Enhanced Affective Wellbeing based on Emotion Technologies for adapting IoT spaces

D1.3 Ethical guidelines

Consortium:	**ITEA3**
Deliverable ID:	**D1.3**
Work package/Task:	**WP1**
Responsible partner:	**UPMC**
Contributing partner(s):	**ALL PARTNERS**
Dissemination level:	**Public**

This page is intentionally left blank.

Index

Document history

Revision	Date	Content description/Modification	Author(s)
V0.1	12/05/2017	Creation	M. Tufis (UPMC)
V0.2	31/05/2017	Structure update according to the ITEA3 requirement	M. Tufis (UPMC)
V0.3	18/03/2018	Structure update according to the ITEA3 requirement	F. Berreby (UPMC)
V0.4	08/02/2019	Structure update according to the ITEA3 requirement	A. Bretel (UPMC)

Glossary

EmoSpaces	Enhanced Affective Wellbeing based on Emotion Technologies for adapting IoT spaces
ITEA3	Information Technology for European Advancement 3
Bias	Bias is a prejudice for or against something or somebody, that may result in unfair decisions. It is known that humans are biased in their decision making. Since AI systems are designed by humans, it is possible that humans inject their bias into them, even in an unintended way. Many current AI systems are based on machine learning data-driven techniques. Therefore a predominant way to inject bias can be in the collection and selection of training data. If the training data is not inclusive and balanced enough, the system could learn to make unfair decisions. At the same time, AI can help humans to identify their biases, and assist them in making less biased decisions.
Binding corporate rules	According to Article 4(20) of GDPR: "personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity".
Biometric data	According to Article 4(14) of GDPR: "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".
Confidentiality	Confidentiality in a general sense refers to the duty not to share information with persons who are not qualified to receive that information. In a more specific sense, it refers to the confidentiality of communications provided for in Article 5 of the E-privacy Directive 2009/136/EC and in Article 36 of Regulation (EC) No 45/2001. Confidentiality of processing also refers to the obligation of any person acting under the authority of the controller or the processor, who has access to personal data, not to process them except on instructions from the controller, unless he is required to do so by law (Article 21 of Regulation (EC) No 45/2001).
Consent	According to Article 4(11) of GDPR: "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the

	processing of personal data relating to him or her". Consent is an important element in data protection legislation, as it is one of the conditions that can legitimise processing of personal data. If it is relied upon, the data subject must unambiguously have given his/ her consent to a specific processing operation, of which he/she shall have been properly informed. The obtained consent can only be used for the specific processing operation for which it was collected, and may in principle be withdrawn without retroactive effect.
Controller	According to Article 4(7) of GDPR: "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data".
Data concerning health	According to Article 4(15) of GDPR: "personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status".
Data Protection Officer (DPO)	The Data Protection Officer ensures, in an independent manner, that an organization applies the laws protecting individuals' personal data. The designation, position and tasks of a DPO within an organization are described in Articles 37, 38 and 39 of the EU GDPR.
Ethical purpose	In this document, ethical purpose is used to indicate the development, deployment and use of technology which ensures compliance with fundamental rights and applicable regulation, as well as respecting core principles and values.
Filing system	According to Article 4(6) of GDPR: "any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis".
General Data Protection Regulation (GDPR)	The General Data Protection Regulation (EU) 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. Superseding the Data Protection Directive 95/46/EC, the regulation contains provisions and requirements pertaining to the processing of personal data of individuals (formally called data subjects in the GDPR) inside the EEA, and applies to an enterprise established in the EEA or—regardless of its location and the data subjects' citizenship—that is processing the personal information of data subjects inside the EEA.
Genetic data	According to Article 4(13) of GDPR: "personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and

	which result, in particular, from an analysis of a biological sample from the natural person in question”.
Main establishment	According to Article 4(16) of GDPR: “(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment; (b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation”.
Personal data	According to Article 4(1) and 4(12) of RGDP: “any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; ‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”. The name and the social security number are two examples of personal data, which relate directly to a person. But the definition also extends further and also encompasses for instance e-mail addresses and the office phone number of an employee. Other examples of personal data can be found in information on physical disabilities, in medical records and in an employee's evaluation. Personal data that is processed in relation to the work of the data subject remain personal/individual in the sense that they continue to be protected by the relevant data protection legislation, which strives to protect the privacy and integrity of natural persons. As a consequence, data protection legislation does not address the situation of legal persons (apart from the

	exceptional cases where information on a legal person also relates to a physical person).
Processing	According to Article 4(2) and 4(3) of GDPR: “any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future”.
Processor	According to Article 4(8) of GDPR: “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”.
Profiling	According to Article 4(4) of GDPR: “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements”.
Pseudonymisation	According to Article 4(5) of GDPR: “the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person”.
Recipient	According to Article 4(9) of GDPR: “a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing”.
Representative	According to Article 4(17) of GDPR: “a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation”.
Sensitive data	Sensitive data include data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life" (Article 10 of Regulation 45/2001).

	The processing of such information is in principle prohibited, except in specific circumstances. It is possible to process sensitive data for instance if the processing is necessary for the purpose of medical diagnosis, or with specific safeguards in the field of employment law, or with explicit consent of the data subject.
Supervisory authority	According to Article 4(21) and 4(22) of GDPR: “an independent public authority which is established by a Member State pursuant to Article 51; ‘supervisory authority concerned’ means a supervisory authority which is concerned by the processing of personal data because: (a) the controller or processor is established on the territory of the Member State of that supervisory authority; (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or (c) a complaint has been lodged with that supervisory authority”.
Third party	According to Article 4(10) of GDPR: “a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data”.
Video surveillance	Video-surveillance is the monitoring of a specific area, event, activity, or person by means of an electronic device or system for visual monitoring. Typically, the monitoring is carried out using CCTV systems.

1. Introduction

The problems with current state of the art technologies is the lack of a holistic infrastructure to collect data from different sources (sensors, portals, wearable devices) and to translate data into meaningful information as universal meta-data, which can be processed to characterize the context and the activity of the users. Until today most of the product of the market and research and innovation projects where focusing only on the recognition of some affects, location and some basic physical activities (motions) of users independently from their context. Unfortunately due to several technological issues they put into background the recognition of complex activities and context and their relation to the cognitive abilities of users when they are using applications and services or interacting with other mates.

In EmoSpaces, we are targeting to solve these issues and work on new technologies for capturing/recognizing social and emotional cues/signals and their associate models for characterizing the behavior of users in smart spaces as well as their cognitive and physical context. This research is strongly needed today to make a real shift in the way to augment the level of responsiveness and adaptability of smart spaces and assistive agents. Moreover, we will put these technologies in suitable holistic architecture to guarantee their uptake and sustainability for the market. The architecture must guarantee an adaptive use, effective transmission and accurate interpretation by the actors and stakeholders in the value chain.

2. Scope and deliverable objectives

2.1. Scope

This deliverable concerns Task 1.5 (WP1), entitled “Ethical, social and privacy issues”.

2.2. Deliverable objectives

The purpose of this deliverable is to establish an ethical issue management plan for the user and business requirements analysis and to develop the user studies involvement. The plan will ensure the safeguard of ethical, social and privacy rights of all involved end users.

3. Glossary

The following are excerpts from the Glossary compiled by the European Data Protection Supervisor [5], the European Commission’s – High-level Expert Group on Artificial Intelligence [11] and the General Data Protection Regulation [13].

3.1. Bias

Bias is a prejudice for or against something or somebody, that may result in unfair decisions. It is known that humans are biased in their decision making. Since AI systems are designed by humans, it is possible that humans inject their bias into them, even in an unintended way. Many current AI systems are based on machine learning data-driven techniques. Therefore a predominant way to inject bias can be in the collection and selection of training data. If the training data is not inclusive and balanced enough, the system could learn to make unfair decisions.

3.2. Binding corporate rules

According to Article 4(20) of GDPR: "personal data protection policies which are adhered to by a controller or processor established on the territory of a Member State for transfers or a set of transfers of personal data to a controller or processor in one or more third countries within a group of undertakings, or group of enterprises engaged in a joint economic activity".

3.3. Biometric data

According to Article 4(14) of GDPR: "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data".

3.4. Confidentiality

Confidentiality in a general sense refers to the duty not to share information with persons who are not qualified to receive that information. In a more specific sense, it refers to the confidentiality of communications provided for in Article 5 of the E-privacy Directive 2009/136/EC and in Article 36 of Regulation (EC) No 45/2001.

Confidentiality of processing also refers to the obligation of any person acting under the authority of the controller or the processor, who has access to personal data, not to process them except on instructions from the controller, unless he is required to do so by law (Article 21 of Regulation (EC) No 45/2001).

3.5. Consent

According to Article 4(11) of GDPR: "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her".

Consent is an important element in data protection legislation, as it is one of the conditions that can legitimise processing of personal data. If it is relied upon, the data subject must unambiguously have given his/ her consent to a specific processing operation, of which he/she shall have been properly informed. The obtained consent can only be used for the specific processing operation for which it was collected, and may in principle be withdrawn without retroactive effect.

3.6. Controller

According to Article 4(7) of GDPR: “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data”.

3.7. Data concerning health

According to Article 4(15) of GDPR: “personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status”.

3.8. Data Protection Officer

The Data Protection Officer ensures (DPO), in an independent manner, that an organization applies the laws protecting individuals’ personal data. The designation, position and tasks of a DPO within an organization are described in Articles 37, 38 and 39 of the EU General Data Protection Regulation (GDPR).

3.9. Ethical purpose

In this document, ethical purpose is used to indicate the development, deployment and use of technology which ensures compliance with fundamental rights and applicable regulation, as well as respecting core principles and values.

3.10. Filing system

According to Article 4(6) of GDPR: “any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis”.

3.11. General Data Protection Regulation

The General Data Protection Regulation (EU) 2016/679 (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union (EU) and the European Economic Area (EEA). It also addresses the export of personal data outside the EU and EEA areas. The GDPR aims primarily to give control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. Superseding the Data Protection Directive 95/46/EC, the regulation contains provisions and requirements pertaining to the processing of personal data of individuals (formally called data subjects in the GDPR) inside the EEA, and applies to an enterprise established in the EEA or—regardless of its location and the data subjects' citizenship—that is processing the personal information of data subjects inside the EEA.

3.12. Genetic data

According to Article 4(13) of GDPR: “personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question".

3.13. Main establishment

According to Article 4(16) of GDPR:

> "(a) as regards a controller with establishments in more than one Member State, the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union and the latter establishment has the power to have such decisions implemented, in which case the establishment having taken such decisions is to be considered to be the main establishment;
>
> (b) as regards a processor with establishments in more than one Member State, the place of its central administration in the Union, or, if the processor has no central administration in the Union, the establishment of the processor in the Union where the main processing activities in the context of the activities of an establishment of the processor take place to the extent that the processor is subject to specific obligations under this Regulation".

3.14. Personal data

According to Article 4(1) and 4(12) of RGDP: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person; 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed".

The name and the social security number are two examples of personal data, which relate directly to a person. But the definition also extends further and also encompasses for instance e-mail addresses and the office phone number of an employee. Other examples of personal data can be found in information on physical disabilities, in medical records and in an employee's evaluation.

Personal data that is processed in relation to the work of the data subject remain personal/individual in the sense that they continue to be protected by the relevant data protection legislation, which strives to protect the privacy and integrity of natural persons. As a consequence, data protection legislation does not address the situation of legal persons (apart from the exceptional cases where information on a legal person also relates to a physical person).

3.15. Processing

According to Article 4(2) and 4(3) of RGDP: "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; ‘restriction of processing’ means the marking of stored personal data with the aim of limiting their processing in the future”.

3.16. Processor

According to Article 4(8) of GDPR: “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”.

3.17. Profiling

According to Article 4(4) of GDPR: “any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements”.

3.18. Pseudonymisation

According to Article 4(5) of GDPR: “the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person”.

3.19. Recipient

According to Article 4(9) of GDPR: “a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing”.

3.20. Representative

According to Article 4(17) of GDPR: “a natural or legal person established in the Union who, designated by the controller or processor in writing pursuant to Article 27, represents the controller or processor with regard to their respective obligations under this Regulation”.

3.21. Sensitive data

Sensitive data include data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life" (Article 10 of Regulation 45/2001).

The processing of such information is in principle prohibited, except in specific circumstances. It is possible to process sensitive data for instance if the processing is necessary for the purpose of medical diagnosis, or with specific safeguards in the field of employment law, or with explicit consent of the data subject.

3.22. Supervisory authority

According to Article 4(21) and 4(22) of GDPR: "an independent public authority which is established by a Member State pursuant to Article 51; 'supervisory authority concerned' means a supervisory authority which is concerned by the processing of personal data because:

> (a) the controller or processor is established on the territory of the Member State of that supervisory authority;
>
> (b) data subjects residing in the Member State of that supervisory authority are substantially affected or likely to be substantially affected by the processing; or
>
> (c) a complaint has been lodged with that supervisory authority".

3.23. Third party

According to Article 4(10) of GDPR: "a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data".

3.24. Video surveillance

Video-surveillance is the monitoring of a specific area, event, activity, or person by means of an electronic device or system for visual monitoring. Typically, the monitoring is carried out using CCTV systems. More about video surveillance here [3].

4. General recommendations

Below, we synthesize a list of the European Commission new rules for data protection, which will come in force from May 2018 [2]. Even though this guide concerns small and medium enterprises, most of its provisions should be taken into account when designing, implementing and deploying EmoSpaces.

4.1. What is personal data?

Name, address, localization, online identifier, health information, income, cultural profile, etc.

4.2. Fundamental rights of human beings

Amongst the comprehensive set of indivisible rights set out in international human rights law, the EU Treaties and the Charter, the following families of rights are particularly apt to cover the AI field [11]:

- *Respect for human dignity*: Human dignity encompasses the idea that every human being possesses an “intrinsic worth”, which can never be diminished, compromised or repressed by others – nor by new technologies like AI systems. In this context, respect for human dignity entails that all people are treated with respect due to them as individuals, rather than merely as data subjects. To specify the development or application of AI in line with human dignity, one can further articulate that AI systems are developed in a manner which serves and protects humans’ physical and moral integrity, personal and cultural sense of identity as well as the satisfaction of their essential needs.

- *Freedom of the individual*: This right refers to the idea that human beings should remain free to make life decisions for themselves. It does not only entail freedom from sovereign intrusion, but also requires intervention from government and non-governmental organizations to ensure that individuals or minorities benefit from equal opportunities. In this context, freedom of the individual requires protection from direct or indirect coercion, surveillance, deception or manipulation. In fact, freedom of the individual means a commitment to enable individuals to wield even higher control over their lives.

4.3. Critical concerned for ethical purpose

- ***Identification without Consent*** : A proportionate use of control techniques is needed to uphold the autonomy of consumers. Differentiating between the identification of an individual vs. the tracing and tracking of an individual will be crucial. In this regard, Article 6 of the General Data Protection Regulation (GDPR) can be recalled, which provides that processing of data shall only be lawful if it has a valid legal basis.

  As current mechanisms for giving informed consent in the internet show, consumers give consent without consideration. This involves an ethical obligation to develop entirely new and practical means by which consumers can give verified consent to being automatically identified by AI or equivalent technologies. Noteworthy examples of a scalable AI identification technology are face recognition or other involuntary methods of identification using biometric data (i.e. lie detection, personality assessment through micro expressions, automatic voice detection). Identification of individuals is sometimes the desirable outcome and aligned with ethical principles. Where the application of such technologies is not clearly warranted by existing law or the protection of core values, automatic identification raises strong concerns of both legal and ethical nature, with the default assumption being that consent to identification has not been given. This also applies to the usage of “anonymous” personal data that can be re-personalized.

- ***Covert AI systems, in the event that virtual assistants are used***: A human always has to know if she/he is interacting with a human being or a machine, and it is the responsibility of AI developers and deployers that this is reliably achieved. Otherwise, people with the power to control AI are potentially able to manipulate humans on an unprecedented scale. Developers and deployers should therefore ensure that humans are made aware of – or able to request and validate the fact that – they interact with an AI identity. Note that border-cases exist and complicate the matter – e.g. an AI-filtered voice spoken by a human. It should be born in mind that the confusion between humans and machines has multiple consequences such as attachment, influence, or reduction of the value of being human.

4.4. Principles for protecting the rights of people giving their data

1. Communication
    a. Use plain language
    b. Explain WHO are we, WHY do we process their data, for HOW LONG do we keep it and WHO receives it
    c. Provide, in a clear and proactive manner, information to stakeholders (customers, employees, etc.) about the system's capabilities and limitations, allowing them to set realistic expectations.
2. Consent: get clear consent to process the data. Be careful with age limits!
3. Access and portability: let people access their data and share it with other entities;
4. Profiling: inform for any form of automated processing of personal data, such as economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
5. Safeguard sensitive data: use extra safeguards for information on health, race, sexual orientation, religion or political beliefs;
6. Erase data: give people the "right to be forgotten", but do so without compromising the freedom of expression or the ability to research;
7. Warnings: inform people of data breaches, if there is serious risk to them;
8. Marketing: give people the right to opt out of direct marketing that uses their data;
9. Ensure participation and inclusion of stakeholders in the design and development of the EmoSpaces system: adults or children.
10. Data transfer outside the EU: make legal arrangements when you transfer data to countries that have not been approved by EU authorities;
11. Pay particular attention to situations involving more vulnerable groups: children, persons with disabilities or minorities.
12. Be mindful that there might be fundamental tensions between different objectives: transparency can open the door to misuse; identifying and correcting bias might contrast with privacy protections.

Under the same rules, the European Commission recommends taking into account impact assessments, for high-risk processing. EmoSpaces qualifies for two such high-risk cases, namely: i) new technologies and ii) automatic, systematic processing and evaluation of personal information.

5. Project ethical guidelines

5.1. Recommendations for informed consent and data policy

From an ethical perspective, we recommend that the EmoSpaces is developed around three principles. Though reduced, this set of principles is perfectly aligned with the general recommendations we discussed in the previous section:

1. **Informed consent**

   All users of the EmoSpaces platform should be clearly informed with respect to the purpose of the platform and its objectives. At the same time, users should be made fully aware of the data that is being collected, the data collection methodology, the technologies involved in the data collection process (see 2. below) and how the data is stored and disposed (see 3. below). We recommend that all these elements are included in a Privacy Statement and/or a Terms of Use type of document(s), as well as an Informed Consent sheet which will be developed together with or under the guidance of the ethical advisory board and will be discussed.

   Users will have full access to the services provided by the platform provided they agree to the provisions of these statements. Alternatively, limited access to different services could be provided if users would partially agree only with subsets of these provisions.

   At the same time, the international nature of the project and the possibility of deploying the platform in the several partner countries (at least), recommends that the development of the previous documents is done in several languages (English, French, Spanish, Korean), in order to facilitate users' understanding of their interaction with the platform.

2. **Harmless data collection**

   The system in which data is being collected (methodology and technology) should not, under any circumstances, attempt to the privacy or the dignity of EmoSpaces users or third parties who interact with EmoSpaces system. Potential personal data collection issues in the EmoSpaces project refers to the processing of medical data – in particular that of diabetic or elderly people –, video surveillance [3] and detection and processing of emotions.

3. **Data collection, data annotation and data storage**

   This point refers to the system in which the data is collected, processed and stored. EmoSpaces aims at building a unified infrastructure for building intelligent models able to characterize the context and detect the activity of the users. The multitude of sensor types that are involved in the project means that equally varied data types (a wide range of vital signs, video footage, sound recordings) are collected and processed in order to build the desired models. We need to strike a balance between the sensitivity level of the collected data, the technical characteristics of each of these sensors and the benefits that EmoSpaces users are getting in return. We will detail this in the following section. In the end, we should be able to have a better understanding on how to protect the privacy of EmoSpaces users, by implementing adapted privacy preservation mechanisms. Moreover, the data collection, annotation and storage efforts should be sensitive to the cultural and legal particularities of each of the countries where EmoSpaces will be deployed (France [1], Spain, Korea, to begin with).

4. **Ethics & Rule of law by design (X-by-design)**
   Methods to ensure values-by-design provide precise and explicit links between the abstract principles the system is required to adhere to and the specific implementation decisions, in ways that are accessible and justified by legal rules or societal norms. Central therein is the idea that compliance with law as well as with ethical values can be implemented, at least to a certain extent, into the design of the EmoSpaces system itself. Different "by-design" concepts are already widely used, two examples of which are Privacy-by-design or Security-by-design. To earn trust, EmoSpaces system needs to be secure with its processes, data and outcomes and be able to take adversarial data and attacks into account. In addition, it should implement a mechanism for fail-safe shutdown and resume operation after a forced shut-down (e.g. after an attack) [12].

5.2. Requirements for a trustworthy system

Achieving a trustworthy system means that the general and abstract principles need to be mapped into concrete requirements for applications [11]:

1. **Accountability**

Good governance should include accountability mechanisms, which could be very diverse in choice depending on the goals. Mechanisms can range from monetary compensation (with no-fault insurance) to fault finding or to reconciliation without monetary compensations. The choice of accountability mechanisms may also depend on the nature and weight of the activity, as well as the level of autonomy at play. An instance in which a system misreads an advise for EmoSpaces users and wrongly decides may be compensated for with money. In a case of discrimination, however, an explanation and apology might be at least as important.

Assessment List:

- Who is accountable if things go wrong?
- Are the skills and knowledge present in order to take on the responsibility?

- Can third parties or employees report potential vulnerabilities, risks or biases, and what processes are in place to handle these issues and reports? Do they have a single contact point to turn to?
- Is an (external) auditing of the AI system foreseen?

2. **Data Governance**

While specific uses of data must be taken in context of the regions where specific legislation applies, individuals should always be provided access to, and control of, their data to ensure their fundamental human rights are honored without fear of the risk of breaking applicable laws [15].

In addition, it must be ensured that the proper division of the data which is being set into training, as well as validation and testing of those sets, is carefully conducted in order to achieve a realistic picture of the performance of the system. It must particularly be ensured that anonymisation of the data is done in a way that enables the division of the data into sets to make sure that a certain data – for instance, images from same persons – do not end up into both the training and test sets, as this would disqualify the latter. The integrity of the data gathering has to be ensured. Feeding malicious data into the system may change the behaviour of the AI solutions. This is especially important for self-learning systems. It is therefore advisable to always keep record of the data that is fed to the AI systems. When data is gathered from human behaviour, it may contain misjudgement, errors and mistakes. In large enough data sets these will be diluted since correct actions usually overrun the errors, yet a trace of thereof remains in the data. To trust the data gathering process, it must be ensured that such data will not be used against the individuals who provided the data. Instead, the findings of bias should be used to look forward and lead to better processes and instructions and improving the decisions making for EmoSpaces users.

Assessment List:

- Is proper governance of data and process ensured? What process and procedures were followed to ensure proper data governance?
- Is an oversight mechanism put in place? Who is ultimately responsible?

3. **Design for all**

Systems should be designed in a way that allows all citizens to use the products or services, regardless of their age, disability status or social status. It is particularly important to consider accessibility to EmoSpaces products and services to people with disabilities, which are horizontal category of society, present in all societal groups independent from gender, age or nationality. The applications should hence not have a one-size-fits-all approach, but consider the whole range of human abilities, skills and requirements. Design for all implies the accessibility and usability of technologies by anyone at any place and at any time, ensuring their inclusion in any living context, thus enabling equitable access and active participation of potentially all people in existing and emerging computer-mediated human activities. This requirement links to the United Nations Convention on the Rights of Persons with Disabilities [17].

Assessment List:

- Is the system equitable in use?
- Does the system accommodate a wide range of individual preferences and abilities?
- Is the system usable by those with special needs or disabilities, and how was this designed into the system and how is it verified?
- What definition(s) of fairness is (are) applicable in the context of the system being developed and/or deployed?
- For each measure of fairness applicable, how is it measured and assured?

4. **Autonomy (Human oversight)**

The correct approach to assuring properties such as safety, accuracy, adaptability, privacy, explicability, compliance with the rule of law and ethical conformity heavily depends on specific details of the EmoSpaces system, its area of application, its level of impact on individuals and its level of autonomy. The level of autonomy results from the use case and the degree of sophistication needed for a task. All other things being equal, the greater degree of autonomy that is given to a system, the more extensive testing and stricter governance is required. It must be ensured that EmoSpaces system continue to behave as intended when feedback signals become sparser. Depending on the area of application and/or the level of impact on individuals, different levels or instances of governance (including human oversight) will be necessary. This is relevant for a large number of applications, and more particularly for the use of EmoSpaces system to suggest or take decisions concerning users (algorithmic decision support). Good governance of autonomy in this respect includes for instance more or earlier human intervention depending on the level of societal impact of the EmoSpaces system. This also includes the predicament that a user, particularly in a work or decision-making environment, is allowed to deviate from a path or decision chosen or recommended by EmoSpaces system. The intimacy of thoughts and emotions must be strictly protected from uses capable of causing harm, especially uses that impose moral judgments on people or their lifestyle choices [16].

Assessment List:

- Is a process foreseen to allow human control, if needed, in each stage?

- What measures are taken to audit and remedy issues related to governing AI autonomy?
- Within the organisation who is responsible for verifying that AI systems can and will be used in a manner in which they are properly governed and under the ultimate responsibility of human beings?

5. **Respect for (& Enhancement of) Human Autonomy**

Technological products and services, possibly through "extreme" personalisation approaches, may steer individual choice by potentially manipulative "nudging". At the same time, people are increasingly willing and expected to delegate decisions and actions to machines (e.g. recommender systems, virtual coaches and personal assistants). Systems that are tasked to help the user, must provide explicit support to the user to promote her/his own preferences, and set the limits for system intervention, ensuring that the overall wellbeing of the EmoSpaces user as explicitly defined by the user her/himself is central to system functionality.

Assessment List:

- Is the user informed in case of risks on human mental integrity (nudging) by the product?
- Is useful and necessary information provided to the user of the service/product to enable the latter to take a decision in full self-determination?
- Does the recommendation system indicate to users that a decision, content, advice, or outcome, is the result of an algorithmic decision of any kind?
- Do users have the facility to interrogate algorithmic decisions in order to fully understand their purpose, provenance, the data relied on, etc.?

6. **Respect for Privacy**

Privacy and data protection must be guaranteed at all stages of the life cycle of the EmoSpaces system. This includes all data provided by the user, but also all information generated about the user over the course of his or her interactions with the EmoSpaces system (e.g. advises generated for specific users, how users responded to particular recommendations, etc.). Digital records of human behaviour can reveal highly sensitive data, not only in terms of preferences, but also regarding sexual orientation, age, gender, religious and political views. The person in control of such information could use this to his/her advantage. We must be mindful of how data is used and might impact users, and ensure full compliance with the GDPR as well as other applicable regulation dealing with privacy and data protection.

Assessment List:

- If applicable, is the system GDPR compliant?
- Is the personal data information flow in the system under control and compliant with existing privacy protection laws?
- How can users seek information about valid consent and how can such consent be revoked?
- Is it clear, and is it clearly communicated, to whom or to what group issues related to privacy violation can be raised, especially when these are raised by users of, or others affected by, the AI system?

7. **Robustness**

Trustworthiness requires that algorithms are secure, reliable as well as robust enough to deal with errors or inconsistencies during the design, development, execution, deployment and use phase of EmoSpaces system, and to adequately cope with erroneous outcomes.

Reliability & Reproducibility. Trustworthiness requires that the accuracy of results can be confirmed and reproduced by independent evaluation. However, the complexity, non-determinism and opacity of many AI systems, together with sensitivity to training/model building conditions, can make it difficult to reproduce results. Reproducibility is essential to guarantee that results are consistent across different situations, computational frameworks and input data. The lack of reproducibility can lead to unintended discrimination in AI decisions.

Assessment List:

- Is a strategy in place to monitor and test that our products or services meet goals, purposes and intended applications?
- Are the used algorithms tested with regards to their reproducibility? Are reproducibility conditions under control? In which specific and sensitive contexts is it necessary to use a different approach?
- For each aspect of reliability and reproducibility that should be considered, how is it measured and assured?
- Are processes for the testing and verification of the reliability of AI systems clearly documented and operationalised to those tasked with developing and testing an AI system?
- What mechanisms can be used to assure users of the reliability of an AI system?

Accuracy. Accuracy pertains to an AI's confidence and ability to correctly classify information into the correct categories, or its ability to make correct predictions, recommendations, or decisions based on data or models. An explicit and well-formed development and evaluation process can support, mitigate and correct unintended risks.

Assessment List:

- What definition(s) of accuracy is (are) applicable in the context of the system being developed and/or deployed?
- For each form of accuracy to be considered how is it measured and assured?
- Is the data comprehensive enough to complete the task in hand? Is the most recent data used (not out-dated)?
- What other data sources / models can be added to increase accuracy?
- What other data sources / models can be used to eliminate bias?
- What strategy was put in place to measure inclusiveness of the data? Is the data representative enough of the case to be solved?

Resilience to Attack. AI systems, like all software systems, can include vulnerabilities that can allow them to be exploited by adversaries. Hacking is an important case of intentional harm, by which the system will purposefully follow a different course of action than its original purpose. If an AI system is attacked, the data as well as system behaviour can be changed, leading the system to make different decisions, or causing the system to shut down altogether. Systems and/or data can also become corrupted, by malicious intention or by exposure to unexpected situations.

Assessment List:

- What are the forms of attack to which the EmoSpaces system is vulnerable? Which of these forms of attack can be mitigated against?
- What systems are in place to ensure data security and integrity?

Fall back plan. A secure AI has safeguards that enable a fall-back plan in case of problems with the AI system. In some cases this can mean that the AI system switches from statistical to rule-based procedure, in other cases it means that the system asks for a human operator before continuing the action.

Assessment List:

- What would be the impact of the AI system failing by: Providing wrong results? Being unavailable? Providing societally unacceptable results (e.g. bias)?
- In case of unacceptable impact - Have thresholds and governance for the above scenarios been defined to trigger alternative/fall-back plans?
- Have fall-back plans been defined and tested?

8. **Safety**

Safety is about ensuring that the EmoSpaces system will indeed do what it is supposed to do, without harming users. It includes minimizing unintended consequences and errors in the operation of the system. Processes to clarify and assess potential risks associated with the use of our products and services should be put in place. Moreover, formal mechanisms are needed to measure and guide the adaptability of our systems.

Assessment List:

- What definition(s) of safety is (are) applicable in the context of the system being developed and/or deployed?
- For each form of safety to be considered how is it measured and assured?
- Have the potential safety risks of (other) foreseeable uses of the technology, including accidental or malicious misuse thereof, been identified?
- Is information provided in case of a risk for human physical integrity?
- Is a process in place to classify and assess potential risks associated with use of the product or service?
- Has a plan been established to mitigate and/or manage the identified risks?

9. **Transparency**

Transparency concerns the reduction of information asymmetry. Explainability – as a form of transparency – entails the capability to describe, inspect and reproduce the mechanisms through which AI systems make decisions and learn to adapt to their environments, as well as the provenance and dynamics of the data that is used and created by the system. Being explicit and open about choices and decisions concerning data sources, development processes, and stakeholders should be required from all models that use human data or affect human beings or can have other morally significant impact.

Assessment List:

Purpose:

- Is it clear who or what may benefit from the product/service?

- Have the usage scenarios for the product been specified and clearly communicated?
- Have the limitations of the product been specified to its users?
- Have criteria for deployment for the product been set and made available to the user?

Traceability:

- What measures are put in place to inform on the product's accuracy? On the reasons/criteria behind outcomes of the product?
- Is the nature of the product or technology, and the potential risks or perceived risks (e.g. around biases) thereof, communicated in a way that the intended EmoSpaces users, third parties and the general public can access and understand?
- Is a traceability mechanism in place to make our system auditable, particularly in critical situations?

6. Application ethical guidelines

The EmoSpaces main innovative aspect lies in considering emotion and sentiments as a context source for improving intelligent services in IoT. The aim of EmoSpaces is to go a step further and advance in IoT automation based on affective and persuasive technology. The major expected technical outcomes in EmoSpaces are:

1. Technologies for Multimedia Affect recognition based on Sensing and Smart Devices and eCoaching;
2. Big Data Platform for Semantic Sensor Fusion;
3. Context-aware adaptation and automation of IoT environment.

6.1. Common recommendations for services A1,A3,B,C

1- Wellbeing coaching

A3 - Depressive Disorder

B - Audio experience

C - E-learning

These services all share the feature of placing invasive technologies in private spaces, and as such share some recommendations. Placing cameras and/or microphones inside user's homes poses a number of significant issues, the first being the imperative requirement for airtight data protection. However, even in the case that the service functions optimally and that user data is unequivocally safeguarded, a number of non-trivial difficulties remain.

1. **Mental Health**

The mere presence of surveillance technologies inside a person's home is likely to provoke feelings of anxiety and paranoia, both in mentally sane users and users suffering from mental health disorders, for who the issue is particularly problematic. These users cannot be ignored and represent a significant portion of the population. The Diagnostic and Statistical Manual of Mental Disorders for instance estimates that between 0.5% - 2.5% of the population of the United States are suffering from paranoid personality disorder ([6], p 636), while anxiety disorders are widespread, with up to 33.7% of the population affected by an anxiety disorder during their lifetime [7]. It has also been shown that the target users of service A, people suffering from diabetes, are at a higher risk of anxiety disorders than the general population, see for example [8]. Target users for service A3, teenagers with depressive disorders, are also at a much greater risk of both anxiety and paranoid disorders (see DSM-IV; [9]). It should be noted that the fact that feelings of anxiety or paranoia may correspond to an imagined rather than real risk of privacy loss does not make these feelings less real or less problematic.

2. Public reception

Services using very intrusive technology such as cameras in the home also contain risks related to the image of the companies providing the service. Beyond possible legal issues, breaches or faults with such services may lead to dramatic media backlash and lasting nocuous effects on company image. Yet there may also be negative public reception even *in the absence of faults*. As an example, we point to some of the scepticism that characterised the reception of such devices as the Kinect, Amazon Alexa or Google Home.

Some examples:

- https://gizmodo.com/the-house-that-spied-on-me-1822429852
- http://fortune.com/2017/10/11/google-home-mini-data-privacy/
- "*Microsoft's original vision for the Xbox One involved Kinect in numerous ways users simply didn't care for. It also didn't help when Ad Age, a trade publication for the advertising industry, reported comments from a senior Microsoft executive boasting about the device's ability to gather user data and serve them targeted ads. Microsoft immediately walked back those comments and said the remarks had been taken out of context. At launch, some third-party Kinect mounting kits included plastic sleeves that would cover the sensor's camera, to defeat any presumed spying on users.*"
- https://www.polygon.com/2017/10/25/16543192/kinect-discontinued-microsoft-announcement
- The success of the Kinect 'privacy shield' demonstrates public mistrust in such devices. https://www.amazon.com/Privacy-Xbox-One-Protective-Concealing-Console/dp/B00HQMRTPO

Therefore, we recommand to conduct research about perception and understanding about EmoSpaces services, and the implementation of structured public consultation mechanisms to design policies and rules related to this. This may include the direct elicitation of public opinion via traditional research methods, such as opinion polls and focus groups, as well as more experimental approaches, such as providing simulated examples of the ethical dilemmas introduced by EmoSpaces system or experiments in social science labs, as is currently the case with Spain. This research agenda should not serve merely to measure public opinion, but should also lead to the creation of best practices as a result [18].

Furthermore, the respect of GDPR appears nowadays as an absolute necessity, as demonstrated by the recent case of Google and the penalty of €50 million for the lack of privacy. According to the CNIL, Google is still in breach of the law. CNIL explained that Google had violated two provisions of the law: first by not making its data-collection policies easily accessible enough and second by not obtaining sufficient and specific user consent for ad personalization across each of Google's numerous services, including YouTube, Google Maps, and more. The two complaints were filed jointly on the day the law went into effect by the French digital advocacy group La Quadrature du Net and the group Noyb.eu. Noyb, an English acronym for "None of your business," has also filed related complaints against Instagram, WhatsApp, and Facebook, which remain pending [14].

3. Conclusion

The above considerations lead us to the conclusion that placing RGB cameras, depth cameras or microphones inside user's homes has raised very sensitive and potentially problematic ethical and societal issues. We also urge each partner to err on the side of caution and to produce public privacy statements. "*Trust is something you earn in drops and lose in buckets*," says Kipman, the creator of Kinect.

6.2. EmoSpaces Service A – Wellbeing coaching

This service addresses three use case scenarios: lifestyle coaching for weight management, coaching by detection of abnormal behavior and coaching in critical situations. The core sensitive issue with Service A is that the primarily targeted users are elderly diabetic people. Moreover, the scenario is based on the capability of the EmoSpaces platform to build user profiles based on several surveillance and detection activities:

- Identification of **activities**, based on video footage;
- **Diet** detection based on the analysis of supermarket bills;
- Identification of **social engagement** based on video footage, sound recordings or text analysis (from emails, social media or instant messaging applications);
- Identification of **emotions** based on video footage, sound recordings or text analysis.

All these approaches and the subsequent processing of collected data raise several important ethical problems, which need to be dealt with either when implementing or deploying this service.

Please refer to Section 6.1.

1. **Target users**

Elderly persons suffering from diabetes.

2. **Sensitivity of Data**

The primary data used by this service are medical (healthcare) data. According to the new data protection rules recommended by the European Commission [3], these data are classified as personal and should be treated accordingly. We draw attention on the importance of the anonymisation of medical data as well as at the sensitive nature of its storage and circulation. We thoroughly recommend against the sharing of such data with any party outside the project (e.g., insurance companies, commercial and service suppliers) that might benefit economically from targeting EmoSpaces users. If, at any point, such an entity becomes associated to EmoSpaces our strong recommendation is to immediately inform our users of such a change and on the impact it will have on their interaction with the platform.

We need to be aware that if implemented, the diet detection module that scans shopping bills will have access to all data that can be found on a shopping bill (i.e., location, time, non-dietary shopping items). Collecting such data needs to take into account the sensitive nature of some of the information that we might come across and find a way to deal with it in a trustful manner.

3. **Access issues**

This is an extension of the previous point and is aimed at designating who has access to the personal data of an EmoSpaces user, for non-commercial reasons: family, legal guardians, friends, healthcare professionals (general practitioners, specialists, nurses)? This is a very delicate issue, which will need thorough discussions once we advance in the design phase and we move into the implementation. Based on the different scenarios and different roles of a concerned third party, we might decide to deal with this in different ways; for instance:

a. Opt-in: a third-party requires to have access to some or all data of the EmoSpaces user; the user grants full, partial or no access;
b. Opt-out: an EmoSpaces user gives full or partial access to their data to a third party; the third party chooses to accept be fully, partially or not involved.

4. **Cheating the system.**

This is a very interesting ethical topic, also because it deals with a different type of potential breach of trust. In order for the EmoSpaces platform to provide the best possible services to its users, we need to have a high degree of confidence in the user. This can be a delicate issue in the case of users suffering from different addictions and who might try to cheat the system (e.g., not logging all their meals or medication).

5. **Detection of email and other type of IM communication.**

While the benefits of such an approach are evident, it is difficult to believe that users would accept that the EmoSpaces platform has unlimited access to such data, especially the type of personal data that would be needed to create a social engagement profile. An alternative solution would be the integration of such services within the platform and restrict the data collection effort to the type of correspondence that concerns only the users interaction within EmoSpaces (e.g., with their doctor or therapist). In case such data would nevertheless be collected, this would have to be done according to the principles of informed consent and harmless collection stated in the previous section.

6. Privacy of third parties

Social engagement could alternatively be detected using video surveillance [3] or voice recognition. In this case the ethical issue is with respect to the privacy of the third parties involved in the social interaction that we are trying to detect. We therefore need to state, from onset, that the interaction with an EmoSpaces user can result in the recording of video footage or sound recording of the interacting third party. Both the EmoSpaces user and the third party should be made aware of this.

7. Infantilization

The sheer number of sensors as well as their omnipresence may also infantilize the users that the service intends to help and make more independent. The following case example given by the partner provides an illustration of this: "*Daisy is living alone and feeling depressed. The color scheme changes to more cheerful one, to cheer her up, and a computer or tablet suggests a game that Daisy likes to play a lot. Daisy's daughter looks from her own computer, how Daisy is doing today. She can see that no one has visited Daisy today and she is feeling a bit depressed. She decides to go for a visit*" (14012_EmoSpaces_FPP_Annex-V1 1-CR_V0.4). Such invasion into the user's life and the fact that their relatives might participate in it also carries the risk of adverse effects on family dynamics and relations.

8. Distinction between health benefits and convenience benefits

It is important that the developers clearly identify the specific aims of this service and benefits to the user. In particular, it should be specified from the onset whether the intended benefits are purely related to health or whether they expand further. The following case example suggests the latter: "*During evening hours, a more relaxed music could be played, lights and TV or PC screens dimmed, if the person seems too active to sleep*" (14012_EmoSpaces_FPP_Annex-V1 1-CR_V0.4). If the intended aims extend beyond health benefits, the specific benefits of such aims should be discussed.

Conclusion

Considering that the output for the user essentially consists in targeted and tailored advice for lifestyle management with little notion of urgency or immediate life threat, it seems the service presents a high level of invasivity. We note the exception of fall detection, which demonstrates the benefits of the service in a case of emergency.

6.3. EmoSpaces Service A2 – Autism Spectrum Disorder

1. **Target users**

Children with autism spectrum disorder (ASD), aged between 12 and 18 years old (to be confirmed).

2. **Interacting with children with ASD**

The main risk for this service stems from making children with ASD wear VR glasses. As such we recommend working with specialized clinicians in order to test this and ensure it is safe and appropriate. Age may also be a source of risk for very young users. We also recommend taking specific measures for interacting and conducting experiments with children with ASD (See for instance [10]). The partners have already taken appropriate steps in this direction by developing the service in partnership with the non-profit organization ASTRADE (an association for the care of people with Autism and Developmental Disorders of the Region of Murcia in Spain). This will give the partners access to existing structures and verified methods for working with the target users.

3. **Conclusion**

The partners have already taken appropriate steps in this direction by developing the service in partnership with the non-profit organization ASTRADE (an association for the care of people with Autism and Developmental Disorders of the Region of Murcia in Spain). This will give the partners access to existing structures and verified methods for working with the target users.

6.4. EmoSpaces Service A3 - Depressive Disorder

Please refer to Section 6.1.

1. **Target users**

Teenagers with depressive disorder, or showing early signs of depression, aged between 10 and 18 years old.

2. **Sensitivity of Data**

The primary data used by this service are medical data. According to the new data protection rules recommended by the European Commission [3], these data are classified as personal and should be treated accordingly. We draw attention on the importance of the anonymisation of medical data as well as at the sensitive nature of its storage and circulation. We thoroughly recommend against the sharing of such data with any party outside the project (e.g., insurance companies, commercial and service suppliers) that might benefit economically from targeting EmoSpaces users. If, at any point, such an entity becomes associated to EmoSpaces our strong recommendation is to immediately inform our users of such a change and on the impact it will have on their interaction with the platform.

3. **Consent**

There are two main aspects of the service that require consent: (a) consenting to engaging with the service; (b) deciding how information about the user is shared.

(a) In terms of engaging with the service, the user (teenager) does not have a say: doctors and parents decide for them that they must engage with the technology. As such the user cannot refuse to be monitored. This poses the urgent question of determining at what point a user is sufficiently at risk to justify overriding their consent on such an invasive technology. It seems the answer to this should come from both a medical and legal independent consultation.

(b) The user has a right of say on how information about them (and their mental health) can be shared with third parties, in particular family and friends. What is important here is to ensure that they may do so in a free and well informed way. It would also be helpful to clarify what exactly this information will be.

4. **Efficiency**

What this service suggests is that the multi-sensor monitoring of teenagers with depressive disorder will help identifying moments when the risk of suicide becomes critical, and therefore help prevent suicides. Input from clinicians specialized in this kind of patient seems necessary to establish whether this is indeed likely to be true.

5. **Conclusion**

It appears this service presents a high level of invasivity. We advise in favor of systematic and rigorous consultation with specialized clinicians. Placing cameras behind mirrors inside user's homes raises very sensitive and potentially problematic ethical issues.

6.5. EmoSpaces Service B – Sound Optimization

Please refer to Section 6.1.

1. **Target users**

Customers

2. **Identification and profiling**

This service addresses two use case scenarios – context aware sound optimization on home and wearable devices, respectively. The aim of this service is to provide an optimized sound experience, based on users' location and emotional context. Ethical issues arise concerning the location, identification and profiling tasks as these require parsing sensitive personal data about the user.

3. **Conclusion**

Because the service makes use of invasive technologies for the purpose of enhancing comfort, it appears this service presents a high level of invasivity.

6.6. EmoSpaces Service C - E-Learning

Please refer to Section 6.1.

1. **Target users**

Students with learning difficulties, or cognitive issues. Company staff.

2. **Impact on teaching**

The possibility for a teacher to monitor their students in a remote yet invasive way poses a number of problems. First, this may result in unhealthy or nefarious effects on the student/teacher relationship by conferring unreasonable power to the latter over the former. Conferring these new powers to teachers should therefore result from a wider consultation with students and teachers alike. Second, the information provided by the service may inadvertently lead to discrimination. For example, a student may be penalized for not appearing to engage with a task while nevertheless succeeding in it. Students who are slower learners may also suffer from the existence and dissemination of these types of metrics with their teachers.

It is also unclear whether the new types of information provided by the service will truly improve student and teacher satisfaction and leaning. This should be investigated with the help of professionals from the education community.

3. **Conclusion**

It appears the invasivity of the service outpowers its benefits. Using video footage from user's personal laptop camera raises very sensitive and potentially problematic ethical issues. We recommend systematic and rigorous consultation with students and education professionals.

6.7. EmoSpaces service D - E-Retail

1. **Target users**

Customers

4. **Conclusion**

It appears this service presents a high level of invasivity. The fact that cameras in this service are to be placed in public spaces means that the service is less problematic from an ethical perspective. As such we make no specific recommendations beyond the general recommendations discussed in section 4.

6.8. Summary of service invasivity/urgency balance

This table summarises the appraisal of the services from the point of view of invasivity/urgency balance. It is to be updated as the services and case uses are developed.

Service	Invasivity	Urgency	Balance
A1 - Wellbeing coaching	Critical	Intermediate	Unbalanced
A2 - Autism Spectrum Disorder	Low	Low	Adequate
A3 - Depressive Disorder	Critical	High	Unbalanced
B - Audio Experience	Critical	Null	Unbalanced
C - E-Learning	Critical	Low	Unbalanced
D - E-Retail	Low	Null	Adequate

6.9. Steps taken by the EmoSpace project to address ethical and societal issues.

To address these issues discussed here, the EmoSpaces user interface will present a control panel of services to ensure a user centric approach. The panel will provide a description of services together with a detailed view of the data needed to deploy them, and consent issues. This control board will also allow the EmoSpaces user or his legal representative to modify at any time the consent on data exploitation together with the service typology. This user centric approach will allow the end-user to set up the data level access to his personal data in function on the experimented benefit.

7. Synthesis and roadmap

1. Do data protection by design!
2. Privacy Statement and/or Terms of Use
   a. Development in all languages where the project will be deployed.
   b. Adaptation to the cultural and legal requirements of each of the countries where the project will be deployed (France, Spain, Korea).
   c. Adaptation to all the diversity of customers.
3. Overview of all the sensors (characteristics, required data, data collection method, data processing)
   a. Have a clear idea of the infrastructure required to store and process the collected data.
   b. Subsequently, understand the limitations and propose solutions with respect to user data privacy.
   c. Develops a robust and safe security system.
4. Define the experimental protocols with respect to both the general principles of experimentation ethics, as well as the ethical challenges identified in this document. Ensure

participation and inclusion of stakeholders in the design and development of the EmoSpaces system.

5. Pay close attention to the conformity of our projects with the GDPR. Communicate with consumers exactly what will be done with their data. We must be as exhaustive as possible.

8. Appendix – Relevant recitals and articles of the General Data Protection Regulation (GDPR)

We selected the following retails and articles based on their relevance to EmoSpaces projects. We invite you to pay attention to the following, even with a quick overview, specially to Article 39 about the missions of the Data Protection Officer. We recommend to contact a DPO of Thales to inform him or her about our projects. We also invite you to pay attention to Article 83 about the risks that we incur if we don't comply with the GDPR. We will probably have to contact the CNIL to make sure that our services are not in contradiction with the GDPR. It will be done by the DPO.

8.1. Recitals

- [15] **Filling system**: In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation.

- [32] **Consent**: Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided

- [35] **Personal data concerning health**: Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council (1) to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

- [36] **Main establishment**: The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment. The main establishment of a controller in the Union should be determined according to objective criteria and should imply the effective and real exercise of management activities determining the main decisions as to the purposes and means of processing through stable arrangements. That criterion should not depend on whether the processing of personal data is carried out at that location. The presence and use of technical means and technologies for processing personal data or processing activities do not, in themselves, constitute a main establishment and are therefore not determining criteria for a main establishment. The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority should remain the supervisory authority of the Member State where the controller has its main establishment, but the supervisory authority of the processor should be considered to be a supervisory authority concerned and that supervisory authority should participate in the cooperation procedure provided for by this Regulation. In any case, the supervisory authorities of the Member State or Member States where the processor has one or more establishments should not be considered to be supervisory authorities concerned where the draft decision concerns only the controller. Where the processing is carried out by a group of undertakings, the main establishment of the controlling undertaking should be considered to be the main establishment of the group of undertakings, except where the purposes and means of processing are determined by another undertaking.

- [38] **Specific protection for children**: Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child. The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

- [39] **Transparency and data storage**: Any processing of personal data should be lawful and fair. It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed. Natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing. In particular, the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data. The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means. In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review. Every reasonable step should be taken to ensure that personal data which are inaccurate are rectified or deleted. Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

- [40] **Obligation of the data subject's consent**: In order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law, either in this Regulation or in other Union or Member State law as referred to in this Regulation, including the necessity for compliance with the legal obligation to which the controller is subject or the necessity for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

- [42] **Proof of consent**: Where processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject has given consent to the processing operation. In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC (1) a declaration of consent preformulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms. For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

- [51] **Prohibition of the collection of images, and possible derogation**: Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term ‘racial origin’ in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

- [52] **Derogations in the collection of personal data**: Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

- [53] **Clarification on derogations concerning health data**: Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

- [54] **Authorization to collect health data for public health purposes**: The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council (1), namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

- [58] **Clarification on the principle of transparency**: The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

- [59] **Person's access to his or her personal data**: Modalities should be provided for facilitating the exercise of the data subject's rights under this Regulation, including mechanisms to request and, if applicable, obtain, free of charge, in particular, access to and rectification or erasure of personal data and the exercise of the right to object. The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. The controller should be obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests.

- [60] **Possibility for the person to know, in accordance with the principle of fair and transparent processing, the existence of the processing operation and its purposes**: The principles of fair and transparent processing require that the data subject be informed of the existence of the processing operation and its purposes. The controller should provide the data subject with any further information necessary to ensure fair and transparent processing taking into account the specific circumstances and context in which the personal data are processed. Furthermore, the data subject should be informed of the existence of profiling and the consequences of such profiling. Where the personal data are collected from the data subject, the data subject should also be informed whether he or she is obliged to provide the personal data and of the consequences, where he or she does not provide such data. That information may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner, a meaningful overview of the intended processing. Where the icons are presented electronically, they should be machine-readable.

- [61] **Person must be informed promptly when his or her personal data are processed**: The information in relation to the processing of personal data relating to the data subject should be given to him or her at the time of collection from the data subject, or, where the personal data are obtained from another source, within a reasonable period, depending on the circumstances of the case. Where personal data can be legitimately disclosed to another recipient, the data subject should be informed when the personal data are first disclosed to the recipient. Where the controller intends to process the personal data for a purpose other than that for which they were collected, the controller should provide the data subject prior to that further processing with information on that other purpose and other necessary information. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.

- [62] **Details on data processing**: However, it is not necessary to impose the obligation to provide information where the data subject already possesses the information, where the recording or disclosure of the personal data is expressly laid down by law or where the provision of information to the data subject proves to be impossible or would involve a disproportionate effort. The latter could in particular be the case where processing is carried out for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. In that regard, the number of data subjects, the age of the data and any appropriate safeguards adopted should be taken into consideration.

- [63] **Person's access to his or her personal data, in particular medical data**: A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing.

  Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

- [64] **Verification of the person requesting the personal data information**: The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

- [65] **Modification of personal data and the right to be forgotten**: A data subject should have the right to have personal data concerning him or her rectified and a 'right to be forgotten' where the retention of such data infringes this Regulation or Union or Member State law to which the controller is subject. In particular, a data subject should have the right to have his or her personal data erased and no longer processed where the personal data are no longer necessary in relation to the purposes for which they are collected or otherwise processed, where a data subject has withdrawn his or her consent or objects to the processing of personal data concerning him or her, or where the processing of his or her personal data does not otherwise comply with this Regulation. That right is relevant in particular where the data subject has given his or her consent as a child and is not fully aware of the risks involved by the processing, and later wants to remove such personal data, especially on the internet. The data subject should be able to exercise that right notwithstanding the fact that he or she is no longer a child. However, the further retention of the personal data should be lawful where it is necessary, for exercising the right of freedom of expression and information, for compliance with a legal obligation, for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims.

- [68] **Portability of personal data**: To further strengthen the control over his or her own data, where the processing of personal data is carried out by automated means, the data subject should also be allowed to receive personal data concerning him or her which he or she has provided to a controller in a structured, commonly used, machine-readable and interoperable format, and to transmit it to another controller. Data controllers should be encouraged to develop interoperable formats that enable data portability. That right should apply where the data subject provided the personal data on the basis of his or her consent or the processing is necessary for the performance of a contract. It should not apply where processing is based on a legal ground other than consent or contract. By its very nature, that right should not be exercised against controllers processing personal data in the exercise of their public duties. It should therefore not apply where the processing of the personal data is necessary for compliance with a legal obligation to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of an official authority vested in the controller.

  The data subject's right to transmit or receive personal data concerning him or her should not create an obligation for the controllers to adopt or maintain processing systems which are technically compatible. Where, in a certain set of personal data, more than one data subject is concerned, the right to receive the personal data should be without prejudice to the rights and freedoms of other data subjects in accordance with this Regulation. Furthermore, that right should not prejudice the right of the data subject to obtain the erasure of personal data and the limitations of that right as set out in this Regulation and should, in particular, not imply the erasure of personal data concerning the data subject which have been provided by him or her for the performance of a contract to the extent that and for as long as the personal data are necessary for the performance of that contract. Where technically feasible, the data subject should have the right to have the personal data transmitted directly from one controller to another.

- [70] **Profiling for prospecting purposes**: Where personal data are processed for the purposes of direct marketing, the data subject should have the right to object to such processing, including profiling to the extent that it is related to such direct marketing, whether with regard to initial or further processing, at any time and free of charge. That right should be explicitly brought to the attention of the data subject and presented clearly and separately from any other information.

- [71] **Possibility to refuse automated processing**: The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.

- [74] **Obligation of the data controller to report, on compliance with the GDPR**: The responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should be obliged to implement appropriate and effective measures and be able to demonstrate the compliance of processing activities with this Regulation, including the effectiveness of the measures. Those measures should take into account the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons.

- [75] **Risks associate with processing of personal data**: The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.

- [76] <u>**Need to objectively measure the risks associated with the processing of personal data**</u>: The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the nature, scope, context and purposes of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk.

- [77] <u>**Risk assessment by a committee or a DPO**</u>: Guidance on the implementation of appropriate measures and on the demonstration of compliance by the controller or the processor, especially as regards the identification of the risk related to the processing, their assessment in terms of origin, nature, likelihood and severity, and the identification of best practices to mitigate the risk, could be provided in particular by means of approved codes of conduct, approved certifications, guidelines provided by the Board or indications provided by a data protection officer. The Board may also issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.

- [78] <u>**Taking of appropriate technical and organisational measures by the controller to ensure that the rules of the GDPR are respected, in particular by adopting internal rules, and by applying data protection by design and by default**</u>: The protection of the rights and freedoms of natural persons with regard to the processing of personal data require that appropriate technical and organisational measures be taken to ensure that the requirements of this Regulation are met. In order to be able to demonstrate compliance with this Regulation, the controller should adopt internal policies and implement measures which meet in particular the principles of data protection by design and data protection by default. Such measures could consist, inter alia, of minimising the processing of personal data, pseudonymising personal data as soon as possible, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.

- [80] <u>**Need to appoint a representative and to respect the GDPR when personal data are transmitted outside the EU**</u>: Where a controller or a processor not established in the Union is processing personal data of data subjects who are in the Union whose processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union, or to the monitoring of their behaviour as far as their behaviour takes place within the Union, the controller or the processor should designate a representative, unless the processing is occasional, does not include processing, on a large scale, of special categories of personal data or the processing of personal data relating to criminal convictions and offences, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing or if the controller is a public authority or body. The representative should act on behalf of the controller or the processor and may be addressed by any supervisory authority. The representative should be explicitly designated by a written mandate of the controller or of the processor to act on its behalf with regard to its obligations under this Regulation. The designation of such a representative does not affect the responsibility or liability of the controller or of the processor under this Regulation. Such a representative should perform its tasks according to the mandate received from the controller or processor, including cooperating with the competent supervisory authorities with regard to any action taken to ensure compliance with this Regulation. The designated representative should be subject to enforcement proceedings in the event of non-compliance by the controller or processor.

- [81] **Need for processors to provide sufficient guarantees to comply with the GDPR**: To ensure compliance with the requirements of this Regulation in respect of the processing to be carried out by the processor on behalf of the controller, when entrusting a processor with processing activities, the controller should use only processors providing sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures which will meet the requirements of this Regulation, including for the security of processing. The adherence of the processor to an approved code of conduct or an approved certification mechanism may be used as an element to demonstrate compliance with the obligations of the controller. The carrying-out of processing by a processor should be governed by a contract or other legal act under Union or Member State law, binding the processor to the controller, setting out the subject- matter and duration of the processing, the nature and purposes of the processing, the type of personal data and categories of data subjects, taking into account the specific tasks and responsibilities of the processor in the context of the processing to be carried out and the risk to the rights and freedoms of the data subject. The controller and processor may choose to use an individual contract or standard contractual clauses which are adopted either directly by the Commission or by a supervisory authority in accordance with the consistency mechanism and then adopted by the Commission. After the completion of the processing on behalf of the controller, the processor should, at the choice of the controller, return or delete the personal data, unless there is a requirement to store the personal data under Union or Member State law to which the processor is subject.

- [82] **Keeping of records on the liability for the controller and processor, to be in contact with the supervisory authority**: In order to demonstrate compliance with this Regulation, the controller or processor should maintain records of processing activities under its responsibility. Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations.

- [83] **<u>Importance of data security and measures taken to ensure it, such as encryption</u>**: In order to maintain security and to prevent processing in infringement of this Regulation, the controller or processor should evaluate the risks inherent in the processing and implement measures to mitigate those risks, such as encryption. Those measures should ensure an appropriate level of security, including confidentiality, taking into account the state of the art and the costs of implementation in relation to the risks and the nature of the personal data to be protected. In assessing data security risk, consideration should be given to the risks that are presented by personal data processing, such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

- [84] **<u>Impact assessment of risks related to the processing of data initiated by the controller and its consequences</u>**: In order to enhance compliance with this Regulation where processing operations are likely to result in a high risk to the rights and freedoms of natural persons, the controller should be responsible for the carrying-out of a data protection impact assessment to evaluate, in particular, the origin, nature, particularity and severity of that risk. The outcome of the assessment should be taken into account when determining the appropriate measures to be taken in order to demonstrate that the processing of personal data complies with this Regulation. Where a data-protection impact assessment indicates that processing operations involve a high risk which the controller cannot mitigate by appropriate measures in terms of available technology and costs of implementation, a consultation of the supervisory authority should take place prior to the processing.

- [85] **<u>Consequences of personal data breach and on notification by the controller</u>**: A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

- [86] **Measures taken by the data controller in the event of a data breach**: The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

- [87] **Measures taken to prevent or limit the violation of personal data**: It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

- [88] **Circumstances and constraints need to be taken into account when establishing rules of procedure for notification in the event of a data breach**: In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.

- [90] **Notification in case of a data breach by the controller:** In such cases, a data protection impact assessment should be carried out by the controller prior to the processing in order to assess the particular likelihood and severity of the high risk, taking into account the nature, scope, context and purposes of the processing and the sources of the risk. That impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation.

- [94] **<u>Consultation of the competent supervisory authority in cases where the impact assessment has revealed high risks for the rights and freedoms of natural persons</u>**: Where a data protection impact assessment indicates that the processing would, in the absence of safeguards, security measures and mechanisms to mitigate the risk, result in a high risk to the rights and freedoms of natural persons and the controller is of the opinion that the risk cannot be mitigated by reasonable means in terms of available technologies and costs of implementation, the supervisory authority should be consulted prior to the start of processing activities. Such high risk is likely to result from certain types of processing and the extent and frequency of processing, which may result also in a realisation of damage or interference with the rights and freedoms of the natural person. The supervisory authority should respond to the request for consultation within a specified period. However, the absence of a reaction of the supervisory authority within that period should be without prejudice to any intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation, including the power to prohibit processing operations. As part of that consultation process, the outcome of a data protection impact assessment carried out with regard to the processing at issue may be submitted to the supervisory authority, in particular the measures envisaged to mitigate the risk to the rights and freedoms of natural persons.

- [95] **<u>Processor's contribution to data security</u>**: The processor should assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the carrying out of data protection impact assessments and from prior consultation of the supervisory authority.

- [97] **<u>Characteristics of the DPO</u>**: Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. In the private sector, the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

- [101] **Data transfer outside the EU**: Flows of personal data to and from countries outside the Union and international organisations are necessary for the expansion of international trade and international cooperation. The increase in such flows has raised new challenges and concerns with regard to the protection of personal data. However, when personal data are transferred from the Union to controllers, processors or other recipients in third countries or to international organisations, the level of protection of natural persons ensured in the Union by this Regulation should not be undermined, including in cases of onward transfers of personal data from the third country or international organisation to controllers, processors in the same or another third country or international organisation. In any event, transfers to third countries and international organisations may only be carried out in full compliance with this Regulation. A transfer could take place only if, subject to the other provisions of this Regulation, the conditions laid down in the provisions of this Regulation relating to the transfer of personal data to third countries or international organisations are complied with by the controller or processor.

- [108] **Appropriate safeguards for data subject in a third country**: In the absence of an adequacy decision, the controller or processor should take measures to compensate for the lack of data protection in a third country by way of appropriate safeguards for the data subject. Such appropriate safeguards may consist of making use of binding corporate rules, standard data protection clauses adopted by the Commission, standard data protection clauses adopted by a supervisory authority or contractual clauses authorised by a supervisory authority. Those safeguards should ensure compliance with data protection requirements and the rights of the data subjects appropriate to processing within the Union, including the availability of enforceable data subject rights and of effective legal remedies, including to obtain effective administrative or judicial redress and to claim compensation, in the Union or in a third country. They should relate in particular to compliance with the general principles relating to personal data processing, the principles of data protection by design and by default. Transfers may also be carried out by public authorities or bodies with public authorities or bodies in third countries or with international organisations with corresponding duties or functions, including on the basis of provisions to be inserted into administrative arrangements, such as a memorandum of understanding, providing for enforceable and effective rights for data subjects. Authorisation by the competent supervisory authority should be obtained when the safeguards are provided for in administrative arrangements that are not legally binding.

8.2. Articles

- [5] **Principles relating to processing of personal data**:

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisationa measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (‘storage limitation’);

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and agains accidental loss, destruction or damage, using appropriate technical or organisational measures (‘integrity and confidentiality’).

2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘accountability’).

- [6] **Lawfulness of processing**:

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

- [7] <u>**Conditions for consent**</u>:

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract. »

- [8] **Conditions applicable to child's consent in relation to information society services:**

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child. Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.

- [10] **Processing of special categories of personal data**:

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, ortrade union membership, and the processing of genetic data,

biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons whohave regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

- [11] **<u>Processing which does not require identification</u>**:

  1. If the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation.

  2. Where, in cases referred to in paragraph 1 of this Article, the controller is able to demonstrate that it is not in a position to identify the data subject, the controller shall inform the data subject accordingly, if possible. In such cases, Articles 15 to 20 shall not apply except where the data subject, for the purpose of exercising his or her rights under those articles, provides additional information enabling his or her identification. »

- [19] **Notification obligation regarding rectification or erasure of personal data or restriction of processing**:

  The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.

- [21] **Right to object:**

  2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

  3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

- [32] **Security of processing**:

  1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

  (a) the pseudonymisation and encryption of personal data;

  (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

  (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

  (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

3. Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

4. The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

- [33] **Notification of a personal data breach to the supervisory authority**:

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

3. The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

- [34] **Communication of a personal data breach to the data subject**:

  3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

  (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

  (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

  (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

- [35] **Data protection impact assessment**:

  1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

  2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

  3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

  (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

  (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or services to data subjects or to the monitoring of their behaviour in several Member States, or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

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

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

- [36] **Prior consultation**:

1. The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

2. Where the supervisory authority is of the opinion that the intended processing referred to in paragraph 1 would infringe this Regulation, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers referred to in Article 58. That period may be extended by six weeks, taking into account the complexity of the intended processing. The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay. Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

3. When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:

(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

(b) the purposes and means of the intended processing;

(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;

(d) where applicable, the contact details of the data protection officer;

- [37] **Designation of the data protection officer**

1. The controller and the processor shall designate a data protection officer in any case where:

    (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

    (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

    (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

- [38] **Position of the data protection officer:**

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

- [39] **<u>Tasks of the data protection officer:</u>**

1. The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involve in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

- [83] **General conditions for imposing administrative fines**:

  1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.

  2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

  (a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them ;

  (b) the intentional or negligent character of the infringement;

  (c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;

  (d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

  (e) any relevant previous infringements by the controller or processor;

  (f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;

  (g) the categories of personal data affected by the infringement;

  (h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;

  (i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;

(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and

(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.

4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;

(b) the obligations of the certification body pursuant to Articles 42 and 43;

(c) the obligations of the monitoring body pursuant to Article 41(4).

5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:

(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;

(b) the data subjects' rights pursuant to Articles 12 to 22;

(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;

(d) any obligations pursuant to Member State law adopted under Chapter IX;

(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).

6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.

8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.

9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive. Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

9. References

[1] CNIL, *Guide droit d'accès – Ed. 2016*. Accessed May 31, 2017. https://www.cnil.fr/sites/default/files/atoms/files/cnil_droit_d_acces.pdf_0_0.pdf

[2] European Commission, *Data protection: Better rules for small businesses*. Accessed May 31, 2017. http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_en.htm

[3] European Data Protection Supervisor, *Consultation on the EDPS video-surveillance guidelines*. Accessed May 31, 2017. https://edps.europa.eu/data-protection/our-work/publications/guidelines/consultation-edps-video-surveillance-guidelines_en

[4] European Data Protection Supervisor, *Ethics*. Accessed May 31, 2017. https://edps.europa.eu/data-protection/our-work/ethics_en

[5] European Data Protection Supervisor, *Glossary*. Accessed May 31, 2017. https://edps.europa.eu/data-protection/data-protection/glossary_en

[6] American Psychiatric Association, & American Psychiatric Association. (2000). DSM-IV-TR: Diagnostic and statistical manual of mental disorders, text revision. Washington, DC: American Psychiatric Association, 75, 78-85.

[7] Bandelow, B., & Michaelis, S. (2015). Epidemiology of anxiety disorders in the 21st century. Dialogues in clinical neuroscience, 17(3), 327.

[8] Kruse, J., Schmitz, N., & Thefeld, W. (2003). On the association between diabetes and mental disorders in a community sample: results from the German National Health Interview and Examination Survey. Diabetes care, 26(6), 1841-1846.

[9] Salokangas, R. K. R., Hietala, J., Heinimaa, M., From, T., von Reventlow, H. G., Linszen, D., ... & Klosterkötter, J. (2015). Causal Connection Between Depression and Paranoia. European Psychiatry, 30, 113.

[10] Kylliäinen, Anneli, et al. "Practical guidelines for studying young children with autism spectrum disorder in psychophysiological experiments." Review Journal of Autism and Developmental Disorders 1.4 (2014): 373-386. https://link.springer.com/article/10.1007/s40489-014-0034-5

[11] The European Commission's – High-level Expert Group on Artificial Intelligence (2018). *Draft Ethics Guidelines for Trustworthy AI*. Accessed January 28, 2019. https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_draft_ethics_guidelines_18_december.pdf

[12] Journal du Net, RGPR: signification, rôle du DPO. Accessed January 25, 2019. https://www.journaldunet.com/economie/services/1208625-rgpd-google-ecope-d-une-amende-de-50-millions-d-euros/

[13] Official Journal of the European Union, General Data Protection Regulation (GDPR). Accessed January 23, 2019. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=FR

[14] Ars Technica, Google must pay €50 million for GDPR violations, France says. Accessed February 7, 2019. https://arstechnica.com/tech-policy/2019/01/google-fined-57m-after-france-finds-violations-of-new-eu-privacy-law/

[15] IEEE Standards Association, The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. Accessed January 25, 2019. https://standards.ieee.org/industry-connections/ec/auto-sys-form.html

[16] Montreal Declaration for a responsible development of artificial intelligence. Accessed January 24, 2019. https://www.montrealdeclaration-responsibleai.com/the-declaration

[17] United Nations – Disability, Department of Economic and Social affairs. Convention on the Rights of Persons with Disabilities (CRPD). https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html

[18] Atomium European Institue For Science, Media and Democracy. AI4Peoples's Ethical Framework for a Good AI Society. Accessed Feburary 4, 2019. http://www.eismd.eu/ai4people/