If the platform would be availabe on a server in an EU member state, the use of this equipment would under the current proposals for reform not oblige non-EU controllers to comply with the European data protection regulation, unless goods or services are offererd to data subjects in the Union. In this case, the entity licensing the BEAT platform (licensor) to such non-EU controller could in this case nevertheless advise to respect the obligations to protect the (biometric) data by way of contractual terms.

►►For privacy preserving purposes, it is recommended that the BEAT project advises in the contractual agreement respect to privacy and data protection regulation, to be detailed in the terms and conditions for the use of the BEAT platform, with the Type II Users-Controllers outside the EU.

4. Additional Guidelines for Privacy and Data Protection

Access and use of the BEAT platform by users outside the Union : transborder data flows

The BEAT platform which is available online and set up (including the choice of biometric databases available on the platform) by a Type II user (controller) with activities in the Union, may also be accessible by third parties with activities or established in countries outside the Union. In that case, the Type II User-controller shall ascertain that the principles and rules for transborder data flows are respected.

In principel, there is transborder data flow when personal data is sent to another country. However, there is also transborder data flow if personal data *is merely accessible* in another country. Transborder data flow between countries of the European Union is in principle allowed, because the countries of the European Union have implemented the Directive and hence are deemed to have appropriate privacy laws.

However, a transfer of personal data to a country outside the European Economic Area (EEA) is only allowed if that third country *ensures an adequate level of protection* of the privacy. The adequacy of the protection will be assessed by the European Commission taking into consideration the circumstances surrounding the data transfer, the nature of the data, the purpose for processing the data and how long it is expected to take, the country of origin and country of final destination, the laws, professional rules and security measures, both general and per industrial sector, in force in the third country.

The European Commission has entered into dialogue between its most important trading partners with the aim to improve the knowledge and understanding of their privacy protection systems. The European Commission has already approved several countries, e.g., Switzerland and Canada, as countries that offer an adequate level of protection of privacy.[44] It implies that if personal data are sent or are accessible by one or more recipients or by processors, established in one of these countries, such data transfer is allowed.

The European Commission and the US government have alos negotiated an arrangement on an adequate standard of privacy protection as well. The US Department of Commerce has as a result issued the so-called *Safe Harbor Principles* aimed at providing an acceptable framework for personal data transfers. These Safe Harbor Principles are recognized by the EU Commission as providing an adequate level of protection for the transfer and exchange of personal data in the private and public sector, with the exception of use for law enforcement for which specific rules apply (e.g., the transfer of PNR data for law enforcement purposes). However, each company in the U.S.A. receiving, processing or accessing the data need to explicitly undertake to adhere to these Safe Harbor Principles. This may not really be fit for the BEAT platform.

►►Type II Users-controller may probably not be able to rely on this solution of the so-called

[44] For an updated list of countries which are deemed to ensure an 'adequate level of protection', see http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

Safe Harbor Principles for for example, engaging a processor in the United States, unless such company would engage to adhere to the Safe Harbor Principles.

A transfer of personal data to a third country *which does not ensure adequate protection* however can also *inter alia* take place if 1) the data subject has *unambiguously consented tot the proposed transfer*; (…) or 4) the transfer is necessary or legally required in the public interest, or to establish, exercise or defend a legal claim (…).

►►In case the Type II Users - controllers of the use case applicable to the BEAT platform wish to make the platform available for a wide range of users, for example, in the case of a competition, the controller should hence use such biometric data bases which have been obtained with the consent of the data subjects having accepted unambiguously with the transfer to third countries with no adequate protection.

►►Because it is generally agreed and accepted that there remains currently a lot of uncertainty about the performance of biometric systems, and there might be an acceptance that it is in the interest of various parties that more uniform testing platforms should be made available, Type II users – controller(s) could argue – subject to wider motivation and official acceptance – that a widely availabe BEAT platform employing the making available of particular databases for testing purposes in countries outside the Union, is in the public interest. However, an approval of the DPA(s) or legislative initiative would in that case be preferred.

Finally, a Type II Users-controller may ensure adequate safeguards to protect the privacy, resulting from appropriate clauses being included in a contractual arrangement. Such contract must allocate how responsibility for compliance with data protection laws is shared between the transferor and the recipient of data.[45] If Type II Users-controller(s) and Type III Users-Processors (or processors in e.g., a country where the EU data protection legislation does not apply) agree to conclude such agreement, the data may be transferred as well.

Note on current reform proposals: In the recent proposals, the transborder data protection regime remains to a large extent similar. The transfer by way of Standard Contractual Clauses is also maintained.

[45] Several types of Standard Contractual Clauses have been adopted by the EU Commission for the transfer of personal data from a controller in the EU to a controller/processor outside the EU. These types of Standard Contractual Clauses can be consulted at http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm . This is different from the Binding Corporte Rules (BCRs) which are gradually being adopted by international companies for intra-company transfer of personal data outside the Union and which require approval of the DPAs

Data Protection Impact Assessment for the BEAT platform ?

The current version of the Directive 95/46/EC requires Member States to identify processing operations which are likely to present specific risks and this for purposes of prior examination before the start of the processing (Art. 20.1). Few Member States have determined such operations. The Reform Proposal seems to expand on the prior authorization requirement of the present Directive but now imposes upon the data controllers to perform a Data Protection Impact Assessment (PIA).[46]

A privacy impact assessment can be generally described as a risk assessment tool to assess new programs or systems and technologies for privacy risks and to mitigate or avoid adverse effects, initially most advocated upon the design of large government projects, but spreading into the private sector.

Type II Users-controllers should hence take Art . 33 of the current version of the Reform Proposal into account. This Article does not make any distinction for the use of data for research purposes. It imposes a PIA for biometric data processing, as they 'in particular present specific risks' 'by virtue of their nature, their scope or their purposes'.[47] Such PIA contains at least (1) a general description of the envisaged processing operations, (2) an assessment of the risks to the rights and freedoms of data subjects, (3) the measures envisaged to address the risks, (4) safeguards, security measures and mechanisms to ensue the protection of personal data and to demonstrate compliance with the Regulation. Public authorities processing biometric data because of a legal obligation may be exempted.

It is currently not clear whether this obligation will be adopted, but it is quite possible. Type II Users-controllers, or Type III Users-processors acting on behalf of the controller, may hence have to comply with this new obligation.

ePrivacy: more Privacy and Data Protection rights and obligations

Parties involved in the use of the BEAT platform, which will be available online over the Internet, should also take additional privacy and data protection principles into account which relate to the collection and use of personal data over electronic communications networks (ePrivacy) [48] for example, the collection of personal data relating to users of the BEAT platform, such as the traffic, or location data, if any.

Specific Directives, (to be) implemented by the EU Member States, provide specific rules for data protection in the domain of publicly available electronic communications services, in particular in relation to traffic data and location data. This ePrivacy legislation also introduced

[46] Reform Proposal, Art. 33.

[47] Reform Proposal , Art. 33 §1 and §2.

[48] See Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, *O. J.* L 201, 31.07.2002, pp. 37-47as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 (*O. J.* L 337, 18.12.2009, pp. 11-36).

inter alia the obligation to notify personal data breach. Although the scope of these Directives is focused on ‘the right to privacy and confidentiality, with respect to the processing of personal data in the electronic communications sector’, the precise application field remains unclear and debated.

This deliverable does not focus on ePrivacy or on the use and processing of such other personal data, such as the logging of individual researchers or other persons using the BEAT platform. However, privacy and data protection regulation to this type of data applies as well, as for any web application. Users should therefore also take the existing national data protection regulation for the processing of this type of data as well as eprivacy into account (e.g., in relation to the use of cookies.

It is therefore needed that Type II Users – controller take the ePrivacy principles and obligations into account as well, for example when using cookies, if any, and in addition, if the platform would be offered online for a wide public, advised to comply with such provisions, for example in relation to the processing of traffic data

5. Type I Users: Privacy and Data Protection and Terms of Use

Type I Users as recipients

The Directive 95/46/EC defines the capacity of parties involved in the data processing. A *recipient* is defined as 'a natural or legal person, public authority, agency or any other body to whom data *are disclosed*, whether a third party[49] or not (..)'.[50]

Note on the current Reform Proposal: The current text defines recipient in the same way, meaning 'a natural or legal person, public authority, agency or any other body to which the personal data are *disclosed*' (art. 4.7).

►► Many users of the BEAT platform will only use the so-called front-end of the BEAT platform. They will not decide which databases will be uploaded on the platform and, even if they use the platform, have no access to the biometric data. BEAT partners decided that this type of user will not have direct access to the data, They will only receive the own or shared (depending on the use scenario) test results generated by the platform, including scores, or an attestation, but have direct access to the biometric data nor to any of its (pre)processed forms resulting from the evaluation. They will be having only indirectly access to biometric databases which are installed with the platform in the sense that they can use the databases as input of e.g. a submitted algorithm. In case the user merely runs or accesses the personal (biometric) data indirectly through the platform by online means for evaluation, e.g. of his or her own algorithm, without direct access, it could be defended that this means that the user is merely a recipient of the results of such use, such as scores[51], hence to whom particular data are merely 'disclosed' (see the definition *above*). However, it is not excluded that some may argue that the user becomes in this case processor of the data (e.g., by submitting an algorithm and running it through the biometric data for obtaining scores). Although the role and qualification of such user of the BEAT platform is somewhat unclear under the existing data protection regulation, the fact that the Type I User is only able to access the front-end computing infrastructure, without having direct access to the underlying biometric data, would in our view be important to argue that such user is not processor, but only recipient.

[49] 'Third party' is also defined. It means 'any natural or legal person, public authority, agency or any other body *other than* the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data' (Art. 2 (f) Directive -emphasis added). Recepients could hence be a natural or legal person or entity from within the organisation of the controller or the processor or from outside the organisation of the controller or the processor.

[50] Article 2(g) Directive (emphasis added).

[51] There has been discussion whether the comparison scores of a biometric system should be considered personal data. We take into account that scores could be considered biometric data.

The Directive 95/46/EC does not impose specific obligations upon the recipients, since mainly the controller and processor shall comply with the data protection obligations.

At the same time, it is relevant in the context of the BEAT platform from recipients that they do not attempt to access the underlying databases or other biometric data indirectly accessible through the platform.

►► The Privacy and Data Protection Terms of Use shall hence require from Type I Users-Recipients that they shall not attempt or try to directly access or copy, extract or reproduce in any other way the biometric data offered for use on the platform and to which they have in principle no direct access.

However, as soon as the recipients would also take decisions about using the (personal) data obtained through the platform for particular purposes, other than the going on data processing on the BEAT platform which another entity or party has organized, they may become controller for a new data processing (see *below*).

6. Type III Users: Acting on behalf of Type II Users: Privacy and Data Protection Principles and Terms of Use

Type III users are 'processors' of the (biometric) data processing on the platform

The "processor" is defined in the Directive 95/46/EC as a natural or legal person, public authority, agency or any other body which processes personal data *on behalf of* the controller.

►►As to the qualification of *processor*, this may apply to the 'administrator' as described in Beat Deliverable 2.1 if merely processing data *on behalf of the controller* (e.g., the administrator is uploading a biometric database upon the BEAT platform upon instruction and upon request of a user-controller on behalf of that user-controller). This may for example be the case for the *reviewer* who uses the platform to check whether claimed results correspond with those obtained with an experiment performed on the BEAT platform.[52] In that case, the reviewer(s) merely use(s) the platform and the data available through the platform on behalf and for the account of the 'administrator' or the 'user' (both can be controller) to (double)check the result.

The controller shall always enter into a *written contract* with the processor clearly setting out that the processor shall only act on instructions of the controller and shall implement the appropriate technical and organizational measures to protect the data (see also *below*) (see Article 17.3 Directive).

Such security measures are for biometric data of utmost importantance, considerig the nature and risks of the storage and use of such data.

National data protection legislation may also impose *additional conditions* relating to the content of such written controller-processor agreement, e.g., to specify the categories of personal data processed, …[53]

Note on the current Reform Proposal: The role of processor becomes more important and may further increase under the Reform Proposal.

[52] About this mechanism, see in more detail in D2.1, pp. 16-17.
[53] E.g., Federal German data protection legislation.

7. Proposed structure and content for the Terms of Use for the BEAT platform

Overall structure

The Terms of Use for the BEAT platform would consist of 3 parts:

- Use of biometric databases on the platform: Privacy and Data Protection Terms of Use

In any case, all Users need to be informed properly and should be made aware of their obligations in conformity with the data protection legislation, including the need to protect the biometric data. This will be done in the Privacy and Data Protection Terms of Use to be drafted for the platform.

- General Terms of Use

Users of the platform should also be aware and take responsibility in case the license terms for a particular data base does not allow the use of the database for commercial purposes. In such case, they need to confirm that they will keep the BEAT platform licensor harmless from and against any claim and/or damages in such respect.

In addition, because some information may remain with the BEAT platform ('Shared Information'[54]), it is not excluded that later users, which could also be industrial users, make use of this Shared Information. In such case, the BEAT platform owners or licensors should request the right to keep such Shared Information with the platform. In addition, the user might want to be clear on this issue when obtaining permission of the owner(s) of the biometric databases to use the databases on the BEAT platform, to be warranted as well.[55]

- Open Source Software Terms of Use for the BEAT platform

These terms will contain the open source software license conditions that will apply for the use of the BEAT platform.

- General remarks in relation to online acceptance of the Terms of Use and consumer protection

The acceptance of the Terms of Use by a person authorized by a Type I user – Recipient, a

[54] For a description, see below.
[55] See also *below*.

Type II user – Controller or Type III- User – processor could be off line or online. In the latter case, the validity of the expression of an agreement through an online click, shall be determined under national contract law.

Pursuant to the e-commerce directive, obstacles for online contracting in national Member States had to be removed. Therefore, contract law in most Member States will allow that contracts or binding undertakings do not have to be in paper form, but also electronically, which allows that such contracts can be concluded on line as well. In case of dispute, however, there may remain evidence issues in relation such electronic documents are not provided with an electronic signature, in case particular security measures were not applied, such as secure time stamping, logging, etc. For this reasons, it may be advisable to consider to enter into written agreements with the most important actors, using the BEAT platform, i.e. Type II and Type III users.

►►This implies that while in principle all users of the BEAT platform can be asked to agree online to accept particular Terms of Use, for example by clicking a particular box, paper agreements may be preferable from an evidence point of view. In any case, the information should be provided in a transparent way, and where consent is asked, preferably highlighted with an appropriate 'consent box'.

In addition, the Terms of Use shall also request confirmation that the actual person, expressing the consent, is authorized to represent the organization mentioned in the agreement for use of the BEAT platform and the Terms of Use.

In case a Type I user- Recipient would interact with the platform for purely private purposes, specific provisions, protecting consumers when online contracting and obtaining services, as determined in the EU Directive on consumer protection and implemented in national law, may apply. Specific provisions, in particular in relation to information and a right to revoke, may need to be mentioned in the terms of use for such users.

- Remarks and license terms in relation to a full understanding of the consequences of the use of the BEAT platform

Shared information[56]. Users of the platform further need to understand that the use of the BEAT platform, as developed, offers various advantages while at the same time involves users in progressing the state of the art of biometric system performance by participating and sharing information relating to previous tests performed on the BEAT platform. For this reason, some information relating to tests performed will remain with the BEAT platform and shared with other users. This should be transparent and addressed in the license terms as well.

Algorithms. The license terms may also explain to the users that the algorithms uploaded on the platform will remain the proprietary information of the user.

[56] See also *above*.

Modification of the license terms. The license terms proposed in this report, however, should be fit for further reviewed and possible updates. Users should be informed thereof. These updated license terms will appear on the API.

Conclusion

The present report aims to clarify the roles and obligations of entities using the BEAT platform.

In this deliverable, the roles of parties using the platform is explained as well as under which conditions such use of the platform can be made. Most users will be so-called Type I users, also recipients under the EU data protection legislation. Other parties, taking the decisions about the upload of the biometric databases and the use of the BEAT platform, will by Type II users-controllers. A third category may only perform activities on behalf of Type II users-controlles. Each of these categories have very specific obligations under the EU (national) data protection legislation, as explained herein.

As the BEAT platform is only an aggregation of biometry independent components, it remains however important the keep in mind that the actual use of the platform will always determine which roles and qualifications the parties involved and using the platform have.

Furthermore, under the current European data protection legislation, the use of the platform by controllers outside the EU requires the application of the data protection legislation if the platform and the data processed by the means of it is done in the context of activities of that controller in the Union. If the controller would not have such activities, the regulation would still apply in case of the use of 'equipment' (i.e. the platform) in the Union, if any. Under proposed modifications to the Directive 95/46/EC, while the use of 'equipment' is no longer a criterion for the territorial application of the data protection legislation in the Union, the offering of services in the Union, e.g., through the BEAT platform, would become the new criterion, requiring compliance with the data protection legislation effective in the Union.

The use of biometric data for research purposes is further an area which needs more research and analysis. Specific obligations for the use of personal data for research purposes (e.g., rendering the data anonymous) remain difficult if not impossible to apply. Legal authors are scarce and case law on the use of biometric data for research purposes not existing. In the meantime, different opinions remain as to when biometric data could be (or not) 'anonymous'. These difficulties identified will be subject of the deliverable 9.3 of this work package 9.

This report is a public deliverable in the BEAT project, which ends in 2016. Because of ongoing discussions on the data protection reform, and the BEAT project is not yet finished, this deliverable may be updated from time to time.

Annex A: Privacy and Data Protection Principles

Specifically for biometric data processing, see also the opinions and the recommendations of the Data Protection Working Party 29 in its Working document on biometrics of August 2003, and its follow up Opinion 3/2012 on developments in biometric technologies.[57]

1. Legitimate Processing on the BEAT platform requires a Legal Basis

The controller *must verify for each processing* of personal data whether such processing is based and *covered by one of the legal grounds mentioned in the (national) applicable data protection legislation*.

The Directive 95/46/EC states that the processing of personal data *is only legitimate if*:

- the data subject has given his or her unambiguous consent[58]; or
- it is necessary to perform a contract of which the data subject is a party ; or
- it is necessary to comply with a legal obligation imposed upon the controller; or
- it is necessary to protect the data subject's vital interests; or
- it is necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
- it is necessary to pursue legitimate interests of the controller or a third party to whom the data is disclosed, except if those interests are outweighed by the fundamental rights and freedoms of the data subject.

Note on the current Reform Proposal: The current version basically maintains these legal grounds.

2. Purpose Specification and Finality Principle – Fairly and Lawful processing

Any personal data must be collected for *specified, explicit and legitimate purposes* to be determined by the controller and must be processed in a *compatible way* with these purposes. To verify that the processing is compatible with the original purpose, the expectations of the data subject may also be taken into account.

Note on the current Reform Proposal: The current version basically maintains this principle.

[57] The Article 29 WP is the independent EU Advisory Body on Data Protection and Privacy established by the Directive. The working documents of the The Article 29 WP reflects the view of the national Data Protection Authorities on biometric systems and data protection.

[58] The data subject's consent is defined as "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

For the BEAT platform, controllers shall *carefully specify* the purposes of the processing. Data which were already collected for (research) purposes, shall be processed only for (research) purposes *compatible with the original purposes*. The controller(s) shall hence carefully select the databases for use upon the BEAT platform in each of the use cases described in D2.1. and ensure that the processing of the biometric (and other) data complies with this principle.

If this would not be possible or the case, and the biometric data are re-used, the controller shall consider the processing as a new personal data processing and shall start with reviewing and applying all applicable data protection obligations to this new personal data processing (e.g., new notification/authorization, new information to the data subjects (see below), etc.).

For example, company X has collected an own database for *internal research purposes use*, including for improving algorithms. Company X however now envisages to use the BEAT platform for modifying one or more parameters or code-blocks in an existing task (see use case 2.3 as described in D2.1). One can defend that this use by Company X of the data on the platform is compatible with the original purposes. Company X however should not have third parties access the platform and letting these third parties use its 'own' database, for example for a comparative evaluation (see use case 2.5 as described in D2.1), unless Company X ensures the compliance with all data protection obligations for this new processing (e.g., consent, information, notification, …).

In addition, personal data must be processed *fairly and lawfully.* This is a fairly broad principle, and in general means that the processing shall not be contrary to any law. Some indicate that this 'law' is the data protection legislative framework, while other scholars point to the need to review the processing under any other legislation, including the fundamental rights of the data subjects, such as the right not to be discriminated and the (fundamental) right to protection of privacy and to data protection.

3. Relevancy, Adequacy and Proportionality principle

The personal data processed must be *adequate, relevant and not excessive* in relation to the purposes for which it is collected and processed (Article 6.1,c Directive 95/46/EC). This is an important principle of the data protection legislation which bears also a close relation with the finality principle mentioned above: the relevancy and necessity will be reviewed in relation with the purpose(s) for which the data are collected and processed. This obligation is also known as the basis of the proportionality principle. The proportionality principle is a general principle of law, applicable in many domains of law, generally imposing that the means (e.g., the data collected, selected, the processing, ..) shall be fit and not excessive in relation to the purposes.

The proportionality of the use of biometric data *is a very important criterion* and principle in order decide whether the processing of the biometric data is lawful.

The personal data processed must in addition be *accurate* and *kept up to date,* where necessary. Inaccurate or incomplete data must be erased or rectified.

Note on the current Reform Proposal: the current proposal stresses data minimisation and states that personal data may only be used 'if, and as long as, the purposes could not be fulfilled by processing information that does not involve personal data' (art. 5 c Reform proposal).

Note on current reform proposals: The current proposal of Regulation restricts the processing of personal data for research purposes in so far that such personal data may only be used if the research purposes cannot be obtained by anonymous data[59] and, in that case, the data enabling the attribution of the information to a particular person is kept separately from the other information, to the extent possible (art. 83 Reform proposal). Specific rules are suggested for publication of research results as well.

►►Anonymous data do not allow to relate the data, either directly, but also indirectly (see above) to an individual. Unique biometric characteristics and the data based thereupon in principle allow to identify, hence cannot be considered anonymous data. 'Anonymous' biometric data is hence a contradiction.

4. Obligation upon controller to Notify - Prior checking in specific situations

The Directive imposes an obligation upon the Member States to have a procedure in place which obliges the controller of an automated filing system to make a *notification* to the local Data Protection Authority *prior to* carrying out any processing operation.

The purpose of the notification and related provisions is mainly to ensure transparency and provide information to the public. However, the Member States have the possibility, with regard to certain categories of processing operations, to provide for a simplification for such notification (e.g., in France) or for an exemption from notification (e.g., if a data protection officer is appointed (for example, in Germany).

In addition, the Directive provides that there may be situations where further investigation by the supervisory authority or by the data protection official is both relevant and desirable. In that case, *prior checking* with the supervisory authority is mandatory (Article 20 of the Directive).

In case biometric data are saved in for example a central database, the Working Party recommends that the Member States require prior checking by a legislative measure.

5. Security and confidentiality

The controller must implement appropriate technical and organizational measures to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorized disclosure

[59] About this concept, see also A. Cavoukian and M. Snijder, *A Discussion of Biometrics for Authentication Purposes : The Relevance of Untraceable Biometrics and Biometric Encryption*, July 2009.

or access or other forms of unlawful processing (see Article 17 Directive).

The controller shall for example restrict access to the processing (e.g., by making a list of persons authorized to have access to the application) or use encrypted data to preserve the security of the data. The controller must strike the right balance of security between the nature of the data to be protected, the costs involved and leading edge technology.

The local applicable laws will have several provisions relating to data security. Please note that some countries (for example, Spain, Belgium,) may have very detailed rules governing the data security.

It is clear that with regard to biometric data, the organizational and technical security of the data processing is of utmost importance.

For example: The security measures will in principle include restricted access to biometric data by authorized individuals only under the supervision of the controller, setting up a list of persons involved and require secured storage. Access to the platform or system shall also be secured by an appropriate log-in sysem, access logged and audited and any equipment used for the data processing in a physically secured place. National data protection regulations in this area however shall be closely reviewed and applied.

The Directive also provides that "any person acting *under the* authority *of* the controller or *of* the processor, *including the p*rocessor himself, who has access to personal data, must not process them except on *instructions from* the controller, unless he *is required to do so by* law". This provision also imposes a *confidentiality obligation* (see Article 16 Directive).

The controller may delegate the processing of personal data to a natural or legal person. In that case, the controller shall enter into a written contract which stipulates that the processor will act solely on the controller's instructions, will deploy adequate organizational and security measures for the data processing and will comply with the law.

6. Controller(s) shall inform the data subjects, unless national law provides an exemption for re-use for research purposes

Right of the data subject to receive information

The Directive 95/46/EC states that whether the data is collected directly from the data subject or from a third party, the data subject *must be informed* of:
1) the identity of the controller and his representative, if any; and
2) the purposes of the processing.
If it is necessary to guarantee fair processing towards the data subject (having regard to the specific circumstances in which the data are collected), additional information must be given, including :
1) people or organizations or categories of recipients[60] who will be given the data;

[60] A "recipient" is defined in the Directive as any natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not.

2) whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply.
3) the data subject's right to access his or her file and right to rectify his or her data that is erroneous or incomplete.

If personal data has not been obtained from the data subject, the data subject must be informed about *the categories of data concerned* by the processing.

Exceptions to this obligation to provide the data subject the above information may exist in some Member States, in particular for processing for statistical purposes or for the purposes of historical or scientific research if providing this information is impossible or involves a disproportionate effort.

The above information must be given to the data subject as soon as possible, in principle *when the data is collected*. If the data is not directly obtained from the data subject, the information must be given when the data is recorded or if disclosure to a third party is envisaged, not later than the time when the data is disclosed for the first time.

The Directive does not state how the information must be given to a data subject (orally or in writing, separately to each individual or in a public way). However, a written document is recommended for evidence purposes. Here also, it is important to check a Member State's data protection law.

Because each Member State has implemented the information obligation of the Directive in a somewhat different way, it is important to check the applicable Member State's data protection law and the allowed exceptions to the obligation of information. Because of the use of personal data, including biometric data, the exact definition of the purposes of the use of the data (see above) and the identity of the controller of the file is crucial.

7. Controller(s) shall respect the rights to access and correction of the data subject and the right to object

Right of the data subject access and correction

Controllers are also required to give data subjects a right of access to *inter alia* the following information "without constraint and at reasonable intervals": 1) confirmation as to whether or not data relating to him are being processed, the purpose of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed; and 2) communication to him in an intelligible form of the data undergoing processing and of any available information as to the source of the data.

It should be noted that the right of access by the individual does not always applies as described in the Directive, e.g., in case of the processing of personal data for national or public security or, by a legislative measure used solely for scientific research subject to adequate safeguards (Article 13 of the Directive). When the BEAT platform is used, controllers may want to review whether the national laws contain an exemption to this right of access.

Unless it proves impossible or involves a disproportionate effort, third parties to whom incorrect or incomplete data have been disclosed should be notified.

Right to object ?

The Directive states that the data subject has a right to object to the processing of data relating to him in certain circumstances.[61]

The Member States must ensure that data subjects have this right at least in cases of processing in the public interest and processing in the legitimate interests of the data controller.

Type II BEAT Users-Controllers relying on legitimate interests for using particular biometic databases shall hence take into account that the data subject can thus invoke his right to object *at any time* on compelling legitimate grounds relating to his particular situation to the processing of data relating to him in these situations, save where otherwise provided by national legislation.

[61] Directive 95/46/EC, Article 14.

Annex B : Example controller-processor agreement

Agreement

Between :

[Type II User - controller] _____ (name and address of company), duly represented by _____ (name and function) and _____(name and function),

Hereinafter : the Controller,

And :
[Type III User - processor]_____ (name and address of company), duly represented by _____(name and function) and _____(name and function),

Hereinafter : the Processor,

Whereas

Parties are partners in _____ and agreed to cooperate for the use of the BEAT platform, which is to serve as platform for _____ scenario for testing the technological results _____;

[Type II User - controller] is willing to take the responsibility for the acquisition and management of certain personal data, including biometric data, for above purposes in relation with the BEAT platform, , as the controller of the personal data ;

[Type III User - processor] agrees to _____ and to process the personal data on behalf of the controller for the above purposes in accordance with the instructions of the controller and with the applicable data protection laws ;

Therefore, it has been agreed as follows :

Article 1 – Definitions

1.1. 'Personal Data' shall have the same meaning as in 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 date (hereinafter Directive 95/46/EC). Biometric data will be included in the Personal Data.

1.2. 'the Controller' shall have the same meaning as in Directive 95/46/EC.

1.3. 'the Processor' shall have the same meaning as in Directive 95/46/EC and means the entity who agrees to collect, to process or to receive from the Controller personal data intended for processing on his behalf in accordance with his instructions, the terms of this Agreement and the applicable data protection laws.

1.4. 'BEAT platform' shall mean the platform for research and testing purposes as described and agreed in _____.

Article 2 - Subject

2.1.1. The Controller requests the Processor, who accepts and agrees, to process on his behalf and in compliance with his instructions Personal Data as specified and agreed for the _____scenario.

2.1.2. Parties agree that the specifications and the instructions for the processing of the Personal Data for the testing purposes of the _____scenario are further described in _____, attached in Appendix 1 to this Agreement, and in additional documentation that parties may agree from time to time.

Article 3 – Warranties and obligations of the Controller

3.1. The Controller agrees and warrants that he has instructed and throughout the duration of the Personal Data processing services will instruct the Processor to process the Personal Data only on the Controller's behalf and in accordance with the applicable data protection laws.

3.2. The Controller will instruct the Processor on the technical and organizational security measures required by the national data protection laws and as specified in Appendix 2, to be implemented by the Processor. Parties agree and belief that to the best of their knowledge these measures are adequate to protect the Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, having regard to the state of the art and the cost of their implementation.

Article 4 – Warranties and obligations of the Processor

4.1. The Processor agrees and warrants that he has followed and throughout the duration of the Personal Data processing services will follow the instructions of the Controller to process the Personal Data and will process the Personal Data only on the Controller's behalf and in accordance with the applicable data protection laws.

4.2. The Processor further agrees that he shall not apply or use the Personal Data for purposes other than specified in this Agreement and shall not communicate the Personal Data to third parties, even not for their preservation.

4.3. Processor undertakes and warrants that he will implement the technical and organizational security measures specified in Appendix 2 before processing the Personal Data.

4.4. The Processor undertakes and agrees to deal promptly and properly with all inquiries from the Controller relating to his processing of the Personal Data for the _____scenario and to abide by the advice of the supervisory authority with regard to the processing of this Personal Data.

4.5. The Processor agrees and undertakes to promptly notify the Controller about (1) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless prohibited by law, (2) any accidental or unauthorized access, and (3) any request received from the data subjects.

4.6. In case of a request received from the data subjects, the Processor shall not respond to such request without prior consultation and the express authorization to do so from the Controller.

Article 5 – Term and Termination

5.1. The Agreement is concluded for a period and the time required for the _____scenario as defined in _____.

5.2. Each party is entitled to terminate this Agreement before the end of the aforementioned period with a notice period of one (1) month in case the other party

does not comply with its obligations under this Agreement and failed to remedy such default within fourteen (14) days after due notice.**(notice periods can be changed – please advise).**

5.3. Parties agree that on the termination of the provision of data processing services, the Processor shall, at the choice of the Controller, transmit and/or return all the Personal Data collected and/or received from the Controller and all the copies, support and documentation containing Personal Data processed thereof or shall destroy all the Personal Data and certify to the Controller that he has done so, unless legislation imposed upon the Processor prevents him from returning or destroying such data. In that case, the Processor warrants that he will guarantee the confidentiality of the Personal Data and will not actively process the Personal Data anymore.

Article 6 – Applicable law, Mediation and Jurisdiction

6.1. The laws of the _____ shall apply to this Agreement. Specific laws applicable to the processing of personal data and processors may in addition apply.

6.1. In case of a dispute, parties will try to solve the issue in an amicable way.

6.3. In case a dispute cannot be settled in due time, either party may bring the dispute to a competent court in _____.

Done in _____, on _____ (date), in two copies, each party having received one.

The Processor

_____ (name and function)

_____ (name and function)

The Controller

_____ (name and function)

_____ (name and function)

Appendix 1 : _____scenario.
Appendix 2 : Technical and organizational security measures

Annex C: Overview of the use cases as described in D 2.1 relevant for Type I, Type II and Type III Users

In view of the ten use cases mentioned in D2.1, the possible roles are hereunder summarized in a tentative way for each of the use cases:

The use case 2.2 (security attestation) is the most simple use case in terms of defininig the controller and processor in that the 'administrator' will be the controller and the 'users' will only receive a certificate.

The use cases 2.1, 2.5 and 2.10 are similar in that a 'third party' (examiner) may be organizing respectively the benchmarking, comparative evolution or the use of the platform as an educational tool and in this sense take the decision about the use of particular databases and the choice of the use of the platform and hence may be controller. However, this role could also be taken up by the 'administrator' as described in D2.1 and 2.10. In some cases, the third party (e.g., an examiner or reviewer having access to the BEAT platform under the attestation mechanism (see D2.1, pp. 16-17) may also be a recipient.

In the use cases 2.3, 2.4, 2.6, 2.7, 2.8 and 2.9 there are basically two possibilities: either the 'administrator' or the 'user'[62] can be the controller.

For a more detailed overview, see hereunder;

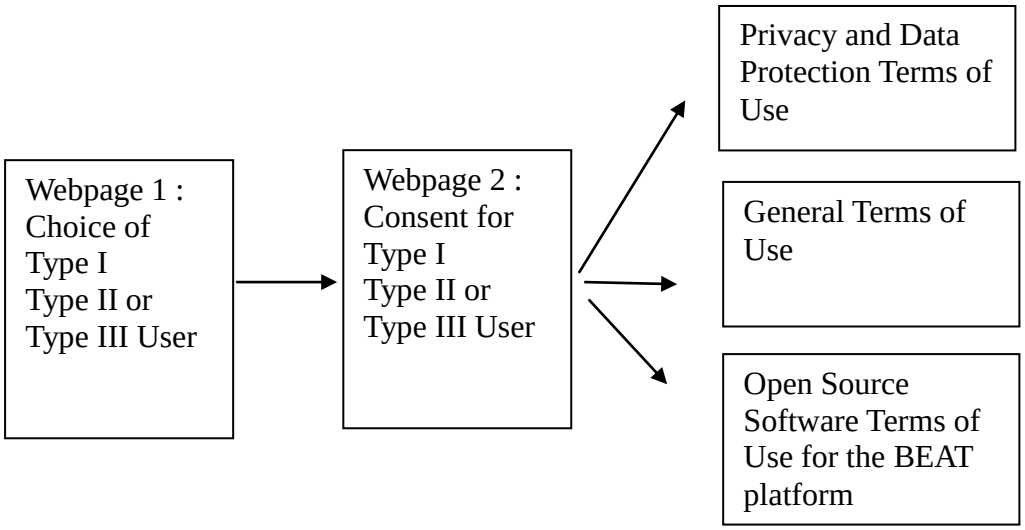
[62] For example, if the 'user' disposes of own biometric databases used only for internal research purposes.

Use cases	Controller ?	Processor ?	Co-controller ?	Comments	Additional Comments
2.1 Benchmarking (Scenario a)	'administrator' This will be a 'standard benchmarking evaluation' where 'required database will be available' (D2.1, p. 12), as decided by the administrator.		'user' ? This remains unclear.	The (end-)users will not process the data on behalf of the controller, and hence would not be processor. It is likely that the end-users could also be considered 'recipients' as they will receive limited information, such as and scores, without however having access to whole or part of the biometric databases	It is presumed that the 'administrator' hence will decide about (and take the responsibility for) the database(s). Is should be reviewed however whether the user could also in particular circumstances become co-controller.
2.1 Benchmarking (Scenario b)	'third party' e.g., international standardization body	'admini-strator'	'administrator and 'third party' could also be co-controllers - depending on factual circumstances	This will be a 'standard benchmarking evaluation' where 'required database will be available', upon decision of the third party. About the end-users, same comment as for 2.1 Benchmarking (scenario a).	It is in this scenario presumed that the 'third party' hence will decide about (and take the responsibility for) the database(s) and the use of the BEAT platform.
2.2. Security Attestation	'administrator'			The 'administrator' is deciding about the databases, their use on the platform and the purposes of their use (security attestation) About the end-users, same comment as for 2.1 Benchmarking (scenario a).	

Use cases	Controller ?	Processor ?	Co-controller ?	Comments	Additional Comments
2.3 Evaluation (Scenario a)	'administrator'		'administrator and 'user' could also be co-controllers - depending on factual circumstances	It is presumed that the 'administrator' decides not only about the use of the platform but *also about the databases* to be used (and the tests). About the end-users, same comment as for 2.1 Benchmarking (scenario a).	It could be clarified who decides about (and takes the responsibility for) the databases to be used for the evaluation on the platform.
2.3 Evaluation (Scenario b)	'user'	'administrator' (if any)	'administrator and 'user' could also be co-controllers - depending on factual circumstances	It is presumed that the 'user' in this case decides not only about the use of the platform but *also about the databases* to be used (and the tests).	It could be clarified who decides about (and takes the responsibility for) the databases to be used for the evaluation on the platform.
2.4 Sensitivity	Same as the use case 2.3 (scenario a and scenario b)	Same as the use case 2.3 (scenario a and scenario b)	Same as the use case 2.3 (scenario a and scenario b)	Same as the use case 2.3 (scenario a and scenario b)	Same as the use case 2.3 (scenario a and scenario b)
2.5 Comparative Evaluation	'third party' (challenge organizer)	'administrator'		It is hereby presumed that the challenge organizer decides about the 'one or more databases' (D2.1. p. 20) About the end-users, same comment as for 2.1 Benchmarking (scenario a).	It is not clear however who decides about (and takes the responsibility for) the databases to be used on the platform. This could be clarified
2.6 Biometric algorithm optimisation	Same as use cases 2.3 and 2.4 (scenario a and scenario b)	Same as use cases 2.3 and 2.4 (scenario a and b)	Same as use cases 2.3 and 2.4 (scenario a and scenario b)	Same as use cases 2.3 and 2.4 (scenario a and scenario b)	Same as use cases 2.3 and 2.4 (scenario a and scenario b)

Use cases	Controller ?	Processor ?	Co-controller ?	Comments	Additional Comments
2.7 Biometric System Optimisation	Same as use cases 2.3, 2.4 and 2.6 (scenario a and scenario b)	Same as use cases 2.3, 2.4 and 2.6 (scenario a and scenario b)	Same as use cases 2.3, , 2.4 and 2.6 (scenario a and scenario b)	Same as use cases 2.3, 2.4 and 2.6 (scenario a and scenario b)	Same as use cases 2.3, 2.4 and 2.6 (scenario a and scenario b)
2.8 Multimodal biometric system brokerage	Same as use cases 2.3, 2.4, 2.6 and 2.7 (scenario a and scenario b)	Same as use cases 2.3, 2.4, 2.6 and 2.7 (scenario a and scenario b)	Same as use cases 2.3, 2.4, 2.6 and 2.7 (scenario a and scenario b)	Same as use cases 2.3, 2.4, 2.6 and 2.7 (scenario a and scenario b)	Same as use cases 2.3, 2.4, 2.6 and 2.7 (scenario a and scenario b)
2.9 Quality assessment	Same as use cases 2.3, 2.4, 2.6, 2.7 and 2.8 (scenario a and scenario b)	Same as use cases 2.3, 2.4, 2.6, 2.7 and 2.8 (scenario a and scenario b)	Same as use cases 2.3, 2.4, 2.6, 2.7 and 2.8 (scenario a and scenario b)	Same as use cases 2.3, 2.4, 2.6, 2.7 and 2.8 (scenario a and scenario b)	Same as use cases 2.3, 2.4, 2.6, 2.7 and 2.8 (scenario a and scenario b)
2.10 Educational Resource (Scenario a)	‘administrator’	The examiner/teacher		About the end-users, same comment as for 2.1 Benchmarking (scenario a). The examiner/teacher could however also be a recipient. In the case of students, this type of use, however, may be considered for ‘purely personal purposes’ and hence for their processing (only) outside the scope of data protection regulation.	It is presumed in this case that the administrator decides about (and takes the responsibility for) the databases to be used on the platform.
2.10 Educational Resource (Scenario b)	The examiner/teacher	‘administrator’		About the end-users, same comment as for 2.1 Bench-marking (scenario a). In the case of students, see above.	It is presumed in this case that the examiner/teacher decides about (and takes the responsi-bility for) the databases to be used on the platform.

Annex D: Overview of acceptance of Terms of Use – Possible scenario



Annex E: Terminology

Note : Any emphasis used in the descriptions and definitions are our own.

Abbreviation / acronym	Description
Controller	The natural or legal person, public authority, agency or any other body which alone or jointly with others *determines the purposes and means* of the processing of personal data (Art 2 (d) EU Directive 95/46/EC).
Data subject	An individual who can be *identified or is identifiable*, directly or indirectly, in particular by reference to an identification number or to *one or more factors specific to his or her physical,* physiological, mental, economic, cultural or social identity (see Art 2.a EU Directive 95/46/EC). In the context of biometric data processing, the data subject is a natural person whose biometric data based on his or her biometric characteristics have been collected and are used.
Directive 95/46/EC	Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (*O.J.* L 281, 23.11.1995), presently under review.
DPA(s)	Data Protection Authority/ies
ePrivacy	Principles and rules as set out in Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, as amended by Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.
Personal data	Any information relating to an *identified or identifiable* natural person (data subject).
Processor	A natural or legal person, public authority, agency or any other body which processes personal data *on behalf of* the controller (Art 2 (d) EU Directive 95/46/EC).
Proposed 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, COM(2012) 11 final, 25.1.2012
Recipient	A natural or legal person, public authority, agency or any other body to whom data are *disclosed*, whether a third party or not (see art 2 (g) EU Directive 95/46/EC).

Reform Proposal	See Proposed General Data Protection Regulation.
'Sensitive' data	Data revealing 'racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership', and 'data concerning health or sexual life' (see current Art. 8 Directive) (see also Art. 9 Proposed General Data Protection Regulation, including 'genetic data' and data concerning 'criminal convictions or related security measures').
Third party	Any natural or legal person, public authority, agency or any other body *other than* the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data (see art 2 (f) EU Directive 95/46/EC).
Type I User	The user of the BEAT platform *without determining* which biometric databases will be offered in combination with the BEAT platform.
Type II User	The user of the BEAT platform who determines *which biometric databases* will be offered for use in combination with the BEAT platform and the *purposes* of the biometric databases and BEAT platform use.
Type III User	The user of the BEAT platform acting on behalf of the Type II User.