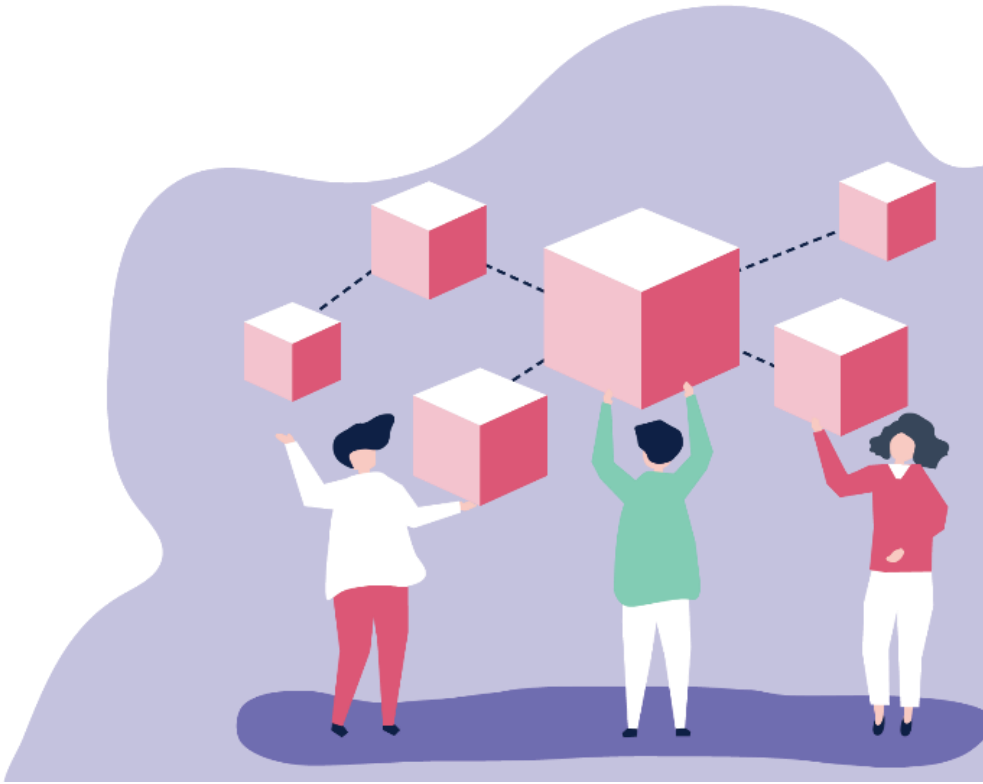
This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement N° 857223

D1.10 Legal, Ethics and Privacy Protection (LEPP) Management

Deliverable No.	D1.10	**Due Date**	30/09/2021
Description	This deliverable is the second version of D1.5. It provides an annual evaluation and assessment of the pilots and includes a compilation of reported ethical risks by all project partners.		
Type	Report	**Dissemination Level**	PU
Work Package No.	WP1	**Work Package Title**	Project coordination, IPR and Ethics management
Version	1.0	**Status**	Final



Authors

Name and surname	Partner name	e-mail
Pasquale Annicchino	UDGA	pannicchino@archimede.ch
Adrián Quesada Rodriguez	MI	aquesada@mandint.org
Stea-Maria Miteva	UDGA	smiteva@udgalliance.org
Vasiliki Tsiompanidou	MI	Vtsiompanidou@mandint.org
Renáta Radócz	MI	rradocz@mandint.org
Sébastien Ziegler	MI	sziegler@mandint.org
Ana Maria Pacheco Huamani	UDGA	admin@udgalliance.org
Kostantinos Votis	CERTH	kostakis@gmail.com
Ioanna Drympeta	CERTH	idrympeta@iti.gr
Franco Mercalli	MME	f.mercalli@multimedengineers.com
Sergio Copelli	MME	s.copelli@multimedengineers.com
Karolina Mackiewicz	ECHA	karolina@echalliance.com
Alessio Antonini	OU	alessio.antonini@open.ac.uk
Daniel Rodriguez	Sense4Care	daniel.rodriguez@sense4care.com
Alejandro Medrano	UPM	amedrano@lst.tfo.upm.es
Eugenio Gaeta	UPM	eugenio.gaeta@lst.tfo.upm.es
Giuseppe Fico	UPM	gfico@lst.tfo.upm.es
Francesco Giuliani	CSS	f.giuliani@operapadrepio.it
Ana Moya	TECNALIA	ana.moya@tecnalia.com
Leire Bastida	TECNALIA	Leire.Bastida@tecnalia.com
Eunate Arana	OSA	eunate.aranaarri@osakidetza.eus
Jon Eneko Idoyaga	OSA	JONENEKO.IDOYAGAURIBARRENA@osakidetza.eus
Leticia Gomez Nubla	OSA	LETICIA.GOMEZNUBLA@osakidetza.eus
Jordi de Batlle	CIBER	jdebatlle@irblleida.cat

History

Date	Version	Change
20/01/2021	0.1	Initial revision of the document based on D1.5
17/02/2021	0.1	Revision of the table of content
7/03/2021	0.2	Work on the privacy checklist for the pilots
26/03/2021	0.3	Additional inputs paragraphs
01/05/2021	0.5	Document tailoring, request for inputs (Ethical assessment form) shared with all project partners
15/03/2022	0.6	Updates from Pilots integrated. Final deadline for ethical assessment form updates from all partners
24/03/2022	0.7	Final draft completed and submitted for peer review
31/05/2022	0.8	Addressing peer review comments
02/08/2022	0.9	Alignment with inputs from other deliverables
10/08/2022	1.0	Final version ready for submission

Key data

Keywords	Data protection; Ethics;
Lead Editor	Pasquale Annicchino (UDGA) Ana Maria Pacheco (UDGA) Stea-Maria Miteva (UDGA) Adrian Quesada Rodriguez (MI) Vasiliki Tsiompanidou (MI)
Internal Reviewer(s)	Frans Folkvord (OE) Eleni Georga (UoI) Giuseppe Fico (UPM)

Abstract

The deliverable presents an iterative review of it first version (D1.5). It provides a short assessment and a LEPP management manual with a focus on the legal and ethical ecosystem of the project. This version of the deliverable also provides an updated ethical

assessment of the pilots (based on a template distributed to all the partners as planned in D1.5).

Statement of originality

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

Table of contents

List of tables

List of figures

1 Executive Summary

This document presents the second iteration of D1.5 (July 2020) which seeks to provide a legal, ethical and privacy protection management baseline assessment of the project. Its contents are based on risk assessments on the project's pilots, as well as on the consortium members' organisations. To this end, it leverages on the identified fundamental principles that guide the project. The document supplements the initially provided data protection and ethical assessments in D1.5, provides updated checklists, showcases the main discussions held in the GATEKEEPER Policy, Legal and Gender Board, and presents a plan for the final evaluation of the project's potential impact, which is to be undertaken in the last year of the project and reported in the final iteration of this deliverable.

2 GATEKEEPER Ethics Framework Update

2.1 Introduction

In the DoA we have highlighted the basic characteristics of the GATEKEEPER project. As mentioned, the project "connects healthcare providers, businesses, entrepreneurs, elderly citizens and the communities they live in, in order to create an open, trust-based arena for matching ideas, technologies, user needs and processes, aimed at ensuring healthier independent lives for the ageing populations. The aim of the project is to be able to produce by 2022 an open source, European, standard-based, interoperable, and secure framework available to all developers, for creating combined digital solutions for personalised early detection and interventions that:

(i) Harness the next generation of healthcare and wellness innovation

(ii) Cover the whole care continuum for elderly citizens, including primary, secondary and tertiary prevention, chronic diseases and co-morbidities

(iii) Straightforwardly fit "by design" with European regulations, on data protection, consumer protection and patient protection

(iv) Are subject to trustable certification processes

(v) Support value generation through the deployment of advanced business models based on the VBHC paradigm[1]

The current document presents the state of the art of on: evaluation of ethics compliance questionnaires provided by pilots, assessment of dataflows and aggregation of datasets in repositories both in terms of pilot's tenants and GATEKEEPER Data Federator. It has been supported by initial checklists.

2.2 The role of IoT and AI in e-health[2]

In Europe and elsewhere, the prevailing hope is that the application of these emerging technologies in the healthcare sector will lead to better health outcomes for individuals as well as to greater cost efficiency for healthcare providers. Proponents of healthcare IoT and AI also foresee a number of specific benefits in the provision and management of care, such as adjustable patient monitoring, patient engagement, enhanced drug management, augmented asset monitoring and tracking, early intervention, improved management of population health, operational improvements, and strengthened innovation. These assumptions have guided many recent initiatives in industry and research, for instance the ACTIVAGE project, which seeks to build a Europe-wide ecosystem for healthcare IoT.[3]

Alongside these 'pull' factors, the changing age composition of populations in industrial societies serves as a formidable 'push' factor. In most highly developed countries, medical

[1] GATEKEEPER DoA.

[2] For further information and a more extensive review of the associated topics, see D5.2, D5.3 and D6.3.1

[3] ACTIVAGE Project (2020) About ACTIVAGE, https://www.activageproject.eu/activage-project/#About-ACTIVAGE.

advances mean that more people reach old age. By 2050, it is estimated that 25% of the population in Europe, the United States and Canada will be over the age of 65. However, the number of healthcare professionals is not projected to increase in a similar fashion. As such, medical innovations – not least using IoT and AI technologies – will be needed in order to meet the increasing healthcare needs of ageing societies.

Unsurprisingly, all this creates considerable financial incentives for developers and manufacturers: according to McKinsey, the total value created in the healthcare industry by IoT alone amounts to nearly US$6.8 trillion.[4] In a recent study, McKinsey estimated that by 2030, the use of IoT could enable $5.5 trillion to $12.6 trillion in value globally, in contrast with the same value captured in 2020 reaching $1.6 trillion. The health sector, expected to account for 10-14% of the estimated economic value in 2030, is expected to reach even $1.7 trillion alone.

Meanwhile, the European Commission estimates that Europeans over 65 constitute a market currently worth more than €300 billion – a figure that is likely to increase drastically, given the projected growth of that segment of the population.[5]

IoT and AI technologies are already in use in the healthcare sector in a number of ways; for instance, in the form of remote monitoring (tele-monitoring) of patients in real-time, testing of new and experimental treatments, actuation of medical devices, and monitoring of fitness and well-being.[6] Applications also include care delivery, management of care for the chronically ill, incoming patient triage, diagnostics, and clinical decision support, as outlined in a recent report on healthcare and AI by EIT Health and McKinsey.[7]

The same report looked at 23 use cases for AI technology in healthcare. The use cases included mobile apps for self-care, online platforms for looking up symptoms, "e-triage" tools (e.g., Babylon Health and Mediktor), virtual agents for hospitals (e.g., Amelia), and even a bionic pancreas (iLet, developed by the US company Beta Bionics) that monitors the blood sugar levels of type 1 diabetes patients and independently administers insulin.[8] In the GATEKEEPER project itself, we have identified a further 21 use cases for both IoT and AI. These include web portals and mobile apps for tele-monitoring, sensor technologies for use in the home and outdoors, fitness applications and smart watches, virtual assistants, Wifi-enabled home applications, and rehabilitation and training tools.

At the moment, most healthcare solutions that implement IoT and AI technologies address routine, repetitive and administrative tasks. Such tasks are not particularly complex, but they can be time-consuming if done manually. In the medium term, experts believe that AI technology in particular will be further integrated into clinical workflows. This will support a transition from care in hospitals to care at home or remotely, in the process also giving patients more control over their own treatment regimens.

[4] See ACTIVAGE Project (2017) Ethics and Privacy Protection Manual, p. 11.

[5] European Commission (2010). eInclusion: Ageing Well Action Plan.

[6] Empirica & WRC (2010) ICT & Ageing – European Study on Users, Markets and Technologies. Brussels: European Commission.

[7] Ibid.

[8] Ibid.

Further down the line, IoT and AI solutions will increasingly be deployed in support of clinical decision-making. One particularly promising area of development entails the use of AI algorithms to establish correct dosages of drugs. At present, most dosing is done according to general guidelines and no small amount of guess work, increasing the risk of human error.[9] Once correct dosages have been ascertained, IoT technology can be used to administer the drugs to the patient.

Overall, IoT and AI technologies have significant potential to improve the management and delivery of healthcare, benefitting both care providers and recipients. However, the deployment of these emerging technologies also raises pressing questions about privacy and ethics. These questions need to be addressed in order to truly harness the potential of IoT and AI in healthcare.

Throughout the project's development, several risk identification and compliance-related actions (as reported in this deliverable) have been proposed which have led to the identification of certification (stemming from GDPR article 42 and the AI act's certification mechanism) as a potential solution which could help bridge the gaps between AI and health-data usage restrictions presented by the current regulatory framework. Cross-WP research activities are ongoing to clarify and propose a viable certification option as part of the activities of WP8 with the support of GATEKEEPER's Policy, Legal and Gender Board. These elements will be reported in the final iteration of this deliverable and in the relevant deliverable for WP8 as necessary.

2.3 Information ethics in IoT and AI

The use of IoT and AI raises a host of ethical concerns related to the interrelations between the" things"/machines and humans. In the context of the use of ICT (including IoT) with respect to applications of personal assistance some common concerns are about:

- The pervasiveness of a technology that is difficult for the users to understand, and that becomes more evident in utilizing IoT-technology in an invisibility manner
- The difficulty of respecting privacy and confidentiality. This is in particular the case when third parties may have a strong interest in getting access to electronically recorded and stored personal data
- The difficulty in ensuring the security of shared personal data
- The lack of the establishment of trust framework that ensures protection of personal data, enhanced privacy and usable security countermeasures on the personal & sensitive data interchange among IoT systems
- The lack of transparency in relation to the data collection and the use of the personal data and its effects on the relationship between the users and the service providers

As a reflection of the above-mentioned types of concerns around personal data, international and European regulatory agencies have increasingly moved from a technical discussion around personal data towards a discussion around human rights, human dignity

[9] Ibid.

and values[10]. The use of personal data involves a risk that the person only becomes data and lose their human value. Ethical discussions in this context evolve around the issues of preserving human dignity and values(ibid).

At the centre of the discussion about how an ethical framework for AI and IoT looks like is the question of trust. All stakeholders involved in the development, deployment and use of AI and IoT applications need to be ensured that the systems are trustworthy from social, technical, and legal perspectives. In accordance with this principle, the development of a framework of ethical guidelines in relation to IoT and AI for the GATEKEEPER project will take into account and build upon The Ethics Guidelines for Trustworthy Artificial Intelligence, by the High-level Expert Group on AI, in April 2019.[11]The publication outlines guiding principles for trustworthy AI and sets out key requirements to be met by trustworthy AI systems.

According to the guidelines, trustworthy AI should be:

(1) lawful - respecting all applicable laws and regulations

(2) ethical - respecting ethical principles and values

(3) robust - both from a technical perspective while taking into account its social environment

The guidelines set out seven key requirements that need to be met by trustworthy AI systems.

Key requirements for trustworthy AI systems

- Allowing for human agency and oversight
- Technical robustness and safety
- Respect for privacy and ensuring adequate data governance mechanisms
- Making sure that the data, system and AI business models are transparent
- Diversity, non-discrimination and fairness: avoiding unfair bias and making sure the systems are accessible to all, regardless of any disability
- Societal and environmental wellbeing: ensuring that the systems are sustainable and environmentally friendly
- Accountability: putting in place mechanisms to ensure responsibility and accountability for AI systems and their outcomes

In particular, the guidelines specify four ethical principles with their roots in fundamental human rights that all trustworthy AI systems must meet.

[10] Fabiano N (2019). Ethics and protection of personal data.*Systemics, cybernetics and informatics volume* 17 - number 2 - year 2019

[11] EPRS BRI (2019)640163

1. **Respect for human autonomy**. This means that the AI systems must allow for human oversight over the work processes in the systems, and also that the persons interacting with the systems must keep their autonomy and self-determination
2. **Prevention of harm**. This includes paying attention to situations where the information collected could be used in a way that has adverse effect on the persons interacting with the system
3. **Fairness.** This involves ensuring non-discrimination and equal opportunity as well as respecting the principle of proportionality between means and ends
4. **Explicability.** This involves transparency in the processes and in the communication about the system and its purposes

These abstract ethical principles provide the baseline for developing actual ethical requirements to be implemented in the development of the GATEKEEPER technical framework, in order to assist developers in addressing real world ethical challenges with the IoT and AI in the context of health applications.[12]

To concretise the four overarching ethical principles, it is proposed to use a set of more concrete guiding principles that have been explicitly developed for the purpose of IoT in the context of Active Health and Ageing, in the ACTIVAGE project.

The list of guiding principles stems from the basic principles of medical ethics and the OECD's Privacy Framework.[13] These principles are listed below, with a comment on their relation to the four principles embedded in the ethics guidelines for trustworthy AI, namely (1) Respect for human autonomy (2) Prevention of harm (3) Fairness (4) Explicability:

Collect the minimum required data and ensure that data processing protocols are transparent and accountable (principles (2) and (4)); Support the ethical capabilities of human beings such as agency, awareness and reflexivity (requiring transparency on how data are collected and distributed) (principles (1) and (4)); Create and maintain trust and confidentiality between users and providers (all 4 principles); Embed inclusiveness in design (principle (3)); Facilitate public health actions and user engagement related to IoT for health (principles (1), (3) and (4).

2.4 Policy, Legal and Gender Board Organization

According to art 6.8 of the GATEKEEPER Consortium Agreement: "*The Policy, Legal and Gender Board will be formed by the Project Steering Committee by appointing experts*

[12] In deliverables D6.3.1 (M12) and D6.3.2 (M24) we have considered the EC's Guidelines for Trustworthy AI, and, upon these guidelines, we have loacted particular AI-powered frameworks and statements (TRIPOD, PROBAST) to address the requirements on: Technical robustness and safety, Making sure that the data, system and AI business models are transparent, Diversity, non-discrimination and fairness: avoiding unfair bias and making sure the systems are accessible to all, regardless of any disability. As the above requirements are part of the AI developments in GK (GK AI Framework developed in T5.2, T5.3, and T6.3), and, importantly, AI services will be assessed with respect to the above qualities, it could be mentioned/commented herein as a step towards the GK Ethical Framework.

[13] Beauchamp & Childress (2009). *Principles of biomedical ethics*. New York: Oxford University Press, 5th ed.; OECD (2013). The OECD Privacy Framework.

from industry and demand users of the consortium (one per local pilot), as well as by policy makers and gender equality officers from the demand cities in the consortium. The work so far has been carried out in the context and resources of WP1 in Annex 1 of the Grant Agreement".

This board is coordinated by and linked with the work of the Ethical, Legal and Gender Issues Manager (ELGM) Ms. Stea Miteva (UDGA) / Mr. Adrian Quesada Rodriguez (MI), who shall provide advice and support (with the support of the Ethical, Legal and Gender Board, described later in this section) on with the following issues: a) Legal aspects: the legal issues associated to the deployment of GATEKEEPER tools and actions (e.g. IPR, data protection and access, privacy issues, ethical aspects, etc.), b) Policy issues: how new policies could help innovative smart living technologies get users acceptance and market uptake, Gender issues: the ELGM will be responsible to supervise the implementation the gender equality policy of the project and c) ethical, security and data management concerns in data management.

This board acts, among other duties, that the GATEKEEPER project pilots are executed in an ethically sound manner and in compliance with relevant national and international ethical requirements for trials involving patients. The board has contributed to the dissemination of the project's principles among partners and their revision. The board has been available on demand upon the request of different partners and has been contributing to the solution of horizontal problems faced by the project and the pilots. They have involved legal and ethical concerns and their potential consequences for the project. The board has approved its terms of reference which were made available as an annex to the first iteration of this deliverable.

2.5 Policy, Legal and Ethics Board main outputs

Following its establishment, the GATEKEEPER Policy, Legal and Ethics Board sought to address a number of issues during its monthly meetings, namely:

- Role identification across consortium and facilitation of negotiation of Data Processing Agreements (Joint Controller Agreements / Data Processing Agreements)
- Identification of data processed by Pilots
- Identification of Key enabling Technologies to be used by the pilots
- Pilot anonymisation activity harmonisation
- Ethical Assessment for every project partner (including multiple discussions with the coordination team to address the significant delays in receipt of partner inputs)
- Gender initiative and reporting activities
- Coordination with UoW with regards to Ethical Approval Process
- Coordination with Pilots to support and obtain information about the DPIAs carried out by each

2.6 GATEKEEPER Ethical Strategy

The ethical approach that shapes GATEKEEPER vision is deeply influenced by the context in which the project operates. The consortium is fully aware of the ethics and data protection issues stemming from the deployment of ICT-related technologies that can collect, distribute and exchange data within intelligent environments.

The ethical approach is shaped around the main target group of GATEKEEPER which will be older adults. As we have already highlighted in our proposal, the inspiring principle will be to fully comply with relevant European and national laws for the collection and management of personal data and in particular with the General Data Protection Regulation and anticipate forthcoming European regulation initiatives such as the AI regulation. GATEKEEPER will adopt a privacy by design and by default approach by minimizing the collected information to the ones strictly required to perform the action at hand and to avoid retaining this information when they are no more required.

A preliminary evaluation of the ethical issues arising from the pilots has already been offered in D1.5. In this deliverable we include an updated version of the first evaluation complement with an analysis, pilot by pilot, on the basis of the GATEKEEPER sets of value identified also in cooperation with the ongoing work in WP2. This exercise contributes to the design of the Ethical Impact Assessment that GATEKEEPER will deliver by the end of the project. The EIA will also benefit from the GATEKEEPER contribution to the activities of the WG5. As far as the GATEKEEPER platform is concerned, the overall approach will be to adopt a security-by design, privacy-by design, as well as to put the user in full control of his/her personal data. Project partners have a common interest in working together in accordance with the project's ethical strategy. The Ethical approach outlined in this document is primarily directed to the partners involved in the pilot zones and the providers of technical solutions. They are expected to follow the basic principles outlined in this document and contribute to its revision in the course of the project (see D6.3.1 and 6.3.2).

Ethical issues to be dealt with in the context of GATEKEEPER are the same as those identified in the context of other e-health related projects. In our case, and in this version of the deliverable we refer to those identified in the context of the PICASO project[14] and aim at further elaborating from them:

a) *Informed consent*[15]

Informed consent is generally seen as guaranteeing that research involving human subjects, especially in clinical and medical context, is ethically sound. It is important to address the context and manner in which the consent is collected, and it is important to be aware of the inherent power relations within the informed consent process. In the context of GATEKEEPER and the technologies that will be developed and tested, informed consent is an important step towards overcoming ethical problems related to privacy and data protection, surveillance and autonomy. Informed consent allows the user/patient to exercise control over his/her personal data by determining who has access to what information and when. All the pilots will follow the necessary steps in order to guarantee an appropriate handling of the informed consent.

b) Autonomy

Autonomy is a core issue to be dealt with in the case of use of ICT in healthcare. Autonomy implies having control of the system/devices and that the informed user/patient is able to switch it on or off. The patient must always be made fully aware of the consequences

[14] D3.3. *PICASO Ethical Guidelines*, 28July 2016, Version 1.0.

[15] These principles are taken from the elaboration of the PICASO project. In our understanding they are key also in the context of GATEKEEPER and will be further integrated and transformed to our future work

of non-concordance. The participants in GATEKEEPER must be informed of their free choice to opt out at any point in time. Patients should also be made aware of what will happen after the trial ends, e.g., what will happen to the devices they have been using or had installed. There is an obvious ethical problem of offering a service for a limited time only and participants should therefore be made fully aware of any limitations, particularly with respect to post-trials.

c) Dignity

The notion of dignity is related to the notion of integrity. Treating people with integrity helps to avoid violating their dignity. According to the European Charter of Fundamental Rights, dignity includes i) the right to life and ii) the right to the integrity of the person, which also implies the right to the free and informed consent of the person concerned. Also, the Universal Declaration of Human Rights adopted in 1948 states that all people are "free and equal in dignity and rights". The notion of dignity has a particular meaning in the context of health care. According to the Declaration of Helsinki, article 11: "It is the duty of physicians who participate in medical research to protect the life, health, dignity, integrity, right to self-determination, privacy and confidentiality of personal information of research subjects". These aspects will be all considered by the GATEKEEPER's pilots.

d) Non-Stigmatisation

Stigmatisation or stigma is something that can be present either directly or indirectly. Stigma means "label" and refers to labels that can be imposed on others, perhaps most often due to ethnic and/or social background, which can lead to discrimination and social exclusion. In a medical context, patients suffering from e.g., life-style disease may often experience that they are being stigmatised (labelled). In the case of GATEKEEPER it is important to consider the design and implantation of technical solutions but also to respect participants' feelings towards using the different devices in the context of the pilots.

e) Inclusion

The notion of inclusion is often used to signify a process, *de facto and de jure*, of including people in a given social structure, most often in society at large. In the context of e-health, access is key and becomes an acute ethical issue. For example, access to assistive technologies targeted at the elderly is not simply about making these technologies available or offer them; access is in this context dependent on the person's ICT literacy. In the context of GATEKEEPER the pilots are invited to facilitate the understanding of the proposed solutions by end-users and, in the design of the platform, to evaluate improvement to the usability aspects in order to adapt the platform to the needs of the various groups, including the needs and vulnerabilities of key minority groups.

f) Privacy and Data Protection

Privacy and data protection are ensured by law, but it is nevertheless useful to assess their ethical implications. They include: what information is collected and how, controlled (non-excessive) use, for what purpose the information is used, to whom it may be transferred, user's access to information and the possibility to correct personal information, storage, etc. The respect of norms and the guarantee of compliance are crucial in the context of e-health. The GATEKEEPER pilots have been invited to perform their data protection impact assessments before deployment and adopt all the necessary organizational and technical measures to guarantee data protection.

g) Incidental findings

Details on this have been already reported in D.10.2.

2.7 GATEKEEPER Participants

GATEKEEPER participants, including researchers, patients and the different partners, are at the core of the respect of the ethical and compliance measures we suggest in the current document and in other deliverables. It is only the respect of applicable norms and a continuous ethical monitoring and assessment of the different actions undertaken in the context of the project that will guarantee the respect of their dignity and their full involvement.

2.8 GATEKEEPER contribution to Health & Care Cluster

Taking into account its research framework and objectives, GATEKEEPER is contributing to the initiatives of the Health & Care cluster in order to aggregate research and innovation efforts into more effective responses to the policy needs of the Union. In particular, this coordination action is needed after the Covid-19 pandemic has brought many challenges to the lives of people in Europe and beyond. The pandemic has affected in many ways all the projects involved in the cluster but can also generate opportunities through the digitalization of many aspects of our lives. This is particularly true in the context of protection of personal data especially in the health-care sector. the pandemic has showcased both the opportunities and limitations of the current approach to personal data protection in Europe and provided learning experiences which have been integrated in GATEKEEPER's use-cases on the subject. The pandemic has clearly had an impact on economic and social European policies. Health is already emerging as one of the priorities on which the European Union will be called to focus on with a proper EU health strategy. GATEKEEPER will continue to follow these developments with the aim of contributing to them on the basis of the research and innovation activities undertaken in the context of the project, particularly through coordination between this task and the expected actions on standardization and certification (including particularly ongoing work towards clarifying the diverging and converging requirements of the diverse data-related regulations that have been proposed in the recent years.).

2.9 Findings

GATEKEEPER has designed and pursued an ethical strategy that takes into account a robust protection and promotion of individual and collective well-being. The project continues its work towards the ethical impact assessment and other compliance-related actions as described in the first iteration of this deliverable, particularly as necessary to support the activities of Pilots. Ongoing discussions with the non-EU pilots seek to clarify the extent (if any) on which the ethical framework will be applicable given their different approach, this will be reported on the final version of the deliverable.

3 Ethical Principles Assessment and Mitigation Strategies

3.1 Introduction and Strategy

Having identified relevant and applicable tools (PICASO project)[16] and principles[17] we submitted them for an evaluation to WP2. WP2 feedback has helped to streamline and better define the relevant principles in the context of the GATEKEEPER ecosystem. This then led to the request for contributions both from the partner[18] and pilot level. This section showcases an updated version of the ethical assessment and sets the baseline elements to be considered in the final iteration of this deliverable.

3.2 Identified ethical principles:

3.2.1 Respect for confidentiality and privacy (GKP1):

Legal compliance should be guaranteed, but also a moral and ethical commitment to respect confidentiality and privacy. A key aspect is here represented by the principle of informed consent

Application guidelines:

- The GATEKEEPER project (all project partners) must treat participant information with confidentiality
- Participants may exercise control over personal information by consenting to, or withholding consent for, the collection, use and/or disclosure, modification, loss or theft
- Implement the Privacy by design principle and provide with transparency all the relevant information
- Adherence to national and international regulations on privacy and data protection

3.2.2 Beneficence (GKP2):

Persons are treated in an ethical manner not only by respecting their decisions and protecting them from harm, but also by making efforts to secure their well-being. A key aspect is here represented by person-centered care (or tailor-made/customised)

Application guidelines:

[16] Picaso project, D3.3. PICASO Ethical guidelines.

[17] M. Ienca, E.Vayena, AI Ethics Guidelines: European and Global Perspectives, Council of Europe-Ad Hoc Committee on Artificial Intelligence, 15/6/2020. See also A. Mantelero, AI and Big Data: A blueprint for human rights, social and ethical impact assessment, Computer Law & Security Review, 34, 2018, pp. 754-772.

[18] For transparency purposes it is important to note that the proposed partner-specific assessment actions (reported on Section 4.6) were severely disrupted by lack of response to the proposed actions from the diverse project partners despite multiple reminders at various levels (including two express requests during Plenary meetings). This problem can be partially attributed to COVID-19 issues faced throughout the project.

- Explain the limitations of the GATEKEEPER pilots, particularly in terms of probable personal and/or health benefits during and after the pilot
- Inform of possible clinical incidental findings prior of informed consent form and how these will be handled
- Follow standard clinical practices for consulting relevant specialist and for informing patients of clinical incidental findings and take appropriate actions
- Maximise probable benefits and minimise possible harms
- Continuously assess probable risk and benefits. The probable benefits must be deemed higher than the probable harm
- Put the health and welfare of participants at the highest priority

3.2.3 Justice (GKP3)

This principle includes the process of selecting participants in a justifiable manner. A key aspect is here represented by the issues of inclusion and non-stigmatisation.

Application guidelines:

- The selection of participants must be fair and equal i.e., inclusion/exclusion in the trial must not be denied a person without good reason but must be based on reason directly related to the objectives of the pilot
- Pilots should strive to address the differences between participants, by calibrating recruitment effort with the aim of mitigating socio/economic barriers to participation especially in the field of digital literacy

3.2.4 Respect for Persons (GKP4)

It includes respect for autonomy and dignity. Respect for persons demands that subjects enter into the research voluntarily and with adequate information. A key aspect is here represented by the issues concerning autonomy and dignity.

Application guidelines:

- Inform and seek advice if there are concerns related to the integrity and quality of the project and pilots
- Pilots should try to support older citizens/patients to be active participants in the intervention processes and not passive recipients
- Treat patients as autonomous agents and respect their right to determine their own best interest
- Actions conducted in the pilot should always consider the respect of the dignity of the participants and of all the people involved
- Enable participants to make reasoned informed choices and decisions
- The collection of informed consent must follow four steps:
    - Accessibility: The information must be formulated in a non-technical, plain language. The achievement of the accessibility level of the information must be verified, i.e., the definition of the key information is co-designed with participants and/or its efficacy been tested with end users

- Information: detailed information of the pilot, including potential benefits, intended use of the collected data, risks and limitations, must be provided
- Comprehension: The information must be given both verbally and written in clear language, in a precise and calm manner and in the proper context. Participants should be invited to ask any questions they may have
- Voluntariness: The informed consent form must stress that participation is voluntary and that participants are free to withdraw at any time at their own discretion and at no cost (without reprehension)

3.2.5 Transparency (GKP5)

Open and transparent information shall be guaranteed to researchers and patients. In this domain the interaction with the project Platform Cluster will be particularly relevant especially as far as AI transparency is concerned.[19]

Application guidelines:

- The GATEKEEPER project must be as transparent as possible in explaining its goals
- Information shall be explained to help citizens/users to navigate themselves through the available sources
- The GATEKEEPER project should also strive to empower participants as only ensuring access to information is not enough. Skills to have access to the information and how to use technologies should be part of the empowerment process
- The use of AI and machine learning should be made as transparent as possible by enabling end-users to access relevant information
- Access to public documents of the project shall be guaranteed

3.2.6 Sustainability (GKP6)

The solutions proposed by the project are sustainable in the medium and long term. In this domain the interaction with the project Business Cluster will be particularly relevant.

Application guidelines:

- The GATEKEEPER project must strive to find sustainable solutions both for the hospitals and for the patients
- The GATEKEEPER project must aim to minimize the impact of the suggested solutions on the environment and on the use of energy
- The GATEKEEPER project should pursue the social acceptability of its solutions also by analysing the potential negative impact in the specific deployment context

[19] To this end, joint work between WP6 and WP1 is envisioned in the upcoming months.

- The GATEKEEPER project should ensure the safety/security of its solutions in terms of functional safety in relation to the technologies but also as a condition of being able to live at home or outside his/her personal life

3.3 Ethical Approval from local committees

The GATEKEEPER pilots will apply for approval for the trials to the relevant local ethical committee. Approval must be obtained prior to the start of the pilot. Relevant information, also on the current situation, are provided in D.6.5.

3.4 Ethical Risks in GATEKEEPER

Following the identified ethical principles in section 4.2, a checklist for mapping of data protection and ethical issues in the context of the pilots was produced and shared with the pilot owners. As outlined in the table below, each pilot has been requested to identify if and how the tenants comply with the recommendations.

Table 1: Checklist

Checklist	Compliance (yes/no/not applicable)	Comments
Privacy and data protection - The organization makes use of privacy by design principles. Describe them.		
Privacy and data protection - A data protection impact assessment has been performed		
Privacy and data protection - Organizational and technical measures to guarantee the safety of data are in place. Detail the measures which are in place in the comments section. Highlight any relevant problem.		
Informed consent – Participants have been given detailed information about the pilot, including its purpose, limitations and potential benefits and risks. Information has been provided also on the use of data gathered in the context of the pilot The decided informed consent procedure included an assessment of the participants' understanding of their rights and the implications of their participation in terms of obligations, efforts, and risks		
Informed consent - The information has been given verbally with supporting written information and in clear language.		

Informed consent - Participants have had the opportunity to rethink if they want to participate or not.		
Informed consent - The decided informed consent procedure has been followed and copies of all participants signed informed consent forms have been forwarded to the responsible person.		
Autonomy - The voluntariness of the participation has been highlighted as have the option to withdraw at any time without any repercussion		
Autonomy - The pilot will not use a technology/device that constrains a person or curtails their freedom of movement or association.		
Autonomy - Participants are able to control the technologies/devices used for monitoring (i.e., they can switch them off or choose not to send data).		
Autonomy - In the recruitment process and during the pilot participants are/have been treated as autonomous agents and their right to determine their own best interest is respected.		
Dignity - Participants' personal information is treated with confidentiality.		
Dignity-The pilot recognizes and respects the right of participants to lead a life of dignity and independence and to participate in social and cultural life.		
Non-Stigmatisation - Utmost efforts have been made to ensure that the least intrusive, physically and aesthetically, devices and technologies are used in the trial.		
Non-Stigmatisation - The pilot does not require participants to use a technology that marks them in some way as cognitively or physically disabled.		
Inclusion - Participants' needs and requirements have been defined and used to guide the selection of technologies/devices as usability is a priority.		
Transparency - Researchers have been transparent explaining the project goals.		
Transparency - Full access, in compliance with applicable laws, to the public documents of the project is guaranteed.		
Sustainability - The development of the technologies employed is done taking into account their long-term sustainability.		

Sustainability - Users and not only the organization benefits from the collection of data.		

As described in the initial version of this deliverable, this checklist provides an initial identification of controls that will be checked through several iterations with the pilots. The answers provided by each pilot were assessed against the data protection and ethics principles outlined both in the current legal, ethical, and privacy framework, as well as in the Data Management Plan (D1.4). The assessment allowed to identify established good practices, but also recommendations for identifying areas that need improvement.

All of the proposed mitigation actions in the following sections shall be complimented by direct application by the data controllers of each pilot, of the relevant EDPBn (European Data Protection Board) guidelines and recommendations and national dispositions showcased in section 5 of this deliverable, the controllers should ensure proper documentation regarding actions towards compliance is kept on file and shared with the Policy, Legal, and Gender Board before the end of the project.

3.4.1 Saxony pilot

The Saxony pilot is committed to follow the GDPR and the German Data Protection Act to ensure the compliance of its actions with the Regulations and data protection of the participants. The DPO of the projects has granted a data protection plan for RUC 1 and is in process of providing one for RUC 7. Participants' data is stored in local servers with a dedicated access management policy and tokenized (pseudonymized), processed only for research purposes and not shared with the consortium. Appropriate TOMs have been adopted. Participants' involvement is based on freely given informed consent, which participants receive and give in writing and are aware of their right to revoke it without any negative consequences. For example, in the RUCs where device monitoring is included, patients can switch off the monitoring technology. The health monitoring devices are assessed by the local ethics committees to least intrusive measures to monitor the health data needed for the RUC, and dues not "mark" participants in a stigmatizing way.

As the ethics protocol[20] for the pilot concludes, the study is of overall low risk; the study is being conducted in a data protection compliant manner, and neither of the data processing technology can worsen, intensify or increase the symptoms of the participating patients.

Proposed mitigation actions: The Saxony pilot need to ensure:

- Report the completion and outcomes for the DPIA for RUC 7
- Explain the provided opportunities for data subjects to ask questions before granting their consent via app

[20] Task 6.5.

- Demonstrate efforts towards facilitation of the exercise of will to withdraw from the study

3.4.2 Aragon pilot

The Aragon pilot is committed to respect and comply both with the GDPR, as well as with complementary national regulations. As the pilot will use different types of technologies for its studies, including Artificial Intelligence model that will be trained with collected data to predict potential worsening of patients' conditions, a Data Protection Impact Assessment has been performed. Personal data will be tokenized (pseudonymized) and only some of the data, generated precisely for specific RUCs will be transferred to the GATEKEEPER platform, stored and processed in servers belonging to the GATEKEEPER consortium. The data processing is based on the informed and written expressed consent of the patients. The participants are keeping their autonomy as they are made aware of the opportunity to withdraw from the study at any given point without any adverse effects for them or for their health. The technology used for the RUCs is as least intrusive as possible, collecting and processing data only when the patient knowingly interacts with the device, not permitting any "passive" data collection.

UNESCO Recommendations on the Ethics of Artificial Intelligence note that "*AI technologies can be of great service to humanity […], but also* ***raise fundamental ethical concerns****, for instance regarding the* ***biases*** *they can embed and exacerbate, potentially resulting in* ***discrimination, inequality, digital divides, exclusion and a threat to cultural, social and biological diversity and social or economic divides****; [there is a] need for* ***transparency and understandability of the workings of algorithms*** *and the data with which they have been trained; and their potential impact on, including but not limited to, human dignity, human rights and fundamental freedoms, gender equality, democracy, social, economic, political and cultural processes, scientific and engineering practices, animal welfare, and the environment and ecosystems*"[21]. This is further supported by the WHO guidance on Ethics and governance of artificial intelligence for health, identifying the elevated risk of misuse of obtaining informed consent: "*The use of predictions throughout health care also raises ethical concern about informed consent and individual autonomy if predictions are shared with people who did not consent to surveillance, detection or use of predictive models to draw inferences about their future health status or to provide them with a "predictive diagnosis" that they did not request in advance*"[22].

Proposed mitigation actions: Aragon pilot should therefore ensure that:

- Algorithms used to train Artificial Intelligence with health data are explainable
- Privacy-by-design and privacy-by-default methods are used to ensure data minimization, purpose limitation and contribute to bias prevention

[21] UNESCO Recommendation on the Ethics of Artificial Intelligence, accessible here: https://unesdoc.unesco.org/ark:/48223/pf0000380455.

[22] World Health Organization. (2021). Ethics and governance of artificial intelligence for health: WHO guidance. World Health Organization. https://apps.who.int/iris/handle/10665/341996.

- The process of health data processing is transparent[23]
- The consent form specifically informs about the usage of decision-making predictive algorithms and requests the explicit consent of the patients to be subject to it

3.4.3 Basque Country

The Basque Country pilot commits to following and respecting both the GDPR and the national complementary data protection and other relevant regulations. As outlined in the ethical protocol of the Basque Country pilot provided by Task 6.4, the main objective of this study is to implement and assess the effectiveness and user experience of a self-managed mobile health application that recommends activities to promote healthy lifestyle habits. Personal data is, depending on the needs and its specific purpose either tokenized or fully anonymized, with only the treating physician and collaborators being able to relate the patient data to their medical history. Participants' involvement is based on freely given informed consent, which participants receive and give in writing and are aware of their right to revoke it without any negative consequences. The study is performed with as least intrusive technology as possible, Adequate TOMs have been adopted; the data is stored only in local servers.

This research is not a clinical trial, but a technology testing study. The ethical risk of the pilot is therefore low.

Proposed mitigation actions: The Basque Country Pilot should:

- Reason which datasets will be pseudonymized and which fully anonymized
- Demonstrate adequate technical and organisational measures to safeguard the rights and freedoms of data subjects beyond access management policy

3.4.4 Cyprus

The Cyprus pilot commits to respecting and complying with both the GDPR and complementary national legislative provisions. The pilot has adopted adequate TOMs, including encryption for APIs when storing the collected data in secure cloud repositories; clear task allocation and access rights management, as well as privacy-by-design approaches and data anonymization. Participants' involvement is based on freely given informed consent.

Ethically challenging is the participation/ recruitment of the pilot's target group: Patients with mild, moderate, and severe **dementia aged 60+** and high complexity level **cancer patients**, aged 50+. The capacity to consent or to decline consent to participate in research is regarded as acceptable criterion to determine vulnerability.[24] Nevertheless adults who are not capable of giving informed consent must be included in health-related research unless a good scientific reason justifies their exclusion. As these individuals are not able to

[23] In T6.3, the importance of adoption of TRIPOD and PROBAST statements towards increasing the transparency and reproducibility of results, in addition to the technical frameworks allowing us to implement trustworthy AI has been stressed.

[24] Council of International Organizations for Medical Science (2016), International Ethical Guidelines for Health-Related Research Involving Humans, Guideline 15, available here: https://cioms.ch/wp-content/uploads/2017/01/WEB-CIOMS-EthicalGuidelines.pdf.

protect alone their own interest, specific protections to safeguard their rights and welfare in research are needed. Dementia patients are a standard example of vulnerable individuals who may be incapable of giving an informed consent.[25] In accordance with relevant national regulations, the permission of an immediate family member or other person with a close personal relationship with the individual must be sought. Surrogate decision-makers must evaluate to what extent study participation is consistent with the individual's previously formed preferences and values (if any), and, in the case of research that offers participants a prospect of clinical benefit, to what extent study participation promotes the individual's clinical interests.

As outlined in the ethical protocol of the pilot in Task 6.5, the Cyprus pilot mainly focuses on the early detection of the condition worsening of cancer and dementia patients by monitoring whether the use of technology can trigger appropriate management, therefore reducing the need for higher acuity care, and improving survival[26]. Secondary Objective for patients includes improved parameters of participation in full and limited intervention groups associated with the improvement in disease self-management; symptom burden; motivation; mobility; sleep hygiene; depression and anxiety.

Proposed mitigation actions: Cyprus pilot should therefore ensure that:

- It does not exclude vulnerable individuals who are not capable of providing consent without providing special consideration by researchers and the pilot's local ethical committee
- Seeks consent by a legally authorized representative, a family member, or another person with close personal relationship to the vulnerable individual
- Provides specific protection to safeguard the rights and welfare of the vulnerable individuals

3.4.5 Greece

The Greek pilot aims at assessing the effect of the GATEKEEPER intervention on Glycaemic control; health-related quality of life over a period of one month comparing the intervention group with the control group, as well as the cost-effectiveness of the GATEKEEPER intervention for those purposes.

The study design of RUC 3 includes two phases: 1) single-arm study to optimize the AI algorithms and 2) randomised control study to. Validate AI algorithms. For this, advanced GATEKEEPER "things" will collect clinical data at home (i.e., blood glucose concentration data or continuous glucose monitoring data, physical activity, galvanic skin response, heart rate variability), whose input-output dynamics with respect to the short-term prediction of the interstitial glucose concentration will be represented via an adaptive machine-learning-based regression model.

The objective of RUC 1 is to assess the effect of the intervention on waist circumference (in cm) reduction over a period of 3 months.

[25] Ibid, Guideline 16.

[26] AI services will be developed for this purpose but will not be real-time tested.

The pilot has adopted adequate TOMs to guarantee the safety of participants' data. Approaches like privacy-by-design, encryption, secure networks and secure repositories are followed. Task and responsibility allocation management are in place. There is a destruction policy for sensitive data after the end of the project. Datasets will be anonymised in the GATEKEEPER platform and donated after the lifetime of the project.

Participants' involvement is based on freely given informed consent, which participants receive and give in writing and are aware of their right to revoke it without any negative consequences. The technology used is as least intrusive as possible, allowing participants to cease its usage at any given time by switching off the devices or turn off the Bluetooth connection to the respective tablet/smartphone app. Furthermore, the ethical protocol in Task 6.4 identifies that the pilot's primary aim is to provide participants with personalized guidance to improve their lifestyle behaviours, increase their health literacy and ultimately, improve their quality of life, and does not interfere with participants' social and cultural life, preventing the hazard of potential stigmatisation.

Ethically challenging factors in the Greek pilot are the machine learning for training of AI algorithm, as well as the involvement of elderly people as participants. According to the Declaration of Helsinki, vulnerable groups and individuals "*may have an increased likelihood of being wronged or of incurring additional harm*".[27] It is recognised that vulnerability is the increased probability and degree of physical, psychological, or social harm, as well as a greater susceptibility to deception or having confidentiality breached. This refers not only to the ability to provide initial consent to the research; it concerns also the participation in the research studies and its aftermath. In its guidelines, WHO classifies among "other potentially vulnerable individuals" people faced with physical frailty, for example, because of age and co-morbidities.

Proposed mitigation actions: The Greek pilot should:

- Explicitly state and document its compliance with the European Data Protection Regulation (EU-GDPR), as well as with any relevant national legislations
- Ensure that specific protection is in place to protect the rights and freedoms of vulnerable individuals
- Explicitly inform the participants that they might be subject to automated decision-making for the purposes of predictive disease management
- Ensure transparency, explainability and bias prevention in the AI model.[28]

3.4.6 Poland

The main objective of the Polish pilot is to lower the risk of non-adherence in older adults and elderly people. Main participants in the pilot are older adults and elderly citizens with asymptomatic/low symptomatic chronic physical condition(s) typically leading to life-long medication. The pilot commits to following and complying with the established guidelines and recommendations by the Data Management Plan.

[27] WMA Declaration of Helsinki (amended 2013), Article 19; available here: https://www.wma.net/policies-post/wma-declaration-of-helsinki-ethical-principles-for-medical-research-involving-human-subjects/.

[28] Transparency, explainability, and bias prevention are being considered as part of AI activities inT6.3.

Ethically challenging is the participation of elderly individuals, who might be considered vulnerable.

Proposed mitigation actions: The Polish pilot should:

- Demonstrate commitment to compliance with the GDPR and other relevant national legislation
- Ensure that technical and organisational measures are put in place to safeguard the rights and freedoms of the data subjects
- Demonstrate that utmost efforts have been made to ensure that the least intrusive, physically intrusive devices and technologies are used in the trial
- Demonstrate that the patients' participation in the pilot is based on informed consent
- Explicitly inform the participants that they might be subject to automated decision-making for the purposes of predictive disease management
- Provides specific protection to safeguard the rights and welfare of the vulnerable individuals.

3.4.7 UK

The UK pilot participates in two RUCs, RUC 9 with elderly people in good health, and RUC 7 with elderly people with multiple pre-existing chronic conditions. Elderly people in care homes; such in poor physical and/or mental health, those dependent on caregivers, as well as those without direct internet access or unwilling to use the applications, are excluded from the study.

This study involves collecting data by the robots in the participants homes, including maps of houses of rooms (shape and sizes), including the types and location of objects and activities during time. The pilot commits to following and complying with the European and national regulations on data protection, as well as to follow the binding recommendations in the DMP (D1.4) and those of Open University.

Participants' involvement is based on freely given informed consent, which participants receive and give in writing and are aware of their right to revoke it without any negative consequences. The technology used is as least intrusive as possible, allowing participants to cease its usage at any given time without the hazard of adverse effect. Furthermore, the technology will be owned by the participants, which effectively ensures autonomy - that there will be no use of a technology/device that constrains a person or curtails their freedom of movement or association) and that participants are able to control the technologies/devices used for monitoring.

Ethically challenging is the monitoring of the houses of participants, and the preparation of maps of the rooms and interior facilities. In the light of Art. 8 ECHR, the home belongs to the private sphere of a person and needs a higher level of protection. An "intrusion" of this private sphere needs to be justified but also limited by a certain scope, moreover, if there is a constant monitoring ("surveillance").

Proposed mitigation actions: The UK pilot should:[29]

- Prove that the exclusion of certain types of vulnerable people in the stud is not based on stereotypes, i.e., through proof of consultation with relevant stakeholders, where feasible, before, during, and after the study[30]
- Prevent the risk of "surveillance" in the homes of vulnerable individuals; ensure no risk of facial recognition, collection of identifiable information or pairing of collected information to other personal and sensitive data
- Demonstrate adoption of safeguards to protect the rights and freedoms of vulnerable individuals

3.4.8 Puglia

Puglia pilot commits to respecting and following the provisions by the GDPR and the complementary national legislation. The primary objective of the study is to evaluate the cost/utility ratio related to the large-scale introduction of Mobile health technologies for monitoring the effects of healthy lifestyles and health promotion and for monitoring and self-empowering chronic patients, along two samples of elderly people. The study will utilize conventional smartphone apps and certified medical devices, hence, no particularly relevant safety issue is anticipated. Furthermore, the technologies used in the Puglia Pilot will not have detrimental effects on participants' freedom and rights.

Proposed mitigation actions: Puglia pilot should:

- Demonstrate adoption of appropriate technical and organisational measures for safeguarding the rights and freedoms of data subjects
- Provide sufficient information on the process for obtaining informed consent and ensuring it has been given freely
- Demonstrate adoption of safeguards to protect the rights and freedoms of vulnerable individuals.

3.5 GATEKEEPER platform: updated ethical impact assessment

The GATEKEEPER platform conceptually is a set of empty IT tools that are designed to provide services in the health domain. The platform itself does not have an impact on ethics, when it is used by pilots to build applications on top of it is when ethics come to play. What has an impact on ethics are the application built by using the services provided by the platform and with which data it is populated. If data has race biases it is not related to the platform service itself, but it is an issue raised from whom is feeding the data into the platform service.

[29] In UK RUC 7, AI services will be trained and tested upon pilots' data, but an AI-based intervention is not considered.

[30] WhO Commentary on Guideline 15 (ibid).

Each pilot owns a decoupled instance of a GATEKEEPER platform, where data and services are not shared, and only the owners (pilots) can decide what they want to share and with whom.

As described, the key value proposition of GATEKEEPER rests on the various tools and solutions that can be implemented by data controllers (pilot owners in the project's context) though the platform. In the previous iteration of this deliverable, an initial ethical assessment of the platform was prepared with the support of the researchers involved in its creation. As we continue to closely monitor the ethical and social implications of the GATEKEEPER platform, an update to this assessment is presented in this section:

Does this platform threaten the freedom of individual humans?

Original Answer: No

Updated Answer: No

- Does this platform alter an individual's freedom of movement?
    - Original Answer: No
    - Updated Answer: No
- Does this platform interfere intentionally with the formation of expression or beliefs?
    - Original Answer: No
    - Updated Answer: No

Does this platform threaten the natural equality of persons?

- Are expected benefits divided between groups for reasons not associated with difference in use?
    - Original Answer: No
    - Updated Answer: No

Does this platform restrict the exercise of a dignified human life?

- Original Answer: No
- Updated Answer: No

- Will this platform reduce the chance of life choices (e.g. nudges) of individuals in ways they are not fully aware of?
    - Original Answer: No
    - Updated Answer: No

Does this platform seek to change the way in which individuals' reason?

- Original Answer: Maybe, some services can promote healthy habits when used in applications for end users
- Updated Answer: No

- Will this platform restrict access to information?
    - Original Answer: The GK platform allow to owner to restrict and anonymize information if they want

    - Updated Answer: The GK platform includes data anonymization and data pseudonymization tools made available to pilot owners. No restriction of access to personal information is generated despite of this, as individuals can still exercise their data subject rights vis-à-vis the data controller (pilot owner). Furthermore, the platform is currently developing tools for synthetic data generation, which further reduces risk of unauthorized data disclosure

- Will this platform promote specific decision-making schemes the users will not be aware of?
    - Original Answer: No
    - Updated Answer: No, all participants in the GK platform, pilots and project-related activities are made aware of any AI-based processing to be performed during the course of the project, all processing activities are under direct human oversight

Does this platform alter the exercise of human moral conscience?

- Will this platform promote specific visions of a good life?
    - Original Answer: Maybe, some services can promote healthy habits when used in applications for end users
    - Updated Answer: No, the platform and applications developed present the user with relevant information regarding their health and seek to promote healthy habits, this however has no impact on the exercise of human moral conscience

Is this platform explicitly designed to create or exacerbate inequalities between individuals or groups?

- Are expected benefits divided between groups for reasons not associated with differences in use?
    - Original Answer: No
    - Updated Answer: No

Is this platform intended to create tiers of persons on the basis of social, international, or political factors?

    - Original Answer: No
    - Updated Answer: No

- Does this limit the rights of any individuals or groups based upon race?
    - Original Answer: No
    - Updated Answer: No
- Does this limit the rights of any individuals or groups based upon biological sex?
    - Original Answer: No
    - Updated Answer: No

Does this platform restrict the enjoyment of basic human rights?

    - Original Answer: No

    - Updated Answer: No, it seeks to ensure the enjoyment and adoption of adequate standards for health and well-being
- Does this limit the natural life of an individual?
    - Original Answer: No
    - Updated Answer: No
- Is this designed to enhance or augment the natural life of an individual?
    - Original Answer: No
    - Updated Answer: No
- Does this restrict an individual's opportunity to exercise liberties?
    - Original Answer: No
    - Updated Answer: No

3.6 Partner ethical risk assessment results

The following section summarizes the result of the risk assessments provided by GATEKEEPER partners. A final ethical risk assessment will be introduced in the final version of this deliverable.

3.6.1 GK1 - Respect for confidentiality and privacy

During the initial risk assessment, the partners identified a number of concerns regarding the privacy of not only the partners, stakeholders and researchers, but also the participants to the pilots, the recipients of communication, final users and patients.

In particular, the majority of partners recognised the legal basis of **consent as a sensitive matter with multiple privacy implications** for all parties involved. Taking into consideration that consent will form the legal basis for a multitude of processing activities involved, as participation in the program will be constructed on a voluntary basis, it is of utmost importance to the partners that sufficient safeguards are placed with regards to the legitimacy of the consent provided. As expected, the same issue was raised in relation to recipients of communication, such as via newsletter subscriptions, social media communications etc, given that no such communication shall be initiated without the recipients' explicit consent.

In response to that, the partners have already incorporated several measures in their practices, including requesting consent prior to the collection and processing of the data, as well as ensuring that consent is specific, informed, given freely with an unambiguous indication of the data subjects' wishes.

Based on the above, it is additionally advised that the partners adapt their strategies to the **following recommendations** so as to eliminate the risks posed by consent as a legal basis as much as possible:

1. The partners should ensure that the participants providing their health data explicitly and clearly consent to the collection and processing. In that context, there could be a separate disclaimer providing the information required for an informed and specific consent, with a direct and distinguishable option to declare their consent.

2. The partners should balance the need to request separate consent for each specific purpose with the need to combat the so-called "click fatigue", i.e. the fatigue caused by having to read through and click multiple options to be able to proceed to the use of a program or application, that could lead to a reckless acceptance of all terms, without studying them.
3. Nonetheless, in particular for personal data that will be used for scientific purposes, the specific consent must be distinguishable.
4. Withdrawal of consent should always be possible, without detriment to the data subject. Partners should ensure that once consent is withdrawn, collection and processing of data ceases entirely, while a balancing assessment should be carried out on whether data already collected should be anonymised or pseudonymised or deleted entirely.
5. The information provided to the participants must also include the anticipated results in case of withdrawal of consent.
6. The partners must ensure that they have acquired prior consent that meets the above criteria specifically for data transfers when such transfers are to be performed.
7. National legislations should be taken into account when applying data protection legislation.

Additionally, partners have deemed that additional **data protection principles** should be further examined, including the need for data minimisation, encryption of personal data collected, pseudonymisation and anonymisation, a privacy by design approach, where possible, as well as access limitations to data, implementing security measures such as an Access control system, Encryption at Rest and VPN protocols, users' authentication procedures and a secure data storage system, among others.

On the above subjects, the partners have identified that the **following measures** should be taken to further enhance their data protection compliance:

1. Partners should ensure that access to personal data is strictly limited to the parties necessary to accomplish the predetermined purposes envisioned.
2. Partners should ensure that data is anonymised and/or pseudonymised where that is possible to further protect the privacy of data subjects.
3. Data collected and processed should be limited to the necessary to meet the envisioned purposes. Limitations should also be placed to the retention period of such data.
4. Partners should consider storing biometric data, where that is collected, only to the users' local devices and not to a server.
5. In order to comply with any requests of access of the participants without facing any issues, it is recommended that data collected is stored in a layered manner.
6. Partners should perform a Data Protection Impact Agreement (hereafter DPIA) prior to the commencement of the project. Said DPIA must be frequently reviewed and maintained up to date.
7. A Data Processing Agreement must be signed, including a precise and clear list of conditions and criteria for the activities in question.
8. A robust cryptography system must be implemented to protect the security of data collected, especially when data transfers are to take place.

3.6.2 GKP2 – Beneficence

Upon this preliminary examination of the **projects' ethical standards and its impact on the participants' well-being**, the partners' main concerns revolved around providing participants' sufficient information so that they comprehend fully the benefits and any potential risks involved in the project. Taking into consideration the nature of the program, the main goal of the partners is always to improve the users' and participants' well-being and health status as much as possible.

In view of that, the partners have already put in place **multiple information points**, not only at the stage of enrolment to the program, but also throughout its duration and at sufficient frequency, also using certified medical devices. Additionally, they have established **contact points** so that participants can be provided any clarifications they desire easily and uninterruptedly. Where applicable, the partners intend to implement **quality management policies** as provided by ISO 13485 and IEC 62304 standards for medical software.

Last but not least, the partners, when designing the platforms, intend to enable **customisation of the care plan** in accordance with the participants' health status, needs and welfare, thus adopting a **person-centred care approach**. In order to maximise efficiency to the participants' benefit, partners also plan to provide constant technical support to healthcare professionals so as to best utilise the platforms.

3.6.3 GKP3 - Justice

This initial risk assessment demonstrated that the partners have already identified the need for **fair criteria of participation in the program**, paying particular attention to **gender equality** and **facilitating the use of the platforms** for elder citizens who may have more limited digital literacy.

To ensure the above, the partners have taken a series of measures, including disclose of gender by the participants on a voluntary basis, without it having any impact on the selection criteria. The selection criteria, on the other hand, will be predetermined, based on the needs of the program. Moreover, the evaluation process is to be carried out by independent experts, chosen on the basis of their expertise and gender equality. Even on a researchers' level, the partners intend to reform any imbalanced groups that will be established, to achieve further gender equality.

Furthermore, the partners intend to integrate features and design elements to their respective platforms that would enhance accessibility and usability, especially for older citizens. For this purpose, the partners will be providing to the data subjects sufficient information of operations prior to participation, in a clear and comprehensible language.

In addition to the above, it is recommended that the partners take into consideration the following **additional measures**:

1) It is essential that partners take into consideration the target group of the information that will be provided at each stage, so as to make any language and/or comprehension adjustments necessary.
2) Partners should ensure that their platforms are accessible for every individual meeting the requirements that will be decided in accordance with the platforms' purposes and intended use. This means that access must be guaranteed also for individuals with disabilities or limited abilities that could prevent them from using

the platforms. For instance, a voice assistant feature would significantly improve access for sight-impaired citizens. Of course, additional privacy safeguards must also be placed in this case.

3) The criteria for participation must not indirectly and unjustifiably limit certain groups from accessing the platforms and the pilots.
4) Frequent checks on the platforms' usability must be performed, ensuring a smooth user experience.
5) Partners should take additional safeguards to ensure that data collected remains accurate, providing the possibility to users to rectify any erroneous information.
6) An effective technical support channel should be implemented, capable of assisting citizens with the use of the platforms, providing sufficient guidance and ensuring that any technical issues that may arise are settled within a reasonable timeframe.

3.6.4 GKP4 - Respect for Persons

When examining the program's adherence to the principle of respect for persons, the partners mainly focused on two elements of potential risks, **supply of sufficient information** and **voluntary participation** in the project.

As a result, the partners have already ensured that participants will have access to all the **information** required to provide consent for the participation to the program, the criteria for participation, the implementation of the projects, the use of platforms, as well as the expected outcomes of their participation. All the above is to be provided in a clear and comprehensible manner to the participants in a language they understand, prior to their participation and any other time they require. Input from previous users shall also be included so that participants have a first-hand view of the experience.

Additionally, they have designed their programs, pilots and/or platforms on the basis of **voluntary participation**. As long as an individual meets the requirements, they have the option to participate, as well as withdraw at any time without detriment.

At the same time, the partners recognised that the **same level of respect must be ensured for the recipients of communication,** whether that is through email or social media, abiding by adequate ethical standards.

In view of the above, **partners are welcomed to**:

a) Provide the above-described information through various means, including in writing, but also orally.
b) The information provided to the participants should include a sufficient description of the ways in which consent can be withdrawn and the participation to the programs ceased. It should also include a thorough explanation of the results of the withdrawal regarding their data, actions already taken etc.
c) Health practitioners participating in the program must also abide by ethical standards and respect participants.
d) Health practitioners participating in the program are advised to also provide in person the above-described information revolving around the participation to the program when directly approached by individuals.

3.6.5 GKP5 - Transparency

Regarding transparency, the partners developed a two-fold approach, **transparency of the project as a whole** and **transparency particularly in cases of employing AI systems**.

As far as open-call **participants** to the pilots are concerned, the partners identified the need to provide a clear image of the evaluation criteria once the calls are open, as well as performing the evaluation process in a fully transparent manner.

At the same time, partners intend to host tailored events to **increase awareness** regarding the project. In any case, the detailed description of the project, its goals and data flow will be included in the **information** provided for the participants to validly consent to the participation. Of course, the **contact points** already established will be in a position to effectively respond to any doubts, clarify any points and, in general, ensure that participants have the full picture of the project.

In order to fulfil the above, the partners have additionally included **tools and mobile phone applications** that will provide further support to and empower both the participants, and healthcare professionals access and use the platforms effectively. In this way, the information provided will be actually put in practice, leaving the theoretical realm and assisting all parties to benefit from the project's full potential.

The partners have also established open communication channels among them, to ensure **transparency on an organisational level,** based on open communication principles. As a result, partners will be in the position to effectively review the total procedures performed. The DPO remains an effective point of contact for the partners, providing further guidance where necessary.

Moreover, they recognised that **the use of AI in the platforms** could incur a number of transparency risks, taking into consideration the nature of AI systems and their decision-making process. To minimise said risks, partners have already implemented Internal Data and AI governance processes in compliance with all relevant guidelines on the subject, including the AI Act, SPIRIT AI, the guidance of the World Health Organisation, the Open Science rules etc. In addition to that, partners also intend to perform heuristic evaluations with both experts and end-users to ensure transparent information access.

In addition to the above, partners plan to provide participants, users, and patients with detailed information about how, why and which of their data are being collected, processed and retained, as well as the retention periods. What is more, they intend to perform clear and complete data and analytics visualisations in order for data subjects to best comprehend procedures that would otherwise remain rather obscure.

In any case, taking into consideration the use of AI and the collection and processing of sensitive personal data, it is always **recommended that a Data Protection Impact Assessment be performed and published** for increased transparency. Of course, it is not necessary that the entire DPIA is published, but it can include either a summary or certain parts that are deemed most crucial for the data subjects.

Certification may also be considered as a valuable asset aiming at enhancing participants' trust in the systems, techniques and platforms employed and adding to the safeguards already at place.

3.6.6 GKP6 - Sustainability

Upon assessing the sustainability of the project, partners addressed both the impact on the participants and the E.U. community and the potential environmental impact,

designing it entirely in a manner that will not cause harm, in accordance with fair and reasonable exploitation principles.

In view of that, the partners have adopted a **responsible research and innovation approach**, emphasising value dynamics and value conflicts, encouraging **participants** to share all impact related to sustainability considerations, whether positive or negative.

For that purpose, **impact assessments** will be performed throughout the lifecycle of the project to review the precise influence of proposed solutions to the participants' daily lives. The knowledge acquired on all sectors, including exploitation, communication, replicability and growth, is to be shared with the rest of the stakeholders to ameliorate any parts required.

What is more, the partners bear the responsibility to increase awareness and visibility of the project, so as to maintain its benefits for the participants in the long run. Besides, the project is designed to withstand any potential future barriers, being **adaptable to changes** and constantly kept **up to date with emerging technologies**.

Upon the finalisation of the project, a **DPIA** is to be performed that would effectively recognise and minimise any long-term data protection risks, ensuring that the non-intrusive design of the tools is maintained.

On the **environmental front**, partners have actively demonstrated their commitment to respect the natural environment and reduce climate change effects. Certain partners have even joined actions against climate change in line with European and global standards and environmental agendas, aiming at achieving climate neutrality by 2040. Finally, partners have favoured the use of electronic Case Report Forms (e-CRF) over paper format archives to collect patient information reducing any potentially negative environmental impact.

3.7 Findings

Ethical compliance actions undertaken thus far have showcased both the strengths of the GATEKEEPER platform and the potential risks to be addressed in the final stages of the project. Given the identified issues and risks, a number of mitigation actions are proposed for their implementation at a partner and pilot level. Cross-partner communication is of particular concern towards ensuring timely reporting of compliance activities. A specific mitigation action has been proposed in the form of the project-wide slack-based communication platform, which is presented in section 6 of this deliverable.

4 Legal Aspects in GATEKEEPER

4.1 Introduction

The following sections will present a summary of the key requirements and recommendations **to be necessarily considered by all project partners** (and particularly by the pilot owners in their role as data controllers) towards ensuring the compliance of all GATEKEEPER-related activities. These elements **shall be reported by the project partner to the project Ethics legal and gender issues manager** who will ensure the coordinated implementation and reporting of compliance actions across the project.

4.2 International and European Instruments in the field of Data Protection

The legal instruments concerning the right to data protection are available both under the Council of Europe and the European Union legal framework. The first covers the right to data protection with the article 8 of the European Convention of Human Rights (from now on ECHR), which guarantees the right to respect private and family life, home and correspondence, and with a specific Convention (known as Convention 108+) for the Protection of Individuals with regard to Automatic Processing of Personal Data. Entered into force in 1985 and modernized in 2018, the Convention establishes all the key principles of a lawful data processing and concerns the automatic data processing, although Member Countries could apply the same rules to non-automatic data processing. In the specific area of health data, art. 6 states that this kind of data can be automatically processed only if the national law defines adequate safeguards. In the area of soft law, in 1999 the Council of Europe adopted a Recommendation on the Guidelines for the protection of privacy information highways, matching the principle affirmed by the European Union legal instruments, such as the duty for the users to use digital signature and encryption techniques, the duty on internet service providers to use certified privacy enhancing technologies, to ensure data confidentiality and integrity, in addition to logical and physical security of the network. Information about the privacy settings implemented by the service providers is also mandatory, and with regard to medical data, it is established that the communication of these sensitive data for marketing purposes requires the previous informed and explicit consent of the data subject.

The European Union legal framework in the field of data protection is primarily made by the Charter of Fundamental Rights (legally binding from the 2009), which, unlike the ECHR, dedicates two separate articles to the right of privacy and the right of data protection, providing a specific legal basis. Indeed, article 8 of the Charter sets out the requirement of a lawful processing of personal data: it has to be fair, realized for specified purposes and based on the consent of data subject or other legitimate basis laid down by the law. Furthermore, the person concerned has the right to access date and the right to have it rectified. Finally, compliance with these rules has to be controlled by an independent authority.

The international legal framework is enriched with the soft law instrument produced by the Organization for Economic Cooperation and Development (OECD), that form the early stage, actively contributed to the protection of data on the Internet, as well as the protection of consumer rights in the context of e-commerce. Since 1980, OECD issued guidelines, recommendations governing the protection of privacy and participating to the definition of the fundamental principles as well as the best practices in this field.

Recently, the legal panorama of the European Union in the area of data protection has been completely modernized with the approval of two different pieces of legislation, having the purpose to enable people to better control their personal data in the new age of digital economy: the General Data Protection Regulation (from now on GDPR) and the Data Protection Law Enforcement Directive (DPLE Directive). The GDPR strengthens the individual right to data protection, at the same time facilitating the compliance with the new normative structure for the companies in the Digital Single Market. The key features of the GDPR cover: easier access to personal data, the right to data portability, the right "to be forgotten", the right to know when the data has been hacked, the principle of clear and affirmative consent to the processing of personal data, an increasing responsibility on data controller and data processor, the principles of "data processing by design" and "data processing by default" and a stronger enforcement of the rules through improved judicial and administrative remedies in case of violation.

Moreover, the European legal landscape has recently been altered following the UK's withdrawal from the European Union. In particular as far as data protection is concerned, it is a fact that the UK is no longer bound by the EU GDPR as of January 1st, 2021. However, the GDPR had already been transposed in the UK legal order in virtue of Data Protection Act 2018, as was further enshrined by the Data Protection, Privacy and Electronic Communications Regulations 2019, thus providing an adequate protective framework for the data subjects. In any case, when UK organisations/enterprises offer good or services or collect and process the data of EU residents, they will need to ensure compliance with the European GDPR, as it stands. In addition, and in spite of the UK's withdrawal from the EU, it remains bound by the ECHR, Convention 108+ and its international obligations. Nonetheless, the Charter of Fundamental Rights will no longer apply in the UK, as set out in the EU Withdrawal Act.

4.2.1 GDPR-Specific dispositions

The GDPR includes a number of specific dispositions of particular relevance towards the use of Personal Data for Scientific Research Purposes, namely:

- **Art. 89 GDPR - Safeguards and derogations relating to processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes:** "Processing for (…) scientific (…) research purposes (…) shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner. Where personal data are processed for scientific (…) research purposes (…) Union or Member State law may provide for derogations from the rights referred to in Articles 15, 16, 18 and 21 subject to the conditions and safeguards referred to in paragraph 1 of this Article in so far as such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes. (…) Where processing referred to in paragraphs 2 and 3 serves at the same time another purpose, the derogations shall apply only to processing for the purposes referred to in those paragraphs.
- **Recital 78**: "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. The principles of data protection by design and by default should also be taken into consideration in the context of public tenders."

- **Recital 156:** "The processing of personal data for (…) scientific (…) research purposes (…) should be subject to appropriate safeguards for the rights and freedoms of the data subject pursuant to this Regulation. Those safeguards should ensure that technical and organisational measures are in place in order to ensure, in particular, the principle of data minimisation. The further processing of personal data for (…) scientific (…) research purposes (…) is to be carried out when the controller has assessed the feasibility to fulfil those purposes by processing data which do not permit or no longer permit the identification of data subjects, provided that appropriate safeguards exist (such as, for instance, pseudonymisation of the data). Member States should provide for appropriate safeguards for the processing of personal data for (…) scientific (…) research purposes (…). Member States should be authorised to provide, under specific conditions and subject to appropriate safeguards for data subjects, specifications and derogations with regard to the information requirements and rights to rectification, to erasure, to be forgotten, to restriction of processing, to data portability, and to object when processing personal data for (…) scientific (…) research purposes (…). The conditions and safeguards in question may entail specific procedures for data subjects to exercise those rights if this is appropriate in the light of the purposes sought by the specific processing along with technical and organisational measures aimed at minimising the processing of personal data in pursuance of the proportionality and necessity principles. The processing of personal data for scientific purposes should also comply with other relevant legislation such as on clinical trials."
- **Recital 157:** "By coupling information from registries, researchers can obtain new knowledge of great value with regard to widespread medical conditions such as cardiovascular disease, cancer and depression. On the basis of registries, research results can be enhanced, as they draw on a larger population. Within social science, research on the basis of registries enables researchers to obtain essential knowledge about the long-term correlation of a number of social conditions such as unemployment and education with other life conditions. Research results obtained through registries provide solid, high-quality knowledge which can provide the basis for the formulation and implementation of knowledge-based policy, improve the quality of life for a number of people and improve the efficiency of social services. In order to facilitate scientific research, personal data can be processed for scientific research purposes, subject to appropriate conditions and safeguards set out in Union or Member State law."

- **Recital 159**: "**Where personal data are processed for scientific research purposes, this Regulation should also apply to that processing**. For the purposes of this Regulation, the processing of personal data for scientific research purposes should be interpreted in a broad manner including for example technological development and demonstration, fundamental research, applied research and privately funded research. In addition, it should take into account the Union's objective under Article 179(1) TFEU of achieving a European Research Area. Scientific research purposes should also include studies conducted in the public interest in the area of public health. To meet the specificities of processing personal data for scientific research purposes, specific conditions should apply in particular as regards the publication or otherwise disclosure of personal data in the context of scientific research purposes. If the result of scientific research in particular in the health context gives reason for further measures in the interest of the data subject, the general rules of this Regulation should apply in view of those measures."
- **Recital 161 Consenting to the Participation in Clinical Trials:** "For the purpose of consenting to the participation in scientific research activities in clinical trials, the relevant provisions of Regulation (EU) No 536/2014 of the European Parliament and of the Council should apply."

4.2.2 Relevant EDPB Guidelines and Recommendations:

4.2.2.1 Article 29 Data Protection Working Party - *Guidelines on Data Protection Officers ('DPOs') (wp243rev.01) (10/2017)*

The GDPR recognises the Data Protection Officer (hereafter DPO) as a key player in the new data governance system and has laid down a specific set rules on the data controllers and processors' obligation to appoint one. The aim of the Article 29 Data Protection Working Party's (hereafter WP29) guidelines is to provide clarifications on the matter and ensure controllers and processors' compliance, as well as assist the DPOs in their role.

Table 2: Obligation to designate a DPO

Categories of controllers and processors	Definitions	Obligation to appoint a DPO
All public authorities and bodies (irrespective of what data they process)	To be determined under national law. Public authorities and bodies usually include national, regional and local authorities, but the concept, typically also includes a range of other bodies governed by public law.	Mandatory
	Other natural or legal persons governed by public or private law, in sectors such as, public transport services, water and energy supply, public service broadcasting etc may place data subjects in a similar situation to when their data are processed by a public authority or body.	Recommended, as a good practice

Other organisations that - as a core activity - monitor individuals systematically and on a large scale, **or that process special categories of personal data** on a large scale	"Core activities" can be considered as the key operations necessary to achieve the controller's or processor's goals. It should not be interpreted as excluding activities where the processing of data forms an inextricable part of the controller's or processor's activity. E.g., **The core activity of a hospital is to provide health care. However, a hospital could not provide healthcare safely and effectively without processing health data, such as patients' health records. Therefore, processing these data should be considered to be one of any hospital's core activities and hospitals must therefore designate DPOs.**	Mandatory
	Determining whether the processing is carried out on a "large scale" should take into consideration several factors, such as the number of data subjects, the volume and range of data processed, the geographical extent of the activity etc, that may include processing of patient data in the regular course of business by a hospital.	Mandatory
On a voluntary basis, even if the GDPR does not specifically request for it.	Unless it is obvious that an organisation is not required to designate a DPO, the WP29 recommends a documented internal analysis is carried out to determine whether or not a DPO is to be appointed, proving that the relevant factors have been taken into account properly.	Recommended, as a good practice

Appointment of a single DPO from a group of undertakings: It is possible for multiple parties to appoint one single DPO, provided that the DPO is easily accessible from each establishment both physically and in terms of communication. For this purpose, it is recommended that the DPO be located where they can carry out their activities more effectively, whether within or out of the E.U.

Qualities of a DPO: The DPO must possess a high level of expertise in the field of data protection, comprehending the sensitivity, complexity, and amount of data an organisation process. In order to be able to fulfil their tasks, expertise is also required in national and European data protection laws and practices, as well as an in-depth understanding of the GDPR, knowledge of the business sector and of the organisation, sound knowledge of the administrative rules and procedures of the organisation. If the DPO is appointed on the basis of a service contract, there must be a clear allocation of tasks within the DPO team.

Provisions as to the DPOs' responsibilities:

- The DPO is bound by secrecy and confidentiality when performing their tasks
- The DPO should be consulted at the outset, to facilitate compliance and promote a privacy by design approach
- The data protection function must be effective and sufficiently well-resourced in relation to the data processing being carried out. The more complex and/or sensitive the processing operations, the more resources must be given to the DPO

- The DPO must be autonomous. DPOs must not be instructed how to deal with a matter, what result should be achieved, how to investigate a complaint or whether to consult the supervisory authority. Furthermore, they must not be instructed to take a certain position in an issue related to data protection legislation, for example, a particular interpretation of the law. The autonomy of DPOs does not, however, mean that they have decision-making powers extending beyond their tasks pursuant to Article 39. The controller or processor remains responsible for compliance with data protection law and must be able to demonstrate compliance
- Penalties are prohibited if they are imposed as a result of the DPO carrying out his/her duties as a DPO

Tasks of the DPO:

1) Monitoring compliance with the GDPR. The DPO may collect information to identify processing activities, analyse and check compliance, inform, advise and issue recommendations to the controller or processor.
2) Providing advice, where requested, as regards the Data Protection Impact Assessment (hereafter DPIA) and monitor its performance pursuant to Article 35. The WP29 recommends that the controller should seek the advice of the DPO on all matters involving DPIAs.
3) Acting as a facilitator. The DPO acts as a contact point to facilitate access by the supervisory authority to the documents and information for the performance of their tasks, as well as for the exercise of its investigative, corrective, authorisation, and advisory powers
4) Create inventories and hold a register of processing operations based on information provided to them by the various departments in their organisation responsible for the processing of personal data, as has been established under multiple national laws of the member states.

4.2.2.2 Article 29 Data Protection Working Party - *Data Protection impact assessments High risk processing (10/2017)*

A DPIA is a process designed to describe the data-processing, assess its necessity and proportionality, and help manage the risks to the rights and freedoms of natural persons by assessing them and determining the measures to address them.

The DPIA is required when the processing is "likely to result in a high risk to the rights and freedoms of natural persons". "The rights and freedoms" of data subjects primarily concerns the rights to data protection and privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience, and religion.

The WP29's guidelines seek to promote the development of:

A) A common European Union list of processing operations for which a DPIA is mandatory

- Evaluation or scoring, including profiling, and predicting, in particular involving "aspects concerning the data subject's performance at work, economic situation, **health**, personal preferences or interests, behaviour, location or movements".
- Automated decision-making with legal or similar significant effect, i.e. data processing leading to decisions on data subjects producing legal effects concerning the natural person or which similarly significantly affects them.

- **Sensitive data or data of a highly personal nature. This includes special categories of personal data as defined in Article 9 of the GDPR. For instance, a general hospital keeping patients' medical records would fall under this category.**
- Data processed on a large scale, as already defined.
- **Matching or combining datasets, originating from two or more data processing operations performed for different purposes and/or by different data controllers** in a way that would exceed the reasonable expectations of the data subject.
- Data concerning vulnerable data subjects, such as minors.
- **Innovative use or applying new technological or organisational solutions**, like combining use of fingerprint and face recognition for improved access control, etc. For example, **certain "Internet of Things" applications** could have a significant impact on individuals' daily lives and privacy, and, therefore, would require a DPIA.
- When the processing in itself "prevents data subjects from exercising a right or using a service or a contract". This includes processing that aims at allowing, modifying or refusing data subjects' access to a service or entry into a contract.
- A DPIA can also be useful for assessing the data protection impact of a technology product, for example a piece of hardware or software, where this is likely to be used by different data controllers to carry out different processing operations.

In most cases, a data controller can consider that a **processing meeting at least two criteria would require a DPIA** to be carried out. Nonetheless, that should be examined on an ad hoc basis, as in some cases, a data controller can consider that a processing meeting only one of these criteria requires a DPIA. Conversely, a processing operation may correspond to the above-mentioned cases and still be considered by the controller not to be "likely to result in a high risk". In such cases the controller should justify and document the reasons for not carrying out a DPIA, as well as recording the views of the DPO.

The WP29 also focuses on providing examples of cases meeting the above criteria. For instance, storage for archiving purpose of pseudonymised personal sensitive data concerning vulnerable data subjects of research projects or clinical trials involves sensitive data, concerning vulnerable data subjects and prevents data subjects from exercising a right or using a service or a contract. Therefore, a DPIA would be required.

The mere fact that the conditions triggering the obligation to carry out a DPIA have not been met does not, however, diminish controllers' general obligation to implement measures to appropriately manage risks for the rights and freedoms of data subjects.

B) A common EU list of processing operations for which a DPIA is not necessary

- Where the processing is not "likely to result in a high risk to the rights and freedoms of natural persons".
- When the nature, scope, context and purposes of the processing are very similar to the processing for which DPIA have been carried out.
- When the processing operations have been checked by a supervisory authority before May 2018 and their specific conditions have not changed.
- Where a processing operation, pursuant to point (c) or (e) of Article 6 par. 1 GDPR, has a legal basis in EU or Member State law, where the law regulates the specific processing operation and where a DPIA has already been carried out as part of the establishment of that legal basis.

- Where the processing is included on the optional list, established by the supervisory authority, of processing operations for which no DPIA is required.

C) Common criteria on the methodology for carrying out a DPIA

- The DPIA should be carried out **"prior to the processing"**, starting as early as is possible even if some of the processing operations remain unknown. The fact that the DPIA may need to be updated once the processing has officially commenced does not constitute a valid reason for postponing or not carrying out a DPIA.
- **Updating the DPIA throughout the lifecycle project is required to maintain compliance**.
- **The controller is responsible for ensuring that the DPIA is carried out.** If the processing is wholly or partly performed by a data processor, the processor should assist the controller in carrying out the DPIA and provide any necessary information.
- The controller must also **seek the advice of the Data Protection Officer (DPO),** where designated and this advice, along with the decisions taken by the controller, should be documented within the DPIA. The DPO should also monitor the performance of the DPIA.
- The controller must "seek the views of data subjects or their representatives", "where appropriate".
- A DPIA must at least include "a description of the envisaged processing operations and the purposes of the processing", "an assessment of the necessity and proportionality of the processing", "an assessment of the risks to the rights and freedoms of data subjects", "the measures envisaged to address the risks and "to demonstrate compliance with the GDPR".
- Compliance with a code of conduct must be taken into account when assessing the impact of a data processing operation. Certifications, seals and marks aiming at demonstrating compliance with the GDPR of such operations by controllers and processors, as well as Binding Corporate Rules, should also be considered.
- The DPIA implementation is scalable, in the sense that even a small data controller can design and implement a DPIA suitable for their processing operations.

D) Common criteria for specifying when the Supervisory Authority shall be consulted

- Where a DPIA reveals high residual risks, the data controller will be required to seek prior consultation for the processing from the supervisory authority.
- Whenever Member State law requires controllers to consult with, and/or obtain prior authorisation in relation to processing by a controller for in the public interest, including processing in relation to social protection and public health.

E) Recommendations, where possible, building on the experience gained in EU Member States

- Where it is not clear whether a DPIA is required, the WP29 recommends that it is carried out nonetheless as it is a useful tool in controllers' path to compliance with data protection requirements.
- **Publishing a DPIA is not a legal requirement of the GDPR**. However, controllers should consider publishing at least parts, such as a summary or a conclusion of their DPIA, to help foster trust in the controller's processing operations and demonstrate accountability and transparency.

The WP29 confirms that a **single DPIA could be used to assess multiple processing operations that are similar in terms of nature, scope, context, purpose, and risks,** for instance because similar technology is used to collect the same tupe of data for the same purposes. This may also be applicable to similar processing operations implemented by various data controllers. In those cases, a reference DPIA should be shared or made publicly accessible, measures described in the DPIA must be implemented, and a justification for conducting a single DPIA must be provided. Moreover, the said DPIA should set out which party is responsible for the various measures mentioned, while each data controller should express their needs and share useful information without either compromising secrets or disclosing vulnerabilities.

Finally, the WP29 proposes a **list of criteria** in Annex 2, which data controllers can use to assess whether or not a DPIA, or a methodology to carry out a DPIA, is sufficiently comprehensive to comply with the GDPR, namely:

- ☐ a systematic description of the processing is provided (Article 35(7)(a)):
  - ☐ nature, scope, context and purposes of the processing are taken into account (recital 90)
  - ☐ personal data, recipients and period for which the personal data will be stored are recorded
  - ☐ a functional description of the processing operation is provided
  - ☐ the assets on which personal data rely (hardware, software, networks, people, paper or paper transmission channels) are identified
  - ☐ compliance with approved codes of conduct is taken into account (Article 35(8));
- ☐ necessity and proportionality are assessed (Article 35(7)(b)):
  - ☐ measures envisaged to comply with the Regulation are determined (Article 35(7)(d) and recital 90), taking into account:
    - ☐ measures contributing to the proportionality and the necessity of the processing on the basis of:
      - ☐ specified, explicit and legitimate purpose(s) (Article 5(1)(b))
      - ☐ lawfulness of processing (Article 6)
      - ☐ adequate, relevant and limited to what is necessary data (Article 5(1)(c))
      - ☐ limited storage duration (Article 5(1)(e))
    - ☐ measures contributing to the rights of the data subjects:
      - ☐ information provided to the data subject (Articles 12, 13 and 14)
      - ☐ right of access and to data portability (Articles 15 and 20)
      - ☐ right to rectification and to erasure (Articles 16, 17 and 19)
      - ☐ right to object and to restriction of processing (Article 18, 19 and 21)
      - ☐ relationships with processors (Article 28)
      - ☐ safeguards surrounding international transfer(s) (Chapter V)
      - ☐ prior consultation (Article 36).
- ☐ risks to the rights and freedoms of data subjects are managed (Article 35(7)(c)):

- ☐ origin, nature, particularity and severity of the risks are appreciated (cf. recital 84) or, more specifically, for each risk (illegitimate access, undesired modification, and disappearance of data) from the perspective of the data subjects:
  - ☐ risks sources are taken into account (recital 90)
  - ☐ potential impacts to the rights and freedoms of data subjects are identified in case of events including illegitimate access, undesired modification and disappearance of data
  - ☐ threats that could lead to illegitimate access, undesired modification and disappearance of data are identified
  - ☐ likelihood and severity are estimated (recital 90)
- ☐ measures envisaged to treat those risks are determined (Article 35(7)(d) and recital 90)
- ☐ interested parties are involved:
  - ☐ the advice of the DPO is sought (Article 35(2))
  - ☐ the views of data subjects or their representatives are sought, where appropriate (Article 35(9))

4.2.2.3 Guidelines on Automated individual decision-making and Profiling for the pu*rposes of Regulation 2016/679 (wp251rev.01)*

With automated decision-making expanding more and more into everyday life, it is, not surprising that profiling and automated decision-making can pose significant risks for individuals' rights and freedoms, thus requiring appropriate safeguards. As such processes can be opaque, they can perpetuate existing stereotypes and social segregation, leading to inaccurate predictions or restricting a data subject with regards to certain products or services. The purpose of the present Guidelines is to provide necessary clarifications concerning the aspects of this emerging sector. In particular, it is focused on the following:

Table 3: Definitions of profiling and automated decision-making and the GDPR approach to these in general

I. Definitions of profiling and automated decision-making and the GDPR approach to these in general	
Profiling elements:	**Automated decision-making**
• it must be an automated form of processing	The ability to make decisions by technological means without human involvement
• it must be carried out on personal data • the objective of the profiling must be to evaluate personal aspects about a natural person, going beyond a mere classification	Can be based on any type of data, such as: • Data provided directly by the individuals concerned (e.g., Responses to a questionnaire) • Data observed about the individuals (e.g., Data collected via an application) • Derived or inferred data such as a profile of the individual that has already been created

	Automated decisions can be made with or without profiling; profiling can take place without making automated decisions.

Table 4: General provisions on profiling and automated decision-making

II. General provisions on profiling and automated decision-making		
Data Protection Principles	**Lawful Basis**	**Rights of the Data Subject**
Lawful, fair and transparent	Consent. Data subjects should have enough information about the envisaged use and consequences of the processing to ensure that any consent they provide represents an informed choice.	Right to be informed. Given the core principle of transparency underpinning the GDPR, controllers must ensure they explain clearly and simply to individuals how the profiling or automated decision-making process works.
Further processing and purpose limitation. Compatibility with the original purposes of the data collection depends on a range of factors, such as the relationship between the purposes, the nature of the data, the impact on the data subjects, potential safeguards etc	Necessary for the legitimate interests pursued by the controller or by a third party. The controller must carry out a balancing exercise to assess whether their interests are overridden by the data subject's interests or fundamental rights and freedoms. It is difficult for controllers to justify using legitimate interests as a lawful basis for intrusive profiling and tracking practices for marketing or advertising purposes.	Right of access. In addition to general information about the processing, the controller has a duty to make available the data used to create the profile, as well as access to information on the profile and details of which segments the data subject has been placed into. The right of access should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property. Where possible, the controller should be able to provide remote access to a secure system which would provide direct access to a data subject's personal data.
Data minimisation, purpose and storage limitation. Controllers should be able to clearly explain and justify the need to collect and hold personal data, as well as consider using aggregated, anonymised or	Necessary to protect vital interests. Examples of this may include profiling that is necessary to develop models that predict the spread of life-threatening diseases or in situations of humanitarian emergencies. In these cases. However, and in principle, the controller can only rely on vital interest	Right to object. Once the data subject exercises this right, the controller must halt the profiling process. The controller may also have to erase the relevant personal data. On the contrary, if they can demonstrate compelling legitimate grounds that override the interests, rights and freedoms of the data subject, they may refuse. In any case, they will need to consider:

pseudonymised data for profiling.	grounds if no other legal basis for the processing is available.	• The importance of the profiling to their particular objective; • The impact of the profiling on the data subject's interest, rights and freedoms, limited to the minimum necessary to meet the objective. • Carrying out a balancing exercise. The burden of proof to show compelling legitimate grounds lies with the controller rather than the data subject.
Accuracy at all stages of the profiling process. Controllers need to introduce robust measures to verify on an ongoing basis that data reused or obtained indirectly is accurate and up to date.	Necessary for the performance of a contract. Controllers may wish to use profiling and automated decision-making processes for reasons of consistency or fairness in the decision-making process or to deliver decisions within a shorter time frame and improve efficiency.	Right to erasure and right to restriction of processing. These rights apply to both the 'input personal data' (the personal data used to create the profile) and the 'output data' (the profile itself or 'score' assigned to the person). The right to restrict processing, in particular, will apply to any stage of the profiling process.
Storage limitation. The controller's retention policy should take into account the individuals' rights and freedoms. The controller should also make sure that the data remains updated throughout the retention period to reduce the risk of inaccuracies.	Necessary for the performance of a task carried out in the public interest or exercise of official authority Necessary for compliance with a legal obligation.	Right to rectification

III. Specific provisions on solely automated decision-making defined in Article 22

Article 22 par. 1 GDPR establishes a general prohibition for decision-making based solely on automated processing, regardless of whether the data subject takes an action regarding the processing of their personal data. In particular, it provides that:

(i) as a rule, there is a general prohibition on fully automated individual decision-making, including profiling that has a legal or similarly significant effect

(ii) there are the following exceptions to the rule, where the decisions are:

- necessary for the performance or entry into a contract

- authorised by Union or Member State law to which the controller is subject, and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests
- based on the data subject's explicit consent

(iii) where one of these exceptions applies, measures must be in place to safeguard the data subject's rights, freedoms and legitimate interests, including at least a way for the data subject to obtain human intervention, express their point of view, and contest the decision. With the emphasis laying on the need for transparency, appropriate procedures should be introduced, as well as measures to prevent errors, inaccuracies or discrimination on the basis of special category data

In that context, any processing likely to result in a high risk to data subjects requires the controller to carry out a DPIA, which is particularly useful for controllers who are unsure whether their proposed activities will fall within the above scope, and, where applicable, what safeguarding measures they must place. As part of the DPIA, the controller should identify and record the degree of any human involvement in the decision-making process and the stage where it takes place.

IV. Children and profiling

The controller must ensure that these safeguards are effective in protecting the rights, freedoms and legitimate interests of children whose data they are processing. Because children represent a vulnerable group of society, organisations should, in general, refrain from profiling them for marketing purposes.

V. Data Protection Impact Assessments and Data Protection Officers

A DPIA can be a useful way for the controller to identify the measures necessary to address the data protection risks involved with the processing.

The Guidelines also provide for a thorough, yet not exhaustive, list of good practice recommendation for controllers who engage in automated decisions, such as:

- Regular quality assurance checks of their systems
- Algorithmic auditing, to ensure proper algorithmic function, refraining from producing discriminatory, erroneous or unjustified results
- Using anonymisation or pseudonymisation techniques in the context of profiling
- A mechanism for human intervention in defined cases
- Certification mechanisms for processing operations
- Codes of conduct for auditing processes involving machine learning
- Ethical review boards to assess the potential harms and benefits to society of particular applications for profiling

- ***Guidelines 3/2019 on processing of personal data through video devices***

With the expansion of video-surveillance, it is recognised that the presence of such tools in the spheres of data subjects' life will affect the individuals' behaviour and choices in their everyday life. De facto, these technologies may limit the possibilities of anonymous movement and anonymous use of services, with data implication resulting to be massive. As such, the guidelines aim at shedding further light into the conditions, legal use of such techniques, as well as relevant data protection provisions, as demonstrated below.

Scope of application: Personal data, meaning data that can directly or indirectly identify a person, especially in cases where they are processed by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, as per Directive E.U. 2018/680. Processing of personal data by a natural person during a purely personal or household activity, which can also include online activity, is out of the scope of the GDPR.

Lawfulness of processing: The purposes of processing must be specified in writing prior to the use of video-surveillance material, and they must:

1) Meet a legal, economic or non-material legitimate interest, unless such interests are overridden by the data subject's interests, fundamental rights and freedoms. The legitimate interest needs to be a real and present issue. The existence of a legitimate interest, as well as the necessity of the monitoring should be reassessed periodically.

   The processing must be necessary and personal data should be adequate, relevant and limited to what is required in relation to the purposes for which they are processed, in accordance with the data minimisation principle.

   Moreover, the controller must balance the interests at play, taking into consideration the extent of impact on the data subject, any potential violations or negative consequences with regard to their interests, fundamental rights and freedoms. Of course, decisions must be made on a case-by-case basis, considering the size of the area under surveillance, the amount of data subjects under surveillance etc.

   Lastly, the data subjects' reasonable expectations must be taken into account. Signs informing the data subject about the video surveillance are not relevant when determining what a data subject objectively can expect.

2) Data can be processed when it is necessary to perform a task carried out in the public interest or in the exercise of official authority vested in the controller.

3) The data subjects must provide their freely given, specific, informed and unambiguous consent, which, as explained, can only serve as the legal basis in exceptional cases.

4) Any disclosure of personal data is a separate kind of processing for which the controller needs to have a legal basis in Article 6 GDPR. A third-party recipient will have to make its own legal analysis, identifying their own legal basis for the processing.

5) Any disclosure of video footage to law enforcement agencies is lawful if it is necessary for compliance with a legal obligation to which the controller is subject.

Processing of special categories of data: Careful consideration should always be given to the data minimisation principle. If a video surveillance system is used to process special categories of data, the data controller must identify both an exception for processing special categories of data under Article 9 of the GDPR and a legal basis under its Article 6.

For instance, when processing biometric data, three criteria must be considered, namely the nature of the data, the means and way of processing, and the purpose of processing. The use of video surveillance including biometric recognition functionality installed by private entities for their own purposes will, in most cases, require explicit consent, without conditioning the access to its services. In such cases, and in order to minimise risks, data controllers must ensure that data extracted from a digital image will not be excessive and will only contain the information required for the specified purpose. Data storage, any cryptographic protective algorithms, as well as all precautions to preserve the availability, integrity and confidentiality of the data processed must be considered.

To this end, the controller shall take measures, such as compartmentalising data during transmission and storage, storing biometric templates and raw data or identity data on distinct databases, encrypting biometric data, defining a policy for encryption and key management, integrating an organisational and technical measure for fraud detection, associating an integrity code with the data (for example signature or hash) and prohibiting any external access to it. Besides, data controllers should proceed to the deletion of raw data (face images, speech signals etc.) and ensure the effectiveness of this deletion. In any case, such measures will need to evolve with the advancement of technologies.

Data subjects' rights that are particularly relevant in video-surveillance cases:

A) *Right to access*: The controller should bear in mind the intrusive nature of the video footage, meaning that in certain cases they should not hand out video footage where other data subjects can be identified. Additionally, there may be cases where the data subject cannot be identified or their request is excessive or manifestly unfounded, and, therefore, the controller cannot comply with the request.

B) *Right to erasure (Right to be forgotten)*: Upon a request, the controller is obliged to erase the personal data without undue delay when they are no longer needed for the purpose for which they were initially stored, or when the processing is unlawful, or when the consent is withdrawn, or where the data subject objects to the processing.

C) *Right to object*: Unless the controller demonstrates compelling legitimate grounds that override the rights and interests of the data subject, the processing of data of the individual who objected must then cease. The controller is obliged to respond to requests from data subjects without undue delay and at the latest within one month.

Transparency and information obligations: The controller must adopt a layered approach, with the first layer of information displaying a warning sign that can sufficiently alert the data subject of the monitoring. The first layer should include the main information as to the surveillance taking place, followed by a second layer, easily accessible, providing the complete information concerning the surveillance, rights etc.

Storage periods and obligation to erasure: Personal data may not be stored longer than what is necessary for the purposes for which the personal data is processed. Whether the personal data is necessary to store or not should be controlled within a narrow timeline.

Technical and organisational measures: Data controllers must have in place sufficient safeguards, ensuring that surveillance measures in place are proportional to the risks to rights and freedoms of natural persons that could result from accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to video surveillance data. They also need to systematically perform overviews of the video-surveillance system, adopting a data protection by design and by default approach. In that context, they need to consider physical security, but also system and data security, as well as access control.

Data Protection Impact Assessment: Where adequate or necessary, the data controllers must proceed to DPIAs to ensure compliance with the data protection legislation.

4.2.2.4 EDPB Guidelines *4/2019 on Article 25 Data Protection by Design and by Default*

Following the implementation of the GDPR, the present Guidelines provide general guidance on the obligation of Data Protection by Design and by Default, as well as on how to effectively implement the data protection principles, listing key design and default elements as well as practical cases for illustration.

Scope of application: Controllers' implementation of Data Protection by Design and by Default based on the obligation in Article 25 of the GDPR.

Data Protection by Design:

a) **Controller's obligation to implement appropriate technical and organisational measures and necessary safeguards into the processing:** Technical and organisational measures and necessary safeguards can be understood in a broad sense as any method or means that a controller may employ in the processing. Being appropriate means that the measures and necessary safeguards should be suited to achieve the intended purpose. When choosing among the various measures, the controller may take the cost of implementation into account, as well as the nature, scope, context and purpose of processing.

b) **Designed to implement the data protection principles in an effective manner and protecting data subjects' rights and freedoms:** They are decided on ad hoc basis and should be sufficiently documented by the controller.

c) **State of the art**: A dynamic concept that cannot be statically defined at a fixed point in time but should be assessed continuously in the context of technological progress.

d) **Risk analysis**: The controller needs to identify the risks to the rights of data subjects incurred by a potential violation of the principles, determining their likelihood and severity, in order to implement measures that will effectively mitigate said risks. Therefore, controllers, although supported by such tools, must always conduct a data protection risk assessment for each specific processing activity at hand and verify the effectiveness of the appropriate measures and safeguards proposed.

e) Data protection by design shall be implemented **at the time of determination of the means for processing, as well as the processing itself**.

Data Protection by Default: The term "by default" when processing personal data, refers to making choices regarding configuration values or processing options that are set or prescribed in a processing system, such as a software application, service or device, or a manual processing procedure, that affect the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. Based on that, controllers should consider both the volume of personal data, as well as the types, categories and level of detail of personal data required for the processing purposes, as well as limiting access, determining the types of access based on an assessment of necessity, while ensuring that personal data is in fact accessible when necessary.

Transparency: Key design and default elements for the principle of transparency may include clarity to the audience in question, accessibility, relevance, universality, should be provided at the relevant time and in the appropriate form, in different channels and media, and should be layered in a manner that resolves the dilemma of completeness and understanding, while accounting for data subjects' reasonable expectations.

Lawfulness: The legal basis of key design and default elements should be predetermined and easily adjusted where necessary, according to the processing conducted, differentiated for each processing activity, and clearly connected to the specific purpose of processing. Such processing must still be necessary to perform the purpose envisioned, while the data subject should be granted the highest degree of autonomy possible, providing and withdrawing their consent freely, specifically and informed. Whenever joint controllership is envisaged, the parties must apportion in a clear and transparent way their respective responsibilities vis-à-vis the data subject and design the measures of the processing in accordance with this allocation.

Fairness: Data subjects must be able to communicate and exercise their rights in respect of the personal data processed. At the same time, processing should correspond to the data subjects' reasonable expectations, must not discriminate nor exploit their needs and vulnerabilities and deceive them, should always balance interests, and utilise fair algorithms. In view of that, regular assessment must take place, incorporating human intervention, while the processing must remain ethical and truthful. Lastly, **data subjects should be thoroughly informed about the functioning of the processing of personal data** based on algorithms that analyse or make predictions about them, especially when it involves **data concerning their health**, personal preferences, behaviour, location etc.

Purpose Limitation: The legitimate purposes must be predetermined and specific, guiding the design of the processing and limiting it to the minimum required. Any new purpose must be compatible with the original purpose for which the data was collected, while reusing and repurposing must remain to a minimum. In view of that, the controller should regularly review whether the processing is necessary for the purposes for which the data was collected.

Data Minimisation: Generally, it is advised to refrain from processing personal data. Where that is not possible, the personal data collected and processed must remain to a minimum, should be relevant and necessary for the purposes, providing access to a minimal number of people according to their duties. When realisable, aggregated data should be used, along with pseudonymisation and anonymisation. The controller should apply up to date and appropriate "state of the art" technologies for data avoidance and minimisation.

Accuracy: Data collected and processed should be sufficiently and measurably accurate, taking into consideration factors such as the reliability of the data source, as well as verification of data, ensuring they are up to date. Controllers should implement technical and organisational measures to decrease inaccuracy and mitigate the effect of an accumulated error, while erasing and/or rectifying inaccurate data without delay. Of course, data subjects should be given information and effective access to personal data to control such accuracy and rectify as needed.

Storage limitation: The controller should have clear internal procedures and functionalities for deletion and/or anonymisation, automatically where possible, without enabling recovery of anonymised/deleted data. The controller shall determine which data and length of storage is necessary for the purpose, back-ups, and logs, justifying their choices. The controller should enforce internal retention policies and conduct tests in accordance with the data flow.

Integrity and confidentiality: The controller must have an information security management system (ISMS) in place, regularly assessing the risks against the security of personal data, maintaining a comprehensive, systematic, and realistic "threat modelling" and an attack surface analysis of the designed software to reduce attack vectors and opportunities to exploit weak points and vulnerabilities. They should opt for a security by design approach, ensuring proper maintenance of the systems, secure transfers, storage and backups/logs, and an adequate security incident response management. Moreover, it should be guaranteed that only authorised personnel have access to the personal data necessary, setting access limitations as to the agents and the content, promoting data segregation, in a way that no individual needs comprehensive access to all data collected about a data subject, much less all personal data of a particular category of data subjects.

Accountability: The controller needs to be able to demonstrate compliance with the principles. To accomplish that, the controller should possess both the knowledge of and the ability to implement data protection. This entails that the controller should understand their data protection obligations under the GDPR and be able to comply with these obligations.

Certification: Certification pursuant to Article 42 GDPR may be used as an element to demonstrate compliance with the Data Privacy by Default and by Design.

Recommendations: Although not directly addressed in Article 25 GDPR, processors and producers are also recognized as key enablers, as controllers are required to only process personal data with systems and technologies that have built-in data protection.

It should be kept in mind that the main design objective is the effective implementation of the principles and protection of the rights of data subjects into the appropriate measures of the processing. Thus, the guidelines recommend the following to all parties involved:

(i) Controllers should bear in mind data protection from the initial stages of planning a processing operation.

(ii) Where the controller has a DPO, they should be actively involved to integrate Data Protection by Design and by Default in the entire processing lifecycle.

(iii) Controllers should consider having processing operations certified, as that serves as a competitive advantage and adds value when choosing between different processing software, hardware, services and/or systems, also guiding data subjects in their choice between different goods and services,

(iv) Controllers, processors and producers, should consider their obligations to provide vulnerable groups with specific protection.

(v) Producers and processors should seek to support the controller's ability to comply with their obligations. Accordingly, controllers, should not choose producers or processors who do not offer systems enabling or supporting the said compliance.

(vi) Producers and processors should be active in ensuring that the criteria for the "state of the art" are met and notify controllers of any changes to the state of the art that may affect the effectiveness of any measures in place. Controllers should even include this requirement as a contractual clause.

(vii) Controllers should require that producers and processors demonstrate how their hardware, software, services or systems enable the controller to comply with the requirements to accountability, for example by using key performance indicators to demonstrate the effectiveness of the measures and safeguards.

(viii) The parties involved should opt for a harmonized approach to implement principles and rights in an effective manner, preparing codes of conduct including sector-specific guidance.

(ix) Controllers should be fair to data subjects and transparent.

(x) Privacy-enhancing technologies with a sufficient state-of-the-art maturity should be employed if appropriate in a risk-based approach, assessing whether the measure is appropriate and effective in enforcing the principles and the rights of data subjects.

(xi) The threshold of requirements for Small and Medium Enterprises (hereafter SMEs) is the same as large enterprises. To facilitate compliance, SMEs are encouraged to perform early risk assessments, start with small processing and slowly progress, cooperating with producers and processors with guarantees.

4.2.2.5 EDPB Guidelines 03/2020 on the processing of data concerning health for the purpose of scientific research in the context of the COVID-19 outbreak

The EDPB recognises that ever since the start of the COVID-19 pandemic, there have been great scientific research efforts in the fight against it, mainly aiming at producing research results as rapidly and as effectively as possible. At the same time, legal questions concerning the use of health data pursuant to Article 4 par. 15 GDPR for such research purposes keep arising. In view of that, the present EDPB Guidelines aim at addressing any relevant concerns, as follows.

Application of the GDPR: It is initially clarified that data protection rules do not hinder measures taken in the fight against the COVID-19 pandemic, although fundamental rights of data subjects must be equally applied when processing health data for the purpose of scientific research. Since neither the Data Protection Rules nor the Freedom of Science pursuant to Article 13 of the Charter of Fundamental Rights of the EU have precedence over the other, these rights and freedoms must be carefully assessed and balanced.

Table 5: Definitions

Data concerning health	Processing for the purpose of scientific research	Further processing
Personal data related to the physical or mental health of a natural person, including provision of health care services, revealing information about their health status.	A research project set up in accordance with relevant sector-related methodological and ethical standards and good practice.	1. Research on personal (health) data which consists in the use of data directly collected for the purpose of scientific studies ("primary use").
Data concerning health can be derived from different sources, such as: - Information collected by a health care provider in a patient record - Information that becomes health data because of its usage in a specific context (such as information regarding a recent trip to or presence in a region affected with COVID-19 processed by a medical professional to make a diagnosis). - Information from a "self-check" survey, where data subjects answer questions	It should take into account the Union's objective under Article 179 par. 1 TFEU of achieving a European Research Area.	2. Research on personal (health) data which consists of the further processing of data initially collected for another purpose ("secondary use").
	Scientific research purposes should also include studies conducted in the public interest in the area of public health.	The distinction between scientific research based on primary or secondary usage of health data is particularly important when discussing the legal basis for the processing, the information obligations and the purpose limitation.
	The term may not be stretched beyond its common meaning.	

related to their health (such as stating symptoms) - Information that becomes health data by cross referencing with other data thus revealing the state of health or health risks		

Legal Basis for the Processing:

A. Consent: Must meet all the conditions for explicit consent, as provided by Articles 4 par. 11, 6 par. 1a, Article 7 and 9 par. 2a of the GDPR. Notably, consent must be freely given, specific, informed, and unambiguous, and it must be made by way of a statement or "clear affirmative action", providing the possibility for withdrawal.

B. National legislation: Where national legislation has such provisions, they should also include suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy. At the same time, they should be proportionate, respect the essence of data protection and provide for sufficient safeguards to the fundamental rights and interests of data subjects.

Data Protection Principles particularly at play when scientific research is involved:

1) **Transparency and data subjects' right to be informed:** Especially when personal data have not been obtained from the data subject, the controller shall provide the information within a reasonable period after obtaining the personal data, but at the latest within one month, with regards to the specific circumstances of the data processing, including information about any changes in the purpose of processing,
2) **Purpose limitation and presumption of compatibility**: Data processing for research purposes shall be subject to appropriate safeguards, ensuring adequate technical and organisational measures.
3) **Data minimisation and storage limitation:** These can be mainly achieved through the requirement of specifying the research questions and assessing the type and amount of data necessary to properly answer these research questions, always complying with the purpose limitation principle,
4) **Anonymisation and Pseudonymisation,** where possible,
5) **Integrity and confidentiality:** Measures shall be taken to include encryption policies, non-disclosure agreements and strict access roles distribution and restrictions. It is recommended that a DPIA be carried out when such processing is likely to result in a high risk to the rights and freedoms of natural persons. Where applicable, DPOs should also be consulted on processing of health data for scientific research.

Exemptions to the information obligation:

- Where it "proves **impossible**" under Article 14 par. 5b GDPR to provide the information. If a data controller seeks to rely on this exemption, it must demonstrate the factors that actually prevent it from providing the information in question to data subjects. If, after a certain period, the factors that caused the "impossibility" no longer exist, the data controller should immediately provide the information.
- Where it would involve a "**disproportionate effort**", based on the number of data subjects, the age of the data and appropriate safeguards in place. The controller should carry out a balancing exercise to assess the effort involved to provide the

information to data subjects against the impact and effects on the data subject if they are not provided with the information.

- Where that would lead to a "**serious impairment of objectives**". To use this exception, controllers must demonstrate that the provision of the information per se would render impossible or seriously impair the achievement of the objectives of the processing.
- Where **obtaining or disclosure is expressly laid down by Union or Member State law**. This exemption is conditional upon the law in question providing appropriate measures to protect the data subject's legitimate interests. The data controller must be able to demonstrate the ways in which the law in question applies to them and requires them to either obtain or disclose the personal data in question.

Exercise of the rights of data subjects: In principle, situations as the current COVID-19 outbreak do not suspend or restrict the possibility of data subjects to exercise their rights. However, Article 89 par. 2 GDPR allows the national legislator to restrict certain data subject's rights. In the light of the jurisprudence of the ECJ, all restrictions of the rights of data subjects must apply only in so far as it is strictly necessary.

International data transfers for scientific research purposes: When personal data is transferred to a non-EEA country or international organisation, in addition to complying with the rules set out in GDPR, especially its Article 5 (data protection principles), Article 6 (lawfulness) and Article 9 (special categories of data), the data exporter shall also comply with Chapter V (data transfers).

In addition to the regular transparency requirement, a duty rests on the data exporter to inform data subjects of the intention to transfer personal data to a third country or international organisation. This includes information about the existence or absence of an adequacy decision by the European Commission, or whether the transfer is based on a suitable safeguard or on a derogation. This duty exists irrespective of whether the personal data was obtained directly from the data subject or not.

Generally, when considering how to address such conditions for transfers of personal data, the EDPB advises that data exporters assess the risks to the rights and the freedoms of data subjects of each transfer and favour solutions that guarantee data subjects ongoing protection and safeguards as to the processing of their data, even after the transfer.

In the absence of an adequacy decision pursuant to Article 45 par. 3 of the GDPR or appropriate safeguards pursuant to Article 46 of the GDPR, Article 49 envisages certain specific situations under which transfers of personal data can take place as an exception. Said derogations must be strictly interpreted, and on a case-by-case basis.

The EDPB explicitly recognises that the fight against COVID-19 has been deemed by the EU and most of its Member States as a crucial public interest, which may require urgent action in the field of scientific research, for instance to identify treatments, develop vaccines. Thus, it may involve transfers to not only third countries or international organisations, but also private entities, such as universities' research institutes.

Any such transfers will need to take into consideration on a case-by-case basis the respective roles (controller, processor, joint controller) and related obligations of the actors (sponsor, investigator), to identify the appropriate measures for framing the transfer.

4.2.2.6 EDPB Guidelines 04/2020 on the use of location data and contact tra*cing tools in the context of the COVID-19 outbreak*

It is evident that since the outbreak of the COVID-19 pandemic, governments and private actors have been turning toward data driven solutions as part of the response to the

healthcare crisis, raising numerous privacy concerns. The EDPB reinstates that the data protection legal framework was designed to be flexible and, thus, is able to achieve both an efficient response to the pandemic and protecting fundamental rights and freedoms.

As such, these guidelines clarify the conditions and principles for the proportionate use of location data and contact tracing tools, for two specific purposes:

- To support the response to the pandemic by modelling the spread of the virus so as to assess the overall effectiveness of confinement measures
- To trace contacts, which aims to notify individuals if they have been in close proximity to someone who is confirmed as a carrier of the virus, so as to break the contamination chains as early as possible

Sources of location data:

- *Location data collected by electronic communication service providers* during the provision of their service. Such data may only be processed in accordance with articles 6 and 9 of the ePrivacy Directive, meaning that they can only be transmitted to authorities or other third parties if they have been anonymised or with the users' prior consent, for data indicating the geographic position of the terminal equipment, which are not traffic data.
- *Location data collected by information society service providers' applications* whose functionality requires the use of such data (e.g. navigation, transportation services, etc.). According to Article 5 par. 3 of the ePrivacy Directive, storing information on the user's device or gaining access to information already stored is allowed only if the user has consented or when the storage and/or access is strictly necessary for the service explicitly requested by the user. Such data can be further processed with the subject's additional consent or on the basis of a Union or Member State law which is necessary and proportionate in a democratic society to safeguard legitimate objectives.

Derogations to the rights and obligations provided for in the "ePrivacy" Directive: According to Article 15, derogations are possible when they constitute a necessary, appropriate and proportionate measure within a democratic society for certain objectives.

Focus on the use of anonymised location data: Preference should always be given to the processing of anonymised data rather than personal data. Anonymisation refers to the use of a set of techniques removing the ability to link the data to an identified or identifiable natural person against any "reasonable" effort. This "reasonability test" must include both objective aspects, as well as contextual elements, such as the rarity of a phenomenon including population density, nature and volume of data.

Upon evaluation of the anonymisation measures, three criteria are to be considered, according to the EDPB:

a) "Singling-out: isolating an individual in a larger group based on the data"

b) "Linkability: linking together two records concerning the same individual"

c) "Inference: deducing, with high probability, unknown information about a data subject"

In addition to the above, the EDPB urges controllers to effectively differentiate between anonymised and pseudonymised data, while monitoring developments in these fields.

Anonymising location data, in particular, is characterised by a high level of difficulty, given that data cannot be anonymised on their own, meaning that only datasets as a whole may be made anonymous. At the same time, the fact that mobility traces of individuals are inherently highly correlated and unique leaves them vulnerable to re-identification

attempts. Thus, data should be carefully processed, building a robust anonymisation system.

Contact tracing applications: Considering the grave intrusion of privacy caused by systematic and large-scale monitoring of location and contact, such measures can only be legitimate if they are based on the users' voluntary adoption, without facing any consequences for either choice. Such applications will need to meet the following criteria:

i. *Accountability*: The controller of any contact tracing application should be clearly defined, whether that is national health authorities or others. If the deployment of contact tracing apps involves different actors, their roles and responsibilities must be clearly established from the outset and explained to the users.

ii. *Purpose limitation*: the purposes must be specifically related to managing the health crisis, collecting only data that is adequate, necessary and proportionate.

iii. *Data minimisation and data protection by design and by default*: it is accepted that only proximity data should be used, as individual personal data is not required. On the same note, direct identification of individuals is not required either for the proper function of the application. At the same time, collected information should remain on the terminal equipment of the user and only relevant data should be collected when necessary.

iv. *Lawfulness of processing*: Based on the provisions of Article 5 par. 3 of the e-Privacy Directive, where processing of contact tracing data is necessary in order for the provider of the application to provide the service explicitly requested by the user, the processing would not require consent. For operations that are not strictly necessary, the provider would need to seek the consent of the user. When contact-tracing is mandated for public interest purposes, the most suitable legal basis for the processing is the necessity for the performance of a task in the public interest or in the exercise of official authority vested in the controller, in accordance with national legislation.

v. *Safeguards*: They should be meaningful and in reference to the voluntary nature of the applications. The categories of data, as well as the entities and purposes of data disclosure should also be identified. Depending on the level of interference, additional safeguards should be placed, based on the processing's nature, scope and purposes.

vi. *Processing of special categories of data*: Health data may be additionally collected and processed for the purposes of tracing the course of the pandemic. When such processing is necessary for reasons of public interest in the area of public health, they controllers should also meet the conditions of Article 9 par. 2(i) GDPR or Article 9 par. 2h when processed for health care purposes. Depending on the legal basis, it might also be based on explicit consent (Article par. 9(2)(a) GDPR). **In accordance with the initial purpose, Article 9(2)(j) GDPR also allows for health data to be processed when necessary for scientific research purposes or statistical purposes**.

vii. *Storage limitation*: The retention period should accurately reflect the true needs and medical relevance of the data collected. Upon the elimination of the pandemic, all data collected should be erased or anonymised.

viii. *Human intervention*: Since such applications are created to support medical personnel possessing adequate knowledge to review the information, procedures and processes including respective algorithms implemented by the contact tracing apps should work under the strict supervision of such personnel to limit the occurrence of any false positives and negatives, instead of being entirely automated.

ix. *Fairness, accountability, and legal compliance*: Algorithms must be auditable and regularly reviewed by independent experts. The application's source code should be made publicly available for the widest possible scrutiny.

x. *Rectification of false data*: Since false positives are an occurrence severely impacting individuals' lives, correction of data and subsequent analysis are to take place, where that is technically feasible.

xi. *Data protection impact assessment (DPIA):* Must always be carried out before implementing such tool as the processing is considered likely high risk, considering that it involves health data, large-scale adoption and systematic monitoring are anticipated, while a new technological solution is implemented. It is recommended that such DPIAs be published for reasons of trust and transparency.

xii.

Table 6: Definitions, as per the EDPB

Contact	For contact tracing applications, a contact is a user who has participated in an interaction with another user confirmed to be a carrier of the virus, and whose duration and distance induce a risk of significant exposure to the virus infection. Parameters for duration of exposure and distance must be estimated by the health authorities and can be set in the application.
Location data	All data processed in an electronic communications network or by an electronic communications service indicating the geographical position of the terminal equipment of a user of a publicly available electronic communications service (as defined in the e-Privacy Directive), as well as data from potential other sources, relating to: • the latitude, longitude or altitude of the terminal equipment • the direction of travel of the user • the time the location information was recorded
Interaction	In this context, an interaction is defined as the exchange of information between two devices located in close proximity to each other in space and time, within the range of the communication technology used. This definition excludes the location of the two users of the interaction.
Virus carrier	For the purposes of the guidelines, virus carriers are defined as users who have been tested positive for COVID-19 and who have received an official diagnosis from physicians or health centres.
Contact tracing	People who have been in close contact, according to criteria defined by epidemiologists, with an individual infected with the virus run a significant risk of also being infected and infecting others. Contact tracing is a disease control methodology that lists all people who have been in close proximity to a virus carrier so as to check whether they are at risk of infection and take the appropriate sanitary measures towards them.

The EDPB has also included a list of recommendations per subject, as follows.

General Recommendations

1.	The application must be complementary to traditional contact tracing techniques, within a wider public health strategy. It must be used only up until the point manual contact tracing techniques can manage alone the number of new infections.
2.	At the latest when "return to normal" is decided by the competent public authorities, a procedure must be put in place to cease the collection of identifiers (global deactivation of the application, automatic uninstallation, etc.) and to activate the deletion of all collected data from all databases.

3.	The source code of the application and of its backend must be open, and the technical specifications must be made public, so that any concerned party can audit the code, and, where relevant, contribute to improving it, correcting possible bugs, and ensuring transparency in the processing of personal data.
4.	The stages of deployment of the application must enable progressive validation of its effectiveness from a public health angle. An evaluation protocol, specifying indicators to measure the effectiveness of the application, must be defined.

Purposes

1.	The application must pursue the sole purpose of contact tracing so that people potentially exposed to the virus can be alerted.
2.	The application must not divert from its primary use for the purpose of monitoring compliance with quarantine or confinement measures and/or social distancing.
3.	The application must not be used to draw conclusions on the location of the users based on their interaction and/or any other means.

Functional considerations

1.	The application must provide a functionality informing users that they have been potentially exposed to the virus based on proximity to an infected user within a window of a predetermined number of days prior to the positive screening test.
2.	The application should provide recommendations to users identified as having been potentially exposed to the virus, relaying instructions regarding the measures they should follow, and allowing the user to request advice. In such cases, a human intervention would be mandatory.
3.	The algorithm measuring the risk of infection based on distance and time, thus determining when a contact has to be recorded in the contact tracing list, must be securely tuneable to the most recent knowledge on the spread of the virus.
4.	**Users must be informed in case they have been exposed to the virus** or must regularly obtain information on whether they have been exposed, within the incubation period of the virus.
5.	The application should be interoperable with other applications developed across EU Member States, so that users travelling across the EU can be efficiently notified.

Data Recommendations

1.	The application must broadcast and receive data via proximity communication technologies (eg. Bluetooth Low Energy) for contact tracing purposes.
2.	This broadcast data must include cryptographically strong pseudo-random identifiers, generated by and specific to the application. These identifiers must be generated by the user's application, possibly based on a seed provided by the central server.
3.	The risk of collision between pseudo-random identifiers should be sufficiently low.

4.	Pseudo-random identifiers must be renewed regularly, at a frequency sufficient to limit the risk of re-identification, physical tracking, or linkage of individuals, by others including central server operators, other users or malicious third parties.
5.	According to the data minimisation principle, the application must not collect data other than what is strictly necessary for the purpose of contact tracing.
6.	The application must not collect location data for the purpose of contact tracing. Location data can be processed for the sole purpose of allowing the application to interact with similar applications in other countries and should be limited to what is strictly necessary for this sole purpose.
7.	The application should not collect health data in addition to those that are strictly necessary for the purposes of the app, except on an optional basis and for the sole purpose of assisting in the decision-making process of informing the user.
8.	Users must be informed of all personal data that will be collected. This data should be collected only with the user authorization.

Technical properties

1.	The application should use available technologies such as use proximity communication technology (e.g., Bluetooth Low Energy) to detect users in the vicinity of the device running the application.
2.	The application should keep the history of a user's contacts in the equipment, for a predefined limited period of time.
3.	The application may rely on a central server to implement some of its functionalities.
4.	The application must be based on an architecture relying as much as possible on users' devices.
5.	At the initiative of users reported as infected by the virus and after confirmation of their status by an appropriately certified health professional, their contact history or their own identifiers should be transmitted to the central server.

Security

1.	A mechanism must verify the status of users reported as positive in the application, for example by providing a single-use code linked to a test station or professional. If confirmation cannot be obtained in a secure manner, data must not be processed.
2.	The data sent to the central server must be transmitted over a secure channel. The use of notification services provided by OS platform providers should be carefully assessed and should not lead to disclosing any data to third parties.
3.	Requests must not be vulnerable to tampering by a malicious user
4.	State-of-the-art cryptographic techniques must be implemented to secure exchanges between the application and the server and between applications. As a general rule they must protect the information stored in the applications and on the server. Such techniques may include symmetric and asymmetric encryption, hash functions, private membership test, private set intersection, Bloom filters, private information retrieval, homomorphic encryption, etc.

5.	The central server must not keep network connection identifiers (e.g., IP addresses) of any users including those who have been positively diagnosed and who transmitted their contacts history or their own identifiers.
6.	In order to avoid impersonation or the creation of fake users, the server must authenticate the application.
7.	The application must authenticate the central server.
8.	The server functionalities should be protected from replay attacks.
9.	The information transmitted by the central server must be signed in order to authenticate its origin and integrity.
10.	Access to all data stored in the central server and not publicly available must be restricted to authorised persons only.
11.	The device's permission manager at the operating system level must only request the permissions necessary to access and use the communication modules, to store the data in the terminal, and to exchange information with the central server.

Protection of personal data and privacy of natural persons for applications whose sole purpose is contact tracing.

1.	Data exchanges must be respectful of the users' privacy and the principle of data minimisation.
2.	The application must not allow users to be directly identified.
3.	The application must not allow users' movements to be traced.
4.	The use of the application should not allow users to learn anything about other users (and notably whether they are virus carriers or not).
5.	Trust in the central server must be limited. The management of the central server must follow clearly defined governance rules and include all necessary measures to ensure its security. The localization of the central server should allow an effective supervision by the competent supervisory authority.
6.	A DPIA must be carried out and should be made public.
7.	The application should only reveal to the user whether they have been exposed to the virus, preferably without revealing information about other users, the number of times and dates of exposure.
8.	The information conveyed by the application must not allow users to identify users carrying the virus, nor their movements.
9.	The information conveyed by the application must not allow health authorities to identify potentially exposed users without their agreement.
10.	Requests made by the applications to the central server must not reveal anything about the virus carrier.
11.	Requests made by the applications to the central server must not reveal any unnecessary information about the user, except, possibly, and only when necessary, for their pseudonymous identifiers and their contact list.
12.	Linkage attacks must not be possible.

13.	Users must be able to exercise their rights via the application.
14.	Deletion of the application must result in the deletion of all locally collected data.
15.	The application should only collect data transmitted by instances of the application or interoperable equivalent applications. No data relating to other applications and/or proximity communication devices shall be collected.
16.	In order to avoid re-identification by the central server, proxy servers should be implemented. The purpose of these *non-colluding servers is to* mix the identifiers of several users before sharing them with the central server, so as to prevent the central server from knowing the identifiers (such as IP addresses) of users.
17.	The application and the server must be carefully developed and configured to avoid collecting any unnecessary data and in order to avoid the use of any third-party SDK collecting data for other purposes.

Principles that apply only when the application sends to the server a list of contacts:

1.	The central server must collect the contact history of users reported as positive to COVID-19 as a result of voluntary action on their part.
2.	The central server must not maintain nor circulate a list of the pseudonymous identifiers of users carrying the virus.
3.	Contact history stored on the central server must be deleted once users are notified of their proximity with a positively diagnosed person.
4.	Except when the user detected as positive shares his contact history with the central server or when the user makes a request to the server to find out potential exposure to the virus, no data must leave the user's equipment.
5.	Any identifier included in the local history must be deleted after a predetermined number of days from its collection.
6.	Contact histories submitted by distinct users should not further be processed e.g., cross-correlated to build global proximity maps.
7.	Data in server logs must be minimised and must comply with data protection requirements

Principles that apply only when the application sends to a server a list of its own identifiers:

1.	The central server must collect the identifiers broadcast by the application of users reported as positive to COVID-19, as a result of voluntary action on their part.
2.	The central server must not maintain nor circulate the contact history of carriers.
3.	Identifiers stored on the central server must be deleted once distributed to the other applications.
4.	Except when the user detected as positive shares their identifiers with the central server or when they make a request to the server to find out their potential exposure to the virus, no data must leave their equipment.
5.	Data in server logs must be minimised and must comply with data protection requirements.

4.2.2.7 EDPB Guidelines 05/2020 on consent under Regulation 2016/679

Consent is recognised as an appropriate legal basis if a data subject is offered control and a genuine choice regarding accepting or declining the terms offered or declining them without detriment. Inviting people to accept a data processing operation should be subject to rigorous requirements, since it concerns the fundamental rights of data subjects, and the controller wishes to engage in a processing operation that would be unlawful without the data subject's consent. These Guidelines provide a thorough analysis of the notion of consent in the GDPR, providing practical guidance to ensure compliance with the GDPR and building upon the Article 29 Working Party Opinion 15/2011 on consent.

Consent in Article 4 paragraph 11 of the GDPR

In order for the consent of data subjects to be valid, it needs to meet the following conditions. Notably, consent needs to be:

A) Freely given

B) Specific

C) Informed

D) Unambiguous indication of the data subject's wishes by which they clearly signify agreement to the processing of their personal data

Table 7: Freely Given conditions

1) Freely Given				
General Information	**Power Imbalance**	**Conditionality**	**Granularity**	**Detriment**
It implies real choice and control for data subjects. Any element of inappropriate pressure or influence which prevents a data subject from exercising their free will, shall render the consent invalid.	Where there is a clear imbalance of powers (e.g., Public authorities, employment etc) it is advised to choose other legal bases that are more appropriate.	When a request for consent is tied to the performance of a contract by the controller, i.e., if consent forms a non-negotiable part of terms and conditions, it is presumed not to have been freely given.	The data subjects should be free to choose which purpose they accept, rather than having to consent to a bundle of processing purposes.	The controller needs to demonstrate that it is possible to refuse or withdraw consent without detriment.
Consent can only be valid if the data subject is able to exercise a real choice, and there is no risk	However, in spite of the imbalance of power, consent is an appropriate lawful basis	In that context, the term "necessary for the performance of a contract" is interpreted strictly. The processing must be necessary	Consent is presumed not to be freely given if the process/ procedure for obtaining it	The controller needs to prove that withdrawing consent does not

of deception, intimidation, coercion or significant negative consequences (e.g. substantial extra costs) if they do not consent.	when it does not deteriorate the data subjects' position in any way.	to fulfil the contract with each individual data subject, establishing a direct and objective link between the processing and the purpose of the execution of the contract.	does not allow data subjects to give separate consent for personal data processing operations respectively.	lead to any costs for the data subject and thus no clear negative impact for those withdrawing consent.
The above is relevant where the requested data is not necessary for the performance of the contract, (including the provision of a service), and the performance of that contract is conditional on the obtaining of these data based on consent. The burden of proof in Article 7(4) GDPR is on the controller, in accordance with the principle of accountability. Access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining of access to information already stored, in the terminal equipment of a user (so called cookie walls).				

Table 8: Specific conditions

2) Specific		
Purpose specification as a safeguard against "function creep" (gradual widening or blurring of purposes for which data is processed, after a data subject has agreed to the initial collection)	**Granularity in consent requests**	**Clear separation of information related to obtaining consent for data processing activities from information about other matters**
Determination of a specific, explicit and legitimate purpose for the intended processing activity.	A controller that seeks consent for various different purposes should provide a separate opt-in for each purpose, to allow users' specific consent for specific purposes.	Controllers should provide specific information with each separate consent request about the data that are processed for each purpose
In line with the concept of purpose limitation, consent may cover different operations that serve the same purpose.		Data subjects need to be aware of the impact of the different choices they have.

Table 9: Informed conditions

3) Informed

Minimum Content	Methods of providing information
The information provided shall include: i. the controller's identity, ii. the purpose of each of the processing operations for which consent is sought, iii. the type of data that will be collected and used, iv. the existence of the right to withdraw consent, v. information about the use of the data for potential automated decision-making, vi. possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards.	The GDPR does not prescribe the form or shape in which information must be provided to meet the requirement of informed consent. Thus, it may be written or oral statements, or audio or video messages. If consent is to be given by electronic means, the request must be clear and concise. Layered and granular information can be an appropriate way to deal with the two-fold obligation of being precise, complete, and understandable. Whether a part of a paper contract or electronic request, the consent request must be separate and distinct.
In case consent sought is to be relied upon by multiple (joint) controllers or if the data is to be transferred to or processed by other controllers who wish to rely on the original consent, these organisations should all be named.	Controllers should ensure that they use clear and plain language in all cases, meaning that a message should be easily comprehensible to the average person. Consent must be clear and distinguishable and provided in an intelligible and easily accessible form, not hidden in general terms and conditions.
Controllers will need to provide a full list of recipients or categories of recipients including processors.	A controller must additionally assess the kind of audience that provides personal data to their organisation, for instance minors etc.

Table 10: Unambiguous indication of the data subject's wishes conditions

4) Unambiguous indication of the data subject's wishes		
Unambiguous indication	**Means through which consent cannot be obtained**	**Recommendations regarding consent**
Consent requires a statement from the data subject or a clear affirmative act, which means that it must always be given through an active motion or declaration.	The use of a pre-ticked opt-in box or opt-out construction that requires an intervention from the data subject is invalid under the GDPR. Silence or inactivity on the part of the data subject, as well as merely proceeding with a service cannot be regarded as an active indication of choice.	Consent should not be unnecessarily disruptive to the use of the service for which it is provided. In any event, consent must always be obtained before the controller starts processing personal data for which consent is needed.

The data subject must have taken a deliberate action to consent to the particular processing.	Consent cannot be obtained through the same motion as agreeing to a contract or accepting general terms and conditions of a service.	Controllers have the liberty to develop a consent flow that suits their organisation, including, for example, physical motions. Consent mechanisms should be clear to data subjects, avoiding ambiguity and ensuring that the action by which consent is given can be distinguished from other actions.
Consent can be provided via a letter or email, as well as a recorded oral statement	Merely continuing the ordinary use of a website is not conduct from which one can infer an indication of wishes by the data subject to signify his or her agreement to a proposed processing operation.	In an online context, and in order to combat "click fatigue", controllers are expected to develop alternative ways, such as obtaining consent through one's browser setting.

Explicit Consent: It is required in certain situations where serious data protection risks emerge, leading to the need for a high level of individual control over personal data.

Where appropriate, the controller could make sure the written statement is signed by the data subject, in order to remove all possible doubt and potential lack of evidence in the future. However, such a signed statement is not the only way to obtain explicit consent. In the digital or online context, a data subject may be able to issue the required statement by filling in an electronic form, by sending an email, by uploading a scanned document carrying the signature of the data subject, or by using an electronic signature.

An organisation may also obtain explicit consent through a telephone conversation, provided that the information about the choice is fair, intelligible and clear, and it asks for a specific confirmation from the data subject (e.g. pressing a button or providing oral confirmation).

Two-stage verification of consent can also ensure explicit consent is valid, for example via an email and the use of an additional verification link or an SMS message containing a verification code to confirm the agreement. This can be particularly useful when medical records are involved.

Special categories of data: The GDPR does not recognize "necessary for the performance of a contract" as an exception to the general prohibition to process special categories of data. Thus, if the controller cannot apply any of the exceptions mentioned in Article 9 par. 2 of the GDPR, they can pursue explicit consent as the final remedy to process such data.

Additional conditions for valid consent:

1) **Demonstrated consent**:
    a. Controllers are free to develop methods to comply with this provision in a way that is fitting in their daily operations, while said methods should not lead to excessive additional data processing.

b. As long as a data processing activity is ongoing, the obligation to demonstrate consent also exists.

c. After the processing activity ends, proof of consent should be kept only as long as strictly necessary for compliance with a legal obligation or for the establishment, exercise or defence of legal claims.

d. Controllers are advised to keep a record of consent statements received, so they can show how and when consent was obtained, and the information provided to the data subject at the time shall be demonstrable. The controller shall also be able to show that the data subject was informed and the controller´s workflow met all relevant criteria for a valid consent.

e. The period of validity of consent will depend on the context, the scope of the original consent and the expectations of the data subject. However, the EDPB explicitly recommends that consent be refreshed at appropriate intervals.

f. The burden of proof in all cases lies with the controller.

2) **Withdrawal of consent**:

a. Consent must be withdrawn as easily as it was given and at any time, without that meaning that is needs the withdrawal must be performed in the exact same way the consent was originally provided. Nonetheless, when consent is obtained via electronic means through only one mouse-click, swipe, or keystroke, data subjects must, in practice, be able to withdraw that consent equally as easily. Accordingly, when consent is obtained through use of a service-specific user interface, the data subject must be able to withdraw consent via the same electronic interface.

b. When consent is withdrawn, all data processing operations that were based on consent and took place before its withdrawal and in accordance with the GDPR, remain lawful. The controller is required to cease processing actions from that point onwards and, if there is no other lawful basis justifying the processing, the respective data should be deleted.

c. In any case, controllers are obliged to assess whether continued processing of the data in question is appropriate, even in the absence of an erasure request by the data subject.

d. A withdrawal of consent does not mean a controller must erase data that are processed for a purpose that is based on the performance of the contract with the data subject.

e. Controllers cannot retrospectively alter the lawful basis of processing if they encounter problems with the validity of consent.

Consent of minors: Given the vulnerability of such groups, the GDPR adds another layer of protection of personal data processing.

Where consent 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. In the latter case, the EDPB recommends that controllers collect at least the parent's/guardian's contact details, performing a risk assessment to determine the level of additional data collection and processing required for the verification.

In any case, Member-States can provide by law a lower age, but this age cannot be below 13 years. As a result, controllers need to be aware of such national laws, taking into account the target group of the services provided.

In cases where a parent/guardian has provided consent in place of the child, once they reach the age of digital consent, the children have the possibility to withdraw consent. Otherwise, it remains a valid lawful base for processing.

Additionally, controllers are expected to make reasonable efforts to verify that the user is over the age of digital consent, and these measures should be proportionate to the nature and risks of the processing activities. Age verification should not lead to excessive data processing, while an assessment of risk is to take place.

The above applies:

I) When the processing is based on consent

II) The processing is related to the offer of information society services directly to a child

- According to the European Court of Justice jurisprudence, that information society services cover contracts and other services that are concluded or transmitted on-line. Where a service has two economically independent components, one being the online component, this component is defined as an information society service.
- If an information society service provider makes it clear to potential users that it is only offering its service to persons aged 18 or over, and this is not undermined by other evidence, then the service will not be considered to be 'offered directly to a child'.

Scientific research: When consent is the legal basis for conducting research in accordance with the GDPR, this consent for the use of personal data should be distinguished from other consent requirements that serve as an ethical standard or procedural obligation.

In principle, scientific research projects can only include personal data on the basis of consent if they have a well-described purpose. For the cases where purposes for data processing within a scientific research project cannot be specified at the outset, an exception is included, specifying that the purpose may be described at a more general level.

When research purposes cannot be fully specified, a controller must seek other ways to ensure the essence of the consent requirements are served best, for example, to allow data subjects to consent for a research purpose in more general terms and for specific stages of a research project that are already known to take place at the outset. Having a comprehensive research plan available for data subjects to take note of, before they consent could also help to compensate a lack of purpose specification.

Yet, appropriate safeguards must still be put in place, possibly including data minimisation, anonymisation and data security, along with transparency. It is moreover noted that no exemptions for scientific research have been set by the GDPR regarding withdrawals of consent.

In all cases, data subjects maintain their rights, including data portability, the right to erasure, restriction, rectification, and access. The right to object is not relevant when data is processed on the basis of consent.

4.2.2.8 EDPB *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*

The concept of controller and its interaction with the concept of processor hold a prominent position in the GDPR ecosystem, since they determine the party responsible for compliance with different data protection rules, and data subjects' rights in practice. As a result, the EDPB has deemed it essential to provide specific guidance on the concepts to ensure a consistent and harmonised approach throughout the EU and the EEA.

Definitions: The concepts of controller and processor are autonomous concepts in the sense that, although external legal sources can help identifying who is a controller, it should be interpreted mainly according to EU data protection law.

1. **The Controller** is determined by the following main concepts:
   a. *Natural or legal person, public authority, agency or other body:* In principle, there is no limitation as to the type of entity that may assume the role of a controller. In practice, though, even if a specific natural person is appointed to ensure compliance with data protection rules, this person will not be the controller but will act on behalf of the legal entity (company or public body) which will be ultimately responsible in its capacity as controller.
   b. *Determining:* Said provision is taking into account whether the control is stemming from legal provisions (explicit or indirect legal competence, provided by the EU or Member-States' national legislation) or factual influence (assessment of which entity exercises determinative influence, based on its concrete activities in a specific context or contractual terms between different parties involved).
   c. *Alone or jointly with others.*
   d. *The purpose and means:* While the controller needs to have predetermined the purposes and means of the processing, the processor retains a small margin of manoeuvre regarding the processing itself.
      - A distinction must be made between essential and non-essential means, to determine if it refers to a controller or a processor acting within the margin of discretion.
      - "Essential means" are closely linked to the purpose and the scope of the processing and are traditionally and inherently reserved to the controller.
      - "Non- essential means" concern more practical aspects of implementation, such as the choice for a particular type of hardware or software or the detailed security measures which may be left to the processor to decide on.
   e. *Of the processing of personal data.*
2. **Joint controllers:** Joint controllership exists regarding a specific processing activity when different parties determine jointly the purpose and means of this processing activity, performing a factual assessment.

   Joint participation can take the form of a common decision taken by two or more entities or the result of converging decisions by two or more entities regarding the purposes and essential means. A main criterion to identify converging decisions in this context is whether the processing would not be possible without both parties' participation in the sense that the processing by each party is inextricably linked.

   An entity will be considered as joint controller with the other(s) only in respect of those operations for which it determines, jointly with others, the means and the purposes of

the processing. This means that, for joint controllership to exist, it is not necessary that each entity involved determines all means in all cases.

Different joint controllers may therefore define the means of the processing to a different extent, depending on who is effectively in a position to do so. Thus, the existence of joint responsibility does not necessarily imply equal responsibility of the various operators involved in the processing of personal data.

It may also be the case that one of the entities involved provides the means of the processing and makes it available for personal data processing activities by other entities. The entity who decides to make use of those means so that personal data can be processed for a particular purpose also participates in the determination of the means of the processing.

It is important to underline that the use of a common data processing system or infrastructure will not in all cases lead to qualify the parties involved as joint controllers, in particular where the processing they carry out is separable and could be performed by one party without intervention from the other or where the provider is a processor in the absence of any purpose of its own (the existence of a mere commercial benefit for the parties involved is not sufficient to qualify as a purpose of processing).

Joint controllership may also be excluded in a situation where several entities use a shared database or a common infrastructure, if each entity independently determines its own purposes. The same is true in situations where various actors successively process the same personal data in a chain of operations, each of these actors having an independent purpose and independent means in their part of the chain.

3. **Processor:** A natural or legal person, public authority, agency or another body, which processes personal data on behalf of the controller. The role of a processor does not stem from the nature of an entity that is processing data but from its concrete activities in a specific context. A service provider may be acting as a processor even if the processing of personal data is not the main or primary object of the service, provided that the customer of the service determines the purposes and means of the processing in practice.

The controller decides to delegate all or part of the processing activities to an external organisation. Nonetheless, a department within a company cannot generally be a processor to another department within the same entity.

Processing is defined as a concept including a wide array of operations ranging from collection, storage and consultation to use, dissemination or otherwise making available and destruction. In practice, this means that all imaginable handling of personal data constitutes processing.

4. **Third-party**: A natural or legal person, public authority, agency or body acting in a capacity for the specific purpose at hand other than the data subject, the controller, the processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
5. **Recipient**: A natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

Relationship between controller and processor:

- The controller must choose the processors providing sufficient guarantees to implement appropriate technical and organisational measures. The controller's assessment of whether the guarantees are sufficient is a form of risk assessment,

taking into account the nature, scope, context and purposes of processing as well as the risks for the rights and freedoms of natural persons.

- The controller in order to assess the sufficiency of the guarantees considers the processor's expert knowledge, their reliability and their resources, as well as the reputation of the processor on the market.

Accountability principle: According to said principle, the controller shall be responsible for the compliance and shall be able to demonstrate compliance. However, some of the more specific rules are addressed to both controllers and processors, such as the rules on supervisory authorities' powers, penalties in case of non-compliance with the obligations of the GDPR and accountability towards supervisory authorities by virtue of the obligations to maintain and provide appropriate documentation upon request, co-operate in case of an investigation and abide by administrative orders. At the same time, it should be recalled that processors must always comply and act only upon the controller's instructions.

Content of the contract or other legal act: Any processing of personal data by a processor must be governed by a contract or other legal act under EU or Member State legislation between the controller and the processor, in writing, including in electronic form. Said contract or other legal act must be binding on the processor with regard to the controller under Union or Member State law. If the initial legal act does not include all the minimum required content, it must be supplemented with a contract or another legal act that includes the missing elements.

A set of standard contractual clauses (SCCs) may be, alternatively, adopted by the Commission or adopted by a supervisory authority, in accordance with the consistency mechanism. These clauses could be part of a certification granted to the controller or processor pursuant to Articles 42 or 43 GDPR. If the parties wish to take advantage of standard contractual clauses, the data protection clauses of their agreement must be the same as those of the SCCs.

The processing agreement should not merely restate the provisions of the GDPR, on the contrary it should include specific, concrete information as to how the requirements will be met and which level of security is required for the personal data processing that is the object of the processing agreement.

It will need to clearly include the subject-matter of the processing, the duration, the nature, the type of personal data and the categories of data subjects, as well as the obligations and rights of the controller.

It, moreover, needs to include or reference information as to the security measures to be adopted, an obligation on the processor to obtain the controller's approval before making changes, and a regular review of the security measures so as to ensure their appropriateness to mitigate risks, which may evolve over time.

The agreement must specify that the processor may not engage another processor without the controller's prior written authorisation, whether specific or general. In both scenarios, the contract should include details as to the timeframe for the controller's approval or objection and as to how the parties intend to communicate regarding this topic

The agreement should contain details as to how the processor is asked to help the controller meet the listed obligations, even including specific timeframes for notifications of data breaches. Furthermore, it should specify what happens to personal data upon termination of the processing activities.

The EDPB recommends the parties to negotiate and agree in the contract the consequences of the notification of an infringing instruction sent by the processor and in case of inaction from the controller in this context.

Obligations of the processor:

(i) The processor must only process data on documented instructions (in any written form) from the controller. When a processor processes data outside or beyond the controller's instructions, and this equals to a decision determining the purposes and means of processing, the processor will be breaching its obligations and will even be considered a controller in respect of that processing.

(ii) The processor may process data other than on documented instructions of the controller when it is required to process and/or transfer personal data on the basis of EU law or Member State law to which the processor is subject.

(iii) The processor must ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. This may be ensured via a relevant contractual agreement or due to statutory obligations already in place.

(iv) The processor must take all the measures required, implementing appropriate technical and organisational security measures.

(v) The processor must respect the conditions referred to in Article 28 par. 2 and 28 par. 4 GDPR for engaging another processor.

(vi) The processor must assist the controller for the fulfilment of its obligation to respond to requests for exercising the data subject's rights. The practical management of individual requests can be outsourced to the processor, but the controller bears the responsibility for complying with such requests.

(vii) The processor must assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the GDPR, notably to adopt adequate technical and organisational measures to ensure security, to notify personal data breaches without undue delay, to carry out data protection impact assessments etc.

(viii) On termination of the processing activities, the processor must, at the choice of the controller, delete or return all the personal data to the controller and delete existing copies.

(ix) The processor must make available to the controller all information necessary to demonstrate compliance with the obligations and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller

(x) The processor must immediately inform the controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

Consequences of joint controllership:

a) Joint controllers should in a transparent manner determine their respective responsibilities for compliance, in particular regarding the exercising of the rights of the data subject and the duties to provide information, unless and in so far as the respective responsibilities of the controllers are determined by Union or Member State law to which the controllers are subject.

b) Each controller must ensure that they have a proper legal basis for the processing of personal data, maintaining compatibility with the purposes for which they were originally collected.

c) The obligations do not need to be equally distributed among the joint controllers.

d) Allocation of responsibilities needs to be done with an arrangement, binding for all parties. Of course, the EDPB recommends that a contract or other legal act be used. The way responsibilities, i.e., the tasks, are allocated between each joint controller has to be stated in a clear and plain language in the arrangement. The arrangement shall duly reflect the respective roles and relationships of the joint controllers with the data subjects, who shall in turn have access to the essence of the arrangement. The arrangement may designate a contact point for data subjects.

e) Irrespective of the terms of the arrangement, data subjects may exercise their rights in respect of and against each of the joint controllers

4.2.2.9 EDPB Guidelines 01/2022 on data subject rights - Right of access

The exercise of the right of access is realised both in the framework of data protection law, in accordance with the objectives of data protection law, and, therefore, holds a prominent position among the various data subjects' rights. Thus, the EDPB considers it necessary to provide more precise guidance on how the right of access has to be implemented in different situations. These guidelines aim at analysing the various aspects of the right of access.

Aim of the right of access: Enabling individuals to have control over their personal data, understanding how it is being processed and the consequences of such processing, verifying at the same time the lawfulness of the processing.

Table 11: Structure of Article 15 of the GDPR providing for the right to access

Structure of Article 15 of the GDPR providing for the right to access	
1.	Confirmation as to whether or not the controller is processing personal data concerning the requesting person
2.	Access to the personal data concerning the requesting person
3.	Access to the following information on the processing: (a) the purposes of the processing (b) the categories of personal data (c) the recipients or categories of recipients (d) the envisaged duration of the processing or the criteria for determining the duration (e) the existence of the rights to rectification, erasure, restriction of processing and objection to processing; (f) the right to lodge a complaint with a supervisory authority (g) any available information on the source of the data, if not collected from the data subject (h) the existence of automated decision-making, including profiling and other information relating thereto

4.	Information on safeguards in case the personal data are transferred to a third country or to an international organisation
5.	The obligation of the controller to provide a copy of the personal data undergoing processing. The notion of a copy must be interpreted in a broad sense and includes the different kinds of access to personal data as long as it is complete and can be kept by the data subject. The first copy should be granted free of charge. However, under some circumstances it could be appropriate for the controller to provide access through other temporary ways instead of providing a copy, especially to verify information or upon the data subject's request.
6.	Charging of a reasonable fee by the controller based on administrative costs for any further copies requested by the data subject. Whether the request concerns a first copy or further copies depends on the time of the request and the type of data processed.
7.	Provision of information in electronic form, unless otherwise requested by the data subject.
8.	Taking into account the rights and freedoms of others

Principles of the right of access:

1) **Completeness of information**: Unless explicitly requested otherwise by the data subject, a request to exercise the right of access shall be understood in general terms, encompassing all personal data concerning the data subject. In case a vast amount of data is processed on the data subject, the controller may request further specifications and clarifications to avoid a data overflow.
2) **Correctness of the information**: This includes the obligation to give information about data that are inaccurate or about data processing, which is not or no longer lawful, without prejudice to the obligation of the controller to end unlawful processing or to correct inaccurate data.
3) **Time reference point of the assessment**: Data provided upon a data subject's request should cover all data available at the time of the request and as soon as possible, adapted to the respective retention periods. This means that controllers are not required to provide personal data, which they processed in the past but which they no longer have at their disposal.
4) **Compliance with data security requirements**: Appropriate technical and organisational measures should be implemented to ensure a level of security appropriate to the risk of the processing.

Form of the request for access to personal data: The EDPB encourages controllers to provide the most appropriate and user-friendly communication channels. Nevertheless, if the data subject makes a request using a communication channel provided other than the one indicated as the preferable one, such request shall be, in general, considered effective and the controller should handle it accordingly. It should be noted that the controller is not obliged to act on a request sent to a random or incorrect email (or postal) address, not directly provided by the controller, or to any communication channel that is clearly not intended to receive requests regarding data subject's rights, as long as the controller has provided an appropriate communication channel.

The EDPB recommends, as good practice, that controllers introduce, where possible, mechanisms to improve internal communication between employees on requests received by those who may not be competent to deal with such requests. Additionally, the EDPB considers as good practice for the controllers to confirm receipt of requests in writing, for example by sending e-mails (or information by post, if applicable) to the requesting persons confirming that their requests have been received and that the one-month period runs from day X to day Y.

Identification of the data subject and link to the personal data: The controller must be able to identify the data subject, the data referring to the data subject, and confirm the identity of the person in case of doubts.

The controller should act upon the requests of data subjects for exercising their individual rights, unless it can demonstrate that it is not in a position to identify the data subject. It is noted that the controller is not obliged to request additional information, but must accept it if provided. Such additional information should not be more than the information initially needed for the verification of the data subject's identity (authentication), in accordance with the principle of proportionality. In case of demonstrated impossibility to identify the data subject, the controller needs to inform the data subject accordingly, if possible.

Where an ID is legally requested, the controller must implement safeguards to prevent its unlawful processing. The EDPB recommends, as good practice, that the controller, after checking the ID card, makes a note such as " ID card was checked " to avoid unnecessary copying or storage of copies of ID cards.

Requests made via third parties / proxies: Since information about individuals' personal data cannot be shared with unauthorised parties, national laws governing legal representation (e.g., powers of attorney), which may impose specific requirements for demonstrating authorisation to make a request on behalf of the data subject, should be taken into account.

The same provisions apply in cases of parents/guardian requesting access to their children's personal data, where verification of parental responsibility may be in place.

Where the right of access is exercised through portals/channels provided by a third party, controllers need to ensure that the third party is acting legitimately on behalf of the data subject. There is, however, no obligation for the controller to provide the data directly to the portal, but they may deem appropriate another means of disclosure directly to the data subject.

Retrieval of personal data: The controller should use available information in the organisation regarding the data subject that likely will result in matches in the systems depending on how the information is structured. It should be designed in such a way that it doesn't compromise the privacy of other data subjects.

The controller shall take appropriate measures to provide any communication relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The term "appropriate" should never be understood as a way of limiting the scope of the data covered by the right of access, but to indicate that the best way to provide the information should be determined. In accordance with the accountability principle, a controller must document their approach to be able to demonstrate how the means chosen to provide the necessary information are appropriate in the circumstances at hand.

Vast amount of information on a data subject: In some cases, there may be a discrepancy between the amount of information the controller needs to provide data subjects with and the requirement that it must be concise. One way of achieving both, and an example of an

appropriate measure for certain controllers, is to use a layered approach, as long as the right of access is not limited, and no extra burden is added for the data subject.

A layered approach in relation to the right of access means that a controller, under certain circumstances, can provide the personal data and the supplementary information required in different layers, the first of which shall include information about the processing and the relevant rights. When deciding what information should be given in the different layers the controller should consider what information the data subject in general would consider as most relevant. For the use of layered approach to be considered as an appropriate measure it is necessary that the data subject is informed at the outset that the information is structured into different layers and provided with a description of what personal data and information that will be contained in the different layers, so they can decide which layers they would like to access.

Extension of the time to respond: Can take place due to the complexity and number of requests of access, the amount of data processed, the ways in which it is stored, the need to redact information or whether the information requires further work to be intelligible. The mere fact that complying with the request would require a great effort does not make a request complex and neither does the fact that a big company receives a large number of requests, as it would require an extraordinary increase of requests.

In addition to the above, the EDPB has also included a descriptive flowchart demonstrating the various factors and steps to consider during a request for access, as below.

Step 1: How to interpret and assess the request?

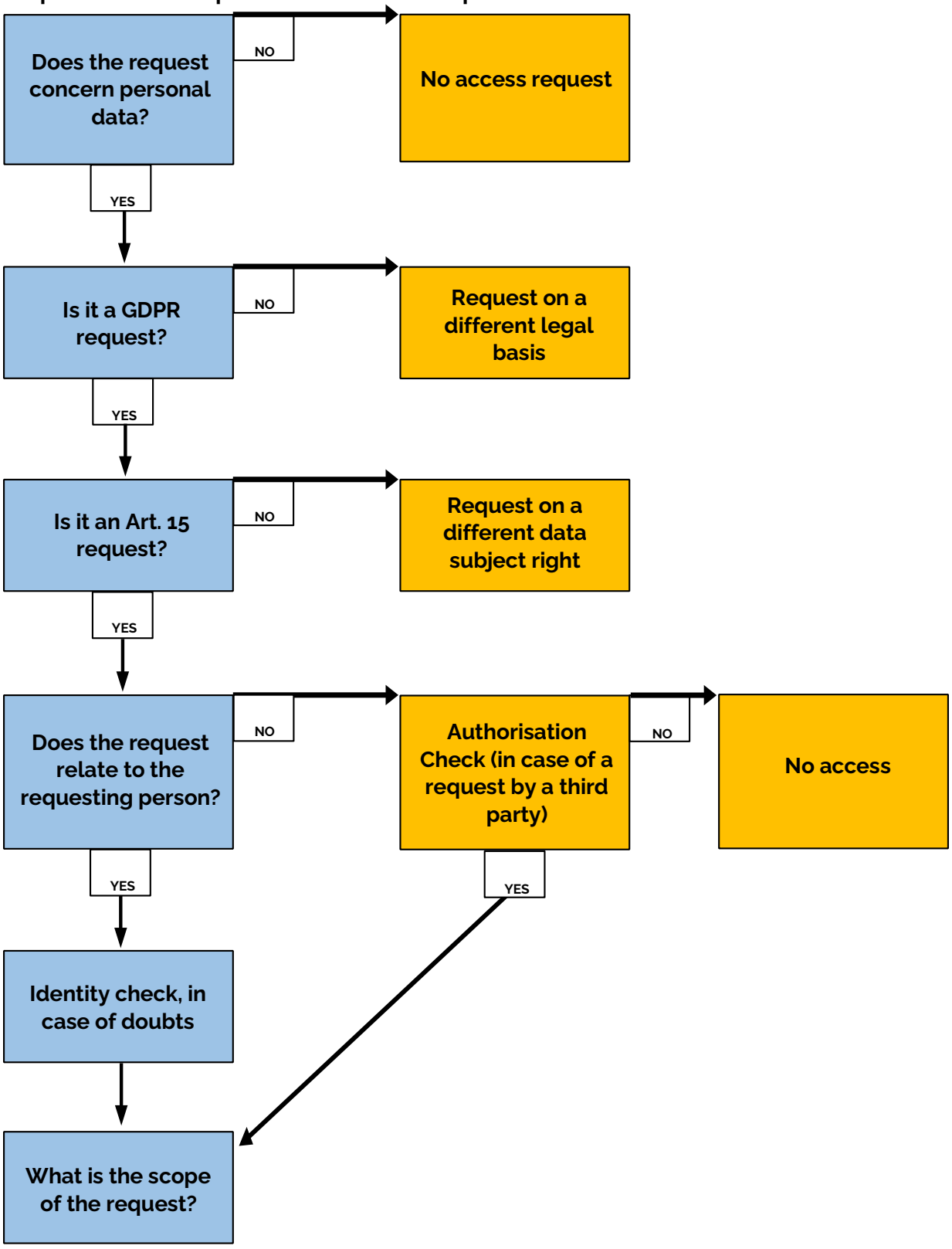


Figure 1: How to interpret and assess the request?

Step 2: How to answer the request (1)?

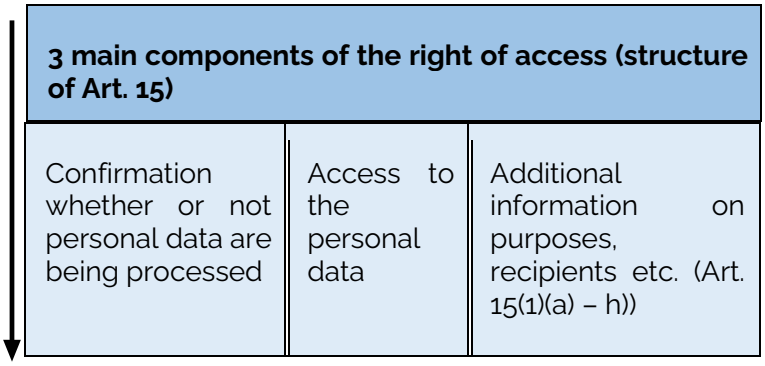


Figure 2: How to answer the request (1)?

Step 2: How to answer the request (2)?

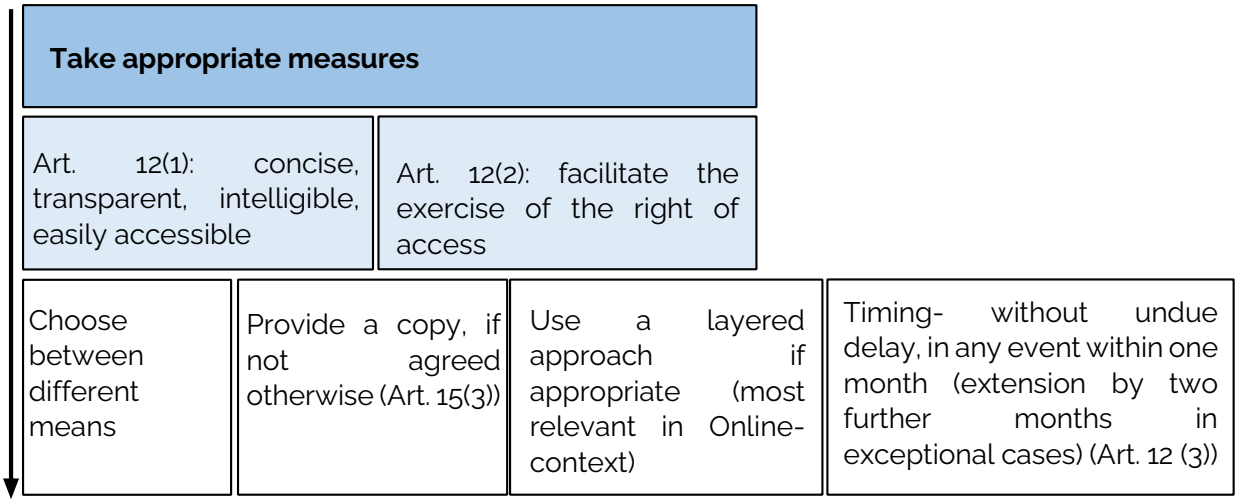


Figure 3: How to answer the request (2)?

Step 2: How to answer the request (3)?

How can the controller retrieve all data about the data subject?			
Define search criteria – based on what the data subject has provided, other information that the controller holds about the data subject and the factors on which data is structured (e.g., customer number, IP addresses, professional title, family relations etc.).	Identify any technical functions that may be available to retrieve data.	Search through all relevant IT or non-IT filing systems.	Compile, extract or otherwise collect data that relates to the data subject in a way that fully mirrors the processing, i.e., that includes all personal data regarding the data subject, and enables the data subject to be aware of and verify the lawfulness of the processing. The retrieving of the information could be done case-by-case or, when relevant, by the use of a privacy by design tool already implemented by the controller.

Figure 4: How to answer the request (3)?

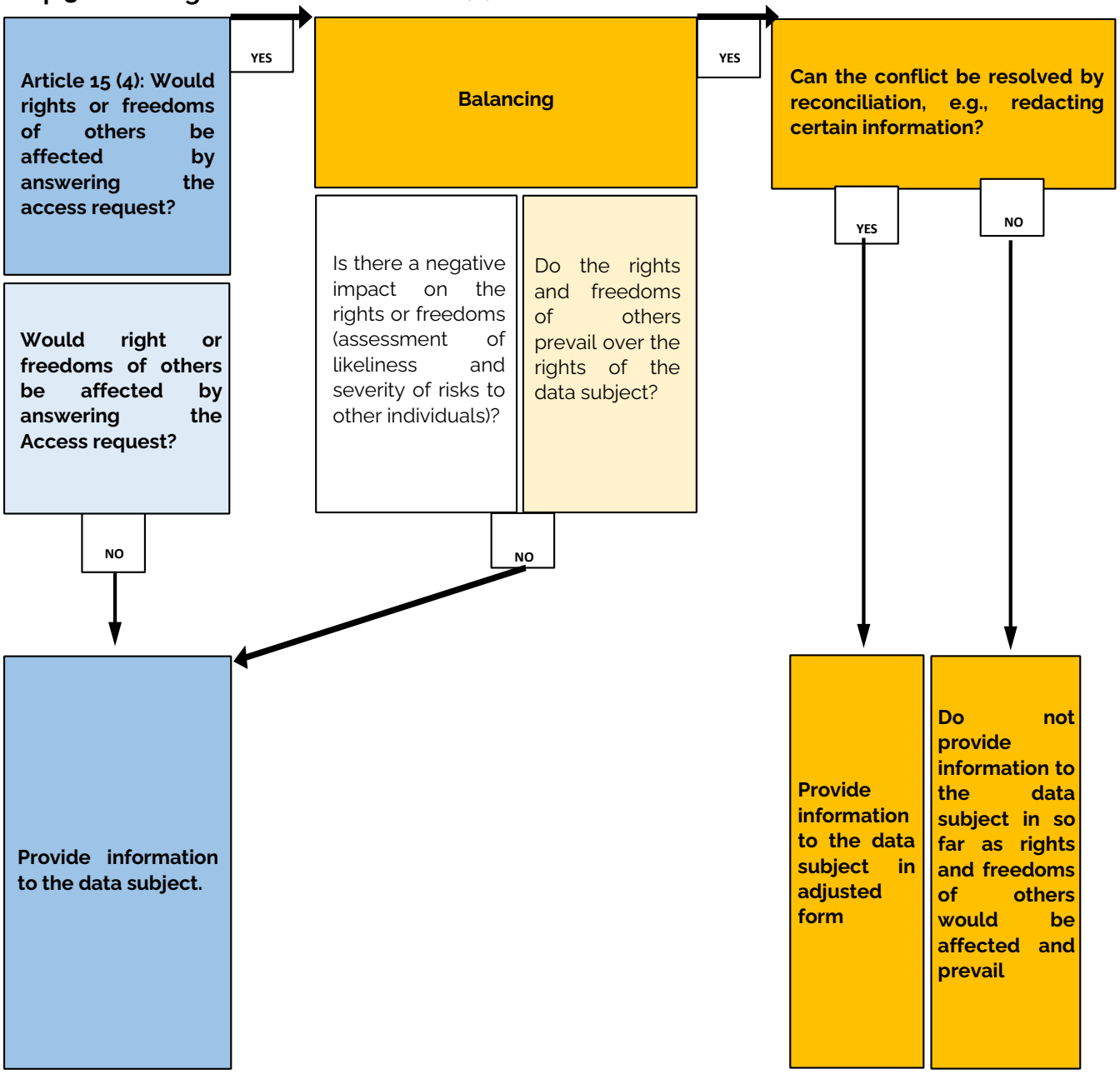


Figure 5: Checking limits and restrictions (1)

Step 3: Checking limits and restrictions (2)

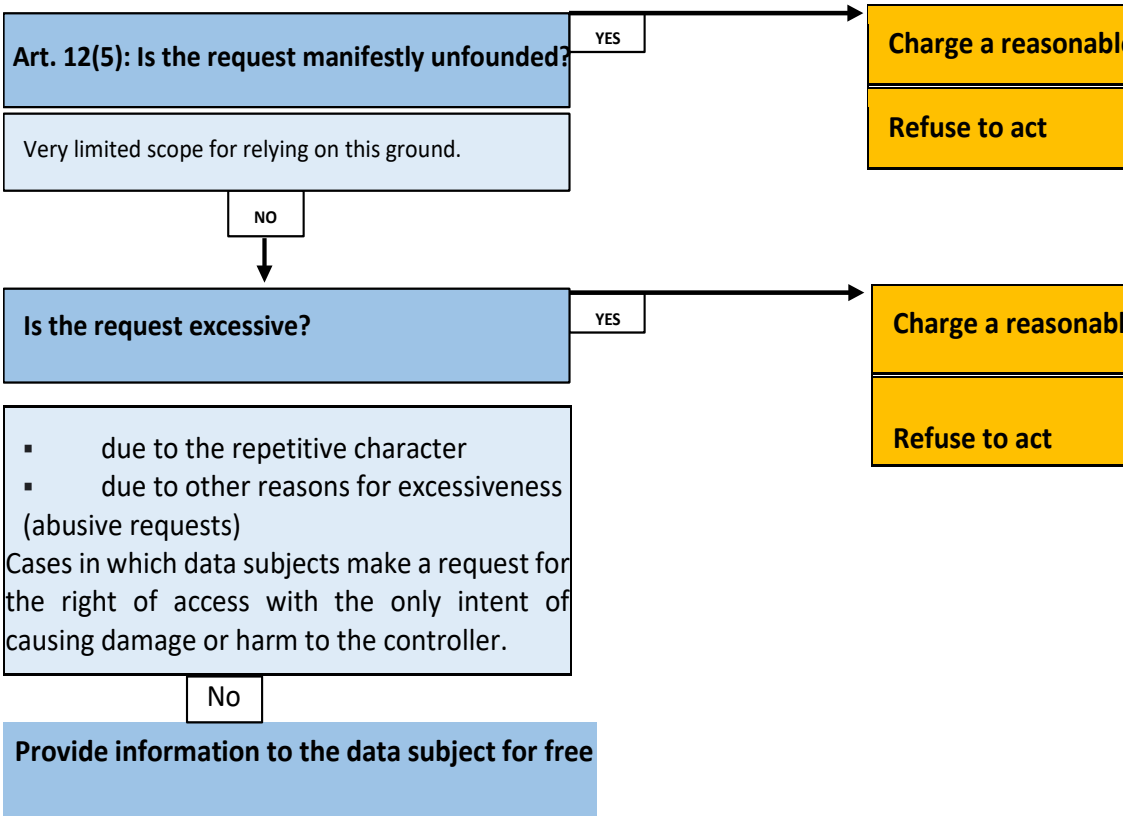


Figure 6: Checking limits and restrictions (2)

4.2.2.10 EDPB Guidelines 02/2021 on virtual voice assistants

As virtual voice assistants (hereafter VVAs) are being incorporated in more and more smartphone applications, connected vehicles, smart appliances etc, there is also an exponential growth of privacy issues arising. Data controllers providing such services have a series of obligations and responsibilities, in compliance with both the GDPR and the e-Privacy Directive. Consequently, the EDPB deemed necessary providing additional guidance on how to make such devices GDPR-compliant.

Definition: Virtual voice assistants can be defined as a software application that provides capabilities of oral dialogue with a user in natural language. A VVA can be broken down into modules allowing to perform different tasks: sound capture and restitution, automatic speech transcription (speech to text), automatic language processing, dialogue strategies, access to ontologies (data sets and structured concepts related to a given domain) and external knowledge sources, language generation, voice synthesis (text to speech), etc.

In practice, a VVA is not a smart speaker, but a smart speaker can be equipped with a voice assistant.

The organization of the underlying data processing may involve multiple information flow patterns, with following being the easiest to identify:

1) The physical instance: the hardware element in which the assistant is embodied (smartphone, speaker, smart TV, etc.) and which carries microphones, speakers and network and computing capacities.
2) The software instance: the part implementing the human-machine interaction strictly speaking and which integrates the modules for automatic speech recognition, natural language processing, dialogue and speech synthesis. This can be operated directly within the physical equipment, but in many cases is performed remotely.
3) The resources: external data such as content databases, ontologies or business applications that provide knowledge or enable the requested action to be carried out in a concrete way.

Automatic Speech Recognition (ASR): Also known as speech-to-text, it is currently being offered by most digital players.

Natural Language Processing (NLP): Natural Language Processing is a multidisciplinary field involving linguistics, computer science and artificial intelligence, which aims to create natural language processing tools for a variety of applications.

Speech Synthesis: It is the artificial production of human speech.

Actors in Virtual Voice Assistants cases:

I. **The VVA provider (or designer):** responsible for the development of the VVA, designs and defines its possibilities and default functionalities, including activation modalities, data access, record management, hardware specifications, etc,
II. **The VVA application developer,**
III. **The integrator**: manufacturer of connected objects, who wishes to equip them with a VVA,
IV. **The owner**: in charge of physical spaces receiving people, they wish to provide a VVA to their audience,
V. **The user.**

The above stakeholders should clearly decide and inform data subjects on the conditions under which each of them will act and comply with the resulting roles of controllers, joint-controllers or processors. Thus, data subjects should be in a position to understand and identify the roles at stake and should be able to contact or act with each stakeholder. The distribution of roles should not be to the detriment of the data subjects, even though scenarios can be complicated or evolving. When these stakeholders are independent controllers, it is important that a clear information notice is given to the data subjects, explaining the various stages and actors of the processing.

e-Privacy Directive: As VVAs use electronic communications networks to access the physical devices that constitute "terminal equipment" in the sense of the e-Privacy Directive, the relevant apply whenever VVA stores or accesses information in the physical device linked to it. In accordance with the definition of "terminal equipment", smartphones, smart TVs and similar IoT devices are examples for terminal equipment.

Legal Basis for processing: Consent is most likely the proper legal basis both for the storing and gaining of access to information already stored and the processing of personal data following the aforementioned processing operations. Exceptionally, consent is not required when carrying out or facilitating the transmission of a communication over an electronic communications network, or, when strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

Transparency: Data controllers are obliged to inform users of the processing of their personal data in a concise, transparent, intelligible form, and in an easily accessible way. Any failure to provide necessary information is a breach of obligations that may affect the legitimacy of the data-processing. In order to comply with the GDPR, data controllers should find a way to inform not only registered users, but also non-registered users and accidental VVA users. These users should be informed at the earliest time possible and at the latest, at the time of the processing.

Taking into consideration the difficulties arising from the multitude of users, the complexity of the systems and the specificities of the vocal interface, the EDPB has included the following recommendations for stakeholders:

a. The privacy policy should have a clearly separated section regarding the VVA processing of personal data.
b. The information provided to the user should match the exact collection and processing that is carried out.
c. It should at all times be apparent which state the VVA is in. Users should be able to determine whether a VVA is currently listening on its closed-loop circuit and especially whether it is streaming information to its back end, ensuring that people with disabilities are also duly informed.
d. VVA controllers should make transparent what kind of information a VVA can derive about its surroundings, such as but not limited to other people in the room, music running in the background, any processing of the voice for medical or marketing other reasons, pets, etc.

Purpose limitation and legal basis; Data controllers should clearly specify their purpose(s) in relation to the context in which the VVA is used, so that they are clearly understood by the data subjects. Among the most common purposes for processing personal data by VVAs the EDPB recognises the following:

- **Execute users' requests.** Any personal data processing that is necessary to execute the user's request can therefore rely on the legal basis of the performance of the contract.
- VVA improvement by **training of the machine learning model and human review** and labelling of voice transcriptions. Such activities are not strictly necessary for the performance of a contract.
- **User identification (using voice data).** The use of voice data for user identification implies the processing of biometric data, leading to the need of implementing an exemption for the processing for such data according to Article 9 of the GDPR. In particular, the user's explicit consent is definitely required.
- **User profiling for personalised content or advertising.** Personalisation of content may constitute an intrinsic and expected element of a VVA, depending on the nature of the services provided, the expectations of the data subjects and the potential of performance without personalisation. If processing is not strictly "necessary for the performance of a contract", the VVA provider must, in principle, seek the consent of the data subject.

In view of the above, the EDPB recommends that the users be informed of the exact purposes for each data-processing activity. In particular when consent is sought, such consent must be given for each specific purpose.

Processing of children's data: When the legal basis for the processing is the performance of a contract, the conditions for processing children's data will depend on national contract laws. However, when the legal basis is consent, the relevant conditions must be met.

Data retention: Following the GDPR data storage limitation principle, VVAs should store data for no longer than is necessary for the purposes for which the personal data are processed. The data minimisation principle is closely related to the data storage limitation principle, limiting not only the data storage period, but also the type and quantity of data. In case the user withdraws their consent, the data collected can no longer be used for further training of the model.

Data subjects should not be nudged to keep their data indefinitely. While deleting stored voice data or transcriptions might have an impact on the service performance, such impact should be explained to users in a clear and measurable way. VVA service providers should avoid making general statements on the degradation of the service after personal data is deleted.

Security: To securely process personal data, VVAs should protect their confidentiality, integrity and availability. Thus, VVA designers and application developers should provide secure state-of-the-art authentication procedures to users. At the same time, human reviewers should always receive the strictly necessary pseudonymised data.

Particularly for reasons of security for biometric data, the EDPB recommends storage solely on the local device and not remote servers. Additionally, due to the sensitiveness of the voiceprints, standards such as ISO/IEC 24745 and techniques of biometric model protection should be thoroughly applied.

Data minimisation: VVA designers should consider technologies deleting the background noise to avoid recording and processing such situational information.

Accountability: For any processing that is based on consent, controllers are obliged to be able to prove the consent of data subjects. Voice data can be used for accountability (e.g. to prove consent). The retention obligation for such voice data would then be dictated by the accountability requirements of the relevant specific legislation.

Data Protection Impact Assessment: It is very likely that VVA meet the conditions identified as needing a DPIA, particularly if the device may be observing monitoring or controlling data subjects or systematically monitoring at large scale, use of "new technology", or the processing of sensitive data and data concerning vulnerable data subjects.

Data protection by design and by default: By default, services which do not require an identified user should not associate any of the VVA identified users to the commands.

Data subjects' rights and VVAs:

1) **Right to access**: On demand, data controllers should send a copy of personal data, and audio data (including voice recordings and transcriptions) in particular, in a common format readable by the data subject.
2) **Right to rectification**: To facilitate data rectification, users, registered or not, should be able to manage and update, at any time, their data by voice directly from the VVA device.
3) **Right to erasure**: Users, registered or not, should be able, at any time, by voice from the VVA device, or from a self-service tool integrated into any device associated to the VVA, to delete data concerning them. The data controller should ensure that no more processing may occur, after the exercise of the right of erasure.

4) **Right to data portability**: In practice, the right to data portability should facilitate switching between different VVA providers. Furthermore, the data controller should offer users the possibility of directly retrieving their personal data from their user area, as a self- service tool. The users should also be able to exercise this right through voice command. In regard to the format, VVA providers should provide personal data using commonly used open formats (e.g., mp3, wav, csv, gsm, etc.) along with suitable metadata used in order to accurately describe the meaning of exchanged information.

4.3 Relevant National Dispositions

4.3.1 Italy

The Italian Data Protection Act (hereafter the IDPA) sets up different rules and requirements for processing personal data for scientific or historical research purposes.

In the first place, Article 101 of the IDPA prohibits the use of personal data that has been collected for historical research purposes, for taking measures, or issuing provisions against the data subject in administrative matters. Moreover, this article specifies that any document containing personal data that is processed for historical research purposes may be used only if it is relevant and indispensable for such purpose and by having regard to its nature.

Secondly, under Article 105 of the IDPA**, the personal data that has been collected for scientific research purposes shall not be used for taking decisions or measures concerning the data subject or processed for different purposes**. Also, following Article 105 (2) the **data controller shall specify unambiguously the scientific research purpose and inform about it the data subject**. However, this requirement can be exempt if it entails a disproportionate effort with the regard to the data subject right on the condition that that information has been appropriately publicised as laid down by the rules of conduct.

Other requirements are provided for the processing of health data by Article 110 of the IDPA. Particularly, the IDPA requires **the data controller to conduct Data Protection Impact Assessment and publish it when processing the health data for scientific research in the medical, bio-medical, or epidemiological sectors, without consent of the data subject** under Article 9(2), letter j) of the GDPR, including research that is part of a biomedical or health care research programme according to Section 12-a of legislative decree No 502 of 30/12/1992.

Besides, the consent of data subjects for processing health data is not required if informing the data subjects proves impossible or entails a disproportionate effort on specific grounds, or if it is likely to render impossible or seriously impair the achievement of the research purposes. However, in this case, the data controller shall take appropriate measures to protect the rights, freedom, and legitimate interest of the data subject. Additionally, **the research programme shall be the subject of a reasonable, favourable opinion by the geographically competent ethics committee** as well as being submitted to the Italian Supervisory Authority for prior consultation.

Nevertheless, the data controller shall process personal data for the purposes of historical or scientific research following the rules of conduct adopted by the Italian Supervisory Authority.

- Rules of conduct for processing for archiving in the public interest or for historical research purposes: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069661 (Available only in Italian)

- Rules for processing for statistical or scientific research purposes: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9069637 (Available only in Italian)

4.3.2 Greece

In Greece, the legal framework consists, along with the GDPR, of the Hellenic Data Protection Authority (HDPA), measures for implementing Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons concerning the processing of personal data, and transposition of Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016, and other provisions (hereafter the DPA) and other national implementation acts.

Under Article 30, the **processing of special categories of personal data is permitted, without consent of the data subject**, only if it is necessary for scientific or historic research purposes and the data controller's interest overrides the data subject's interest. In this respect, **the data controller shall implement appropriate and specific measures for the protection of the data subject's interest, including restriction of access to the data controller and/or processor, pseudonymisation, encryption, and the appointment of a DPO.**

Moreover, **the special categories of personal data shall be anonymised as soon as the research purposes allow**, unless contrary to the data subject's legitimate interest.

Finally, the data controller may publish personal data processed in the context of the research, as long as the data subject has consented in writing or publication is necessary for the presentation of the results of the research, in which case the publication must take place only by means of pseudonymization.

- List of Processing Operations Subject to the Requirement of a Data Protection Impact Assessment: https://www.dpa.gr/en/Organisations/Impact_Assessment (Available in English)

4.3.3 UK

The UK GDPR, along with the Data Protection Act of 2018 (hereafter DPA 2018), lay out specific provisions on personal data processing for scientific or historical research purposes. In particular, Section 19 of the DPA 2018 provides that **processing of personal data that is necessary for scientific or historical research purposes may be permitted, as long as the data controller:**

- is able to **demonstrate why they cannot use anonymised data**
- considers whether they could **use pseudonymisation** to make it more difficult to link the personal data back to specific individuals
- is able to **demonstrate that the processing is not likely to cause substantial damage** or distress to individuals
- **does not use the data to take any action or make decisions in relation to a specific data subject**, unless they are carrying out approved medical research as defined in section 19(4) of the DPA 2018
- has considered other appropriate safeguards and security measures

According to Schedule 1 Part 1 paragraph 4 of the DPA 2018, it is moreover necessary that the personal data processing:

1. is necessary for archiving purposes, scientific or historical research purposes or statistical purposes
2. is carried out in accordance with Article 89(1) of the UK GDPR (as supplemented by section 19)
3. is in the public interest

In addition, Schedule 2 Part 6 paragraph 27 of the DPA 2018 provides for the exact GDPR provisions that do not apply to personal data processed for scientific or historical research purposes to the extent that the application of those provisions would prevent or seriously impair the achievement of the purposes in question, such as the right of access, the right to rectification etc.

Moreover, the UK GDPR contains specific provisions that adapt the application of the purpose limitation and storage limitation principles when processing of personal data for scientific or historical research purposes, or statistical purposes is involved, extending both the scope and the retention period permitted.

Taking into consideration that many of the terms and concepts included in the above provisions remains unclear, the Information Commissioner's Office (hereafter ICO), the UK's independent Supervisory Authority to uphold information rights, has published a **Draft Guidance on the research provisions within the UK GDPR and the DPA 2018**, which will remain open for consultation until the 22nd of April 2022.

In that sense, scientific or historical research should be understood broadly, including research carried out not only in traditional academic settings, but also research carried out in commercial settings, and technological development and demonstration. The guidelines also include a list of indicative criteria for scientific or historical research, as well as an explanation of the further safeguards that must be set in place when handling special categories of data, such as medical information, for the aforementioned purposes.

Finally, the guidelines provide a more thorough explanation of the exemptions of rights available for data processed for research-related purposes.

- Draft Guidance on the research provisions within the UK GDPR and the DPA 2018: https://ico.org.uk/media/about-the-ico/consultations/4019614/research-provisions-draft-consultation-202202.pdf

4.3.4 Spain

The Organic Law 2/2018 on Data Protection and Guarantee of Digital Rights (the Spanish Data Protection Act) does not provide additional requirements or provisions concerning scientific or historical research.

However, in order to assist the data controllers in identifying kinds of data processing that require the Data Protection Impact Assessment (hereafter DPIA), the Spanish Supervisory Authority has published "the list of the types of data processing that requires a data protection impact assessment under Article 35.4". This list sets out what **kind of processing requires a DPIA and facilitates their identification for the data controllers**.

- List of the types of data processing that requires a data protection impact assessment under Article 35.4: https://www.aepd.es/sites/default/files/2019-09/listas-dpia-en-35-4.pdf (Available in English)

4.3.5 Germany

Article 27 of the Federal Data Protection Act (hereinafter FDPA) allows the data controller to process sensitive data for scientific or historical research if the processing is necessary for these purposes and the data controller's interest significantly outweighs the data subject's interest. Moreover, the data controller shall **take specific and measures in order to process sensitive data for such purposes**, which shall include:

1. Technical organizational measures to ensure that processing complies with the GDPR
2. Measures to ensure that it is subsequently possible to verify and establish whether and by whom personal data were input, altered, or removed
3. Measures to increase awareness of staff involved in processing operations
4. Designation of a data protection officer
5. Restrictions on access to personal data within the controller and by processors
6. The pseudonymization of personal data
7. The encryption of personal data
8. Measures to ensure the ability, confidentiality, integrity, availability, and resilience of processing systems and services related to the processing of personal data, including the ability to rapidly restore availability and access in the event of a physical or technical incident
9. A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing
10. Specific rules of procedure to ensure compliance with FDPA and with the GDPR in the event of transfer or processing for other purposes

Additionally, FDPA requires to **anonymise sensitive data as soon as the research purpose allows it.** Until then, the characteristics enabling information concerning personal or material circumstances to be attributed to an identified or identifiable individual shall be **stored separately**. They may be combined with the information only to the extent required by the research or statistical purpose.

Finally, when the data controller intends to publish the personal data, he shall demonstrate that one of the following requirements is met: data subject gives the consent for the publication, or it is indispensable for the presentation of research of findings on contemporary events.

4.3.6 Cyprus

Law 125 (I)/2018 of the Republic of Cyprus providing for the Protection of Natural Persons with regards to the processing of personal data and for the free movement of such data (the Cypriot Data Protection Act) fully encompasses the GDPR and does not provide specific provisions or requirements regarding data processing for scientific or historical research.

Article 31 of the above-mentioned law merely states that the processing which is carried out by a controller or a processor for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be used for taking a decision which produces legal effects concerning the data subject or similarly significantly affects them.

Nonetheless, Article 17 of Law 25 (I)/2021 on Official Statistics specifies that access to confidential data collected by the Statistical Service directly from the statistical units,

which only allow for indirect identification of the statistical units, shall be granted by permission of the Director, after submission of a formal application for the release of confidential data for scientific, research purposes. This is possible under the condition that the said data are necessary for specific scientific, research programs in Cyprus or abroad, the results of which do not disclose specific statistical units and are not to be used for commercial purposes.

Additionally, the Office of the Commissioner for Personal Data Protection (hereafter OCPDP), the Supervisory Authority of Cyprus, has issued Guidelines on the Retention Period for Personal Data concerning health information. Citing directly Article 89 of the GDPR, the guidelines provide for an extension of the retention period for data processed for public interest purposes, scientific, historical or statistical purposes, as long as technical and organizational measures have been put in place to prevent identifying the data subject and ensuring data minimisation.

Finally, the OCPDP has also issued a guide on the indicative cases where a Data Protection Impact Assessment (hereafter DPIA), is deemed necessary, due to the special categories of personal data involved or the large scale of data processing, which may be relevant in research projects.

- The Official Statistics Law of 2021 - Law No. 25(I)/2021: https://www.census2021.cystat.gov.cy/en/images/LawEN.pdf (Available in English).
- Office of the Commissioner for Personal Data Protection - Data Protection Impact Assessment: https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/page2c_en/page2c_en?opendocument (Available in English).
- Office of the Commissioner for Personal Data Protection - Indicative List of Processing Operations subject to DPIA requirements under Article 35 (4) of the GDPR: https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/ED786DE02E8020FCC22582600037714 3/$file/Indicative%20DPIA%20list.pdf?openelement (Available in English).

4.3.7 Poland

The Personal Data Protection Act of 10 May 2018 (hereafter the PDPA) entered into force on 25 May 2018 to help implement the GDPR in Poland. The PDPA does not regulate legal grounds for personal data processing for historical and scientific purposes.

However, some Polish sectoral acts provide specific legal bases for various activities.

The Act of 21 February 2019 Amending Sectoral Acts (hereafter the ASA) introduced changes to the sectoral laws in order to implement the GDPR requirements to the Polish legal system.

In the first place, the ASA adjusts the Act on the Higher Education (hereafter the Act) regulating data processing for scientific research purposes. The changes apply only to the entities and institutions listed in this Act. Under the Act, the processing of special category data for scientific research is permitted provided that the publication of the results takes place in a way that prevents the identification of individuals. Moreover, the Act requires the implementation of specific security measures for personal data processing in relation to scientific research. The Act, following the provisions of the GDPR, allows the exclusion of the Articles 15, 16, 18, and 21 of the GDPR if it is likely that the law specified in these

provisions will prevent or seriously impede research and development purposes and if the mentioned exemptions are necessary to achieve these goals.

Finally, the ASA provides changes to the Act on the Information System in Health Care, under which the data included in the medical records can be made available for the purpose of scientific research only in anonymised form.

- The Act on the Higher Education: http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20051641365/U/D20051365Lj.pdf (Only available in Polish)
- The Act on the Information System in Health Care: http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20111130657 (Only available in Polish)
- List of processing operations requiring data protection impact assessment: https://edpb.europa.eu/sites/default/files/decisions/pl-dpia-list_monitor_polski.pdf (Available in English)

4.4 Evolving European regulatory ecosystem

As the GATEKEEPER project is being implementer, the current European normative ecosystem is evolving rapidly. In particular, the project will need to take into account several legislative proposals made by the European Commission that have the potential to affect the GATEKEEPER project from the point of view of regulatory compliance, business development and sustainability.

A first legislative proposal which needs to be taken into consideration is the Data Governance Act (DGA)[31]. It is a proposal of the European Commission that aims to create a framework to facilitate data sharing. If approved, this piece of legislation will enable the creation of "secure spaces" where different kinds of data, including health data, can be shared and re-used for commercial or altruistic purposes, including scientific research. GATEKEEPER will need to evaluate what will be the impact of this new legislation on its activities. The draft proposal of the Act aims to introduce a "European data altruism consent form" for altruistic data re-use. "Data altruism" and "general interest" as the "consent by data subjects to process personal data pertaining to them, or permissions of other data holders to allow the use of their non-personal data without seeking a reward, for purposes of general interest, such as scientific research purposes or improving public services". E-health related research projects, working in the context of WG5, have already submitted comments to the proposal highlighting a few points that need further refinement. GATEKEEPER has played a leading role in the elaboration of this submission in the context of WG5.

Among the issues worth further analysis are:

- A need to clarify the territorial scope of application of the proposed regulation and also the role and liability of the EU-based representatives.

[31] European Commission, *Proposal for a Regulation of the European Parliament and the Council on European Data Governance (Data Governance Act)*, 25/11/2020, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767.

- A request to extend the scope to non-public entities in health whose data is of great relevance and value (e.g., private not for profit hospitals or third sector organizations providing social care or integrated care)

- Greater clarity about the alignment of the national competent authorities undertaking the Data Governance Act oversight and enforcement with the bodies performing that role for the General Data Protection Regulation

- The different projects welcome, as part of the implementation of data altruism, the introduction of data subject consent for areas of general interest including processing for scientific research purposes that cannot be precisely specified at the time of collecting the consent. However, greater clarity and guidance will be needed on how to remain compliant with the GDPR which requires consent to be specific. Clear and detailed guidance will be required for the public, data intermediaries, research users and regulators to ensure consistent pan-European interpretation and application, and to give confidence to all stakeholders

On April 21st, 2021, the European Commission presented its proposal for a Regulation on Artificial intelligence[32] as part of the European approach to Artificial intelligence legislative package which includes: i) the aforementioned legal framework on AI; ii) an updated coordinated plan with Member States; iii) a new proposal for a Regulation on Machinery products. The proposed regulation joins other EU initiatives in the digital sector (such as the Data Governance Act, Digital Service Act and Digital Markets Act) which are currently being discussed and considered. The proposal of the Commission is based on a risk-based approach which looks at the specific uses of AI and their corresponding level of risk in order to determine the level of requirements they will be subject to. The proposal also includes several provisions aimed at ensuring that the framework remains futureproof for example through the possibility by the Commission of adapting the list of high-risk systems. The proposed regulation includes a number of provisions intended to promote the development and the uptake of AI systems in the European Union. In the context of the regulatory framework envisaged a European Artificial Intelligence Board will oversee and coordinate the enforcement of the regulation.

Importantly, the proposal envisages a two-year period for application following adoption and publication of the final regulation therefore the new requirements could apply as early as 2024. The new European Data Governance ecosystem aims at increasing trust in data sharing, strengthening the mechanisms to increase data availability and overcome technical obstacles to the re-use of data. The research project will also closely follow the developments on common European data spaces in the strategic domain of health. In May 2021 the European Commission also published its Inception Impact Assessment of the

[32] European Commission, *Proposal for a Regulation of the European Parliament and the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts*, 21/4/2021, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

forthcoming Data Act[33]. This legislative initiative will aim at facilitating data access, use and review the rules on legal protection of databases. The initiative therefore aims at ensuring fairness in the allocation of data value among actors of the data economy and has been already considered also by the European Parliament that through the adoption of a report of its Industry, Research and Energy Committee has called the Commission to submit legislation to foster data access and interoperability in the forthcoming Data Act.

4.5 Findings

As it emerges from the mapping of the different legal sources relevant to the project, and from the current evolution of the European normative and regulatory ecosystem, GATEKEEPER will need to closely follow and monitor these evolutions as they will have an important impact on its activities. They will need to be closely discussed at the Business Cluster level. Relevant legislation also impacts the ethical assessment of GATEKEEPER as principles such as transparency, privacy and data protection, respect for human rights and human dignity will need to be further taken into account in the construction of the final ethical impact assessment framework. In this context GATEKEEPER will also need to closely monitor the activities of the institutions and organizations working on the implementation of the European Health Data Space.

[33] European Commission, *Inception Impact Assessment-Data Act (including the review of Directive 96/9/EC on the legal protection of databases)*, available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13045-Data-Act-&-amended-rules-on-the-legal-protection-of-databases_en.

5 GATEKEEPER Data Privacy Policy and internal compliance support structure

5.1 Introduction

The relevance of data protection issues and its intersection with the ethical dimension are of fundamental importance for a proper data management and data valorisation strategy. GATEKEEPER has already implemented in the initial phase of the project the Deliverable 1. Data Management Plan (DMP) which covers both the project and the different pilots. The information shared on the DMP served as baseline towards the identification of some of the issues already addressed in this deliverable. In order to ensure the project's long-term sustainability, work has already begun towards the identification of the necessary contractual and organizational actions that will enable safe and compliant transfers of data in the GATEKEEPER Pilots and the platform as a whole (particularly towards/from the data federation).

5.2 Summary of controller responsibilities

As detailed in the Gatekeeper Data Management Plan and associated deliverables, the project seeks to facilitate the establishment of a multi-centric large-scale pilot on smart living environments. In this context, the project makes available a set of tools for data processing and visualization to the institutions in charge of the project pilots, which have expressly specified the means and purposes of the data processing activities they wish to perform (see D.6.1.2 - Appendix A; D5.2; D5.3; and D.6.3.2).

In this context, alongside with the definition of the means and purposes of the processing to be performed, the project ensures that the initial decision to collect, process and share data remains under the direct control of the corresponding pilots' institutions. The participating local responsible organizations are therefore to be understood as data controllers of the data. The sharing of data with the platform and any relevant processors will be governed by specific agreements which are currently undergoing finalization and signature[34]. As data controllers, the local pilot organizations are also responsible for the definition of any sharing of relevant datasets amongst the consortium or the publication of anonymized data in open access repositories. Pilots are also responsible for the selection, integrity, and compatibility of the data they share with the platform during the project lifetime.

In summary, controllers in the project should:

- Identify relevant national dispositions, guidance and recommendations to be respected by the pilot and associated stakeholders
- Identify relevant personal data flows stemming from the respective pilot
- Generate a register of third parties which may obtain access to the personal data

[34] Current data processing agreements being negotiated/signed are heavily inspired from the EC Standard Contractual Clauses on Article 28 as found in https://ec.europa.eu/info/law/law-topic/data-protection/publications/standard-contractual-clauses-controllers-and-processors_en.

- Maintain records of processing activities detailing: personal data held, source of the personal data, entities/individuals with access to the personal data, detail of processing performed to personal data
- Maintain documentation pertaining: lawful basis for processing, consent forms/ obtained consent and withdrawal of consent by data subjects; privacy notice provided to data subjects, processes in place to recognize and respond to data subjects request to access personal data; processes in place to ensure personal data is accurate and updated; processes to securely delete personal data which is no longer relevant; processes to respond to data restriction requests; processes for data portability and objection requests; anonymization/pseudonymization policies; processes for identifying/reporting data breaches; signed joint data controllership/processing agreements as appropriate; and processes to ensure compliance with signed agreements[35]
- Perform and document a DPIA for the envisioned data processing operations
- Participate in the meetings of the project's Policy, Legal and Ethics Board and share all relevant compliance information with the Board upon request

5.3 Data privacy policy

The project's data privacy policy can be accessed at https://www.GATEKEEPER-project.eu/privacy-policy. A copy is provided below:

The GATEKEEPER project is particularly aware of the importance of confidentiality and protection of personal data of the participants in the European pilot project.

GATEKEEPER is a large-scale multi-centre European pilot on Smart Living Environments. The main objective is enabling the creation of a platform that connects healthcare providers, businesses, entrepreneurs, and elderly citizens and the communities they live in, in order to originate an open, trust-based arena for matching ideas, technologies, user needs and processes, aimed at ensuring healthier independent lives for the ageing populations. The project will demonstrate its value by scaling up, during a 42-months work plan, towards the deployment of solutions that will involve ca. 40.000 elderly citizens, supply and demand side (authorities, institutions, companies, associations, academies) in 8 regional communities, from 7 EU member states.

By means of this Privacy Policy (or Data Protection Policy) GATEKEEPER informs the participants or interested parties of the applications to which the personal data collected in the course of the project is subjected.

In compliance with current legislation on data protection, we inform you that the personal data of participants in the project will be treated in accordance with the provisions of the General Data Protection Regulation (GDPR) of May 25th, 2016, and the state regulations on the subject applicable in the different countries participating in the European project, and by the rest of the laws and regulations mentioned below:

[35] Further details on the specific agreements organized as part of the project shall be provided as part of the D1.4.

- Universal Declaration of Human Rights (UDHR) adopted by the General Assembly of the United Nations in 1948.
- Declaration of Helsinki statement of ethical principles for medical research adopted by the World Medical Association (WMA) and amended in Tokyo on 2004.
- Directive 1999/34/EC of the European Parliament and by the European Council on May 10th, 1999, amending Directive 85/374/EEC on products.
- Directive 2000/31/EC of the European Parliament and of the Council of June 8th, 2000, on legal aspects relating to the information society and electronic commerce.

GATEKEEPER reserves the right to modify this Policy in order to adapt it to new legislation, jurisprudential criteria, practices of the sector, or interests of the entity. Any modification in it will be announced with due notice, so that the updated information of its content is perfectly known.

WHO IS RESPONSIBLE FOR THE PROCESSING OF PERSONAL DATA?

The objective of GATEKEEPER is to align, configure, implement and measure several relevant use cases that provide value for people assisted in 8 deployment sites in multiple European countries: Spain, Cyprus, Italy, Germany, Greece, Poland and United Kingdom. In each of the deployment sites, there are different people in charge of the processing of data, depending on the city where the project has been implemented.

WHICH IS THE PURPOSE OF PERSONAL DATA COLLECTION IN THE GATEKEEPER PROJECT?

Personal data is processed with the aim of working on solutions with technologies for the better quality of life and care. The purpose of the treatment is to carry out the management of stakeholder participation in the project. Likewise, the data may be processed to develop GATEKEEPER's own dissemination activities or to send information about participation in the project to project users.

Personal data of participants will only be used for the development of the implementation in the city where the GATEKEEPER project is developed, being stored with all the possible guarantees of confidentiality and privacy.

WHAT IS THE LEGAL BASIS THAT LEGITIMIZES THE PROCESSING OF YOUR PERSONAL DATA? IN OTHER WORDS, WHAT IS THE CONDITION THAT WE CAN PROCESS YOUR PERSONAL DATA?

The legal basis that legitimates the processing of data of participants in GATEKEEPER is the consent expressed by them, by which will unequivocally be granted that such contribution is considered a clear affirmative act on their part.

HOW LONG DO WE KEEP YOUR PERSONAL DATA?

The data provided will be kept for as long as the interested party does not request its right of suppression. Otherwise, and after the mandatory period of 5 years after the completion of the project, in order to cope with possible internal reviews of this project by the European Union, all personal data will be destroyed.

WHO CAN BE THE CONSIGNEE OR RECEIVER OF YOUR PERSONAL DATA?

Personal data as name, surname, address, telephone number, signature, will not be transferred to other members of the GATEKEEPER project, receivers and providers of services provided, in the territory of a given city, except for the exclusive purposes of installation, technical assistance and verification, always limiting its usage to the purpose justified, as well as the assignments provided for in applicable legislation. No personal data will be transferred to third parties beyond those mentioned. The rest of the data will be computed in a segregated and anonymized way, that it is impossible to link them with the person of the interested party.

INTERNATIONAL TRANSFERS

There are no plans developed for international transfers of personal data.

If you have any questions about this Privacy Policy, please contact us by sending an email to coordinator@GATEKEEPER-project.eu

Table 12: Privacy contacts for consortium members

Organization	DPO contact or Contact Information
MEDTRONIC IBERICA SA	rs.privacyeurope@medtronic.com
ENGINEERING – INGEGNERIA INFORMATICA SA	dpo.privacy@eng.it
SAMSUNG ELECTRONICS UK LIMITED	https://www.europe-samsung.com/gdpr/webform/ch_fr
HEWLETT PACKARD ITALIANA SRL	https://privacyportal.onetrust.com/webform/8c68e411-6bf3-4c9e-8800-9c72d0dc273a/8f599c3a-a3a5-4db9-ae19-2fc954a70130
UNIVERSIDAD POLITECNICA DE MADRID	Proteccion.datos@upm.es
ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	dpo@certh.gr
STMICROELECTRONICS (ALPS) SAS	privacy@st.com

MYSPHERA SL	gdpr@mysphera.com
GEIE ERCIM	contact@ercim.eu
HL7 INTERNATIONAL FONDATION	dpo@hl7.org
ECHALLIANCE COMPANY LIMITED	privacy@echalliance.com
UDG ALLIANCE	admin@udgalliancce.org
MANDAT INTERNATIONAL	https://mandint.org/contact
UNIVERSITEIT UTRECH	privacy@uu.nl
CONSORCIO CENTRO DE INVESTIGACION BIOMEDICA EN RED	info@ciberisciii.es
PANEPISTIMIO IOANNINON	dpo@uoi.gr
FUNDACION TECNALIA RESEARCH & INNOVATION	dpo@tecnalia.com
THE UNIVERSITY OF WARWICK	dpo@warwick.ac.uk
FONDAZIONE POLITECNICO DI MILANO	privacy@fondazione.polimi.it.
MULTIMED ENGINEERS SRL	info@multimedengineers.com
MEDISANTE AG	dataprotection@medisante-group.com
OPEN EVIDENCE	privacy@open-evidence.com
FUNKA NU AB	contact@funka.com
REGIONE PUGLIA	rpd@regione.puglia.it

SERVICIO ARAGONES DE LA SALUD	dpd@salud.aragon.es
SERVICIO VASCO DE SALUD OSAKIDETZA	dpd@osatek.eus
SENSE4CARE SL	info@sense4care.com
TECHNISCHE UNIVERSITAET DRESDEN	informationssicherheit@tu-dresden.de
CARUS CONSILIUM SACHSEN	https://www.carusconsilium.de/contact-info
THE OPEN UNIVERSITY	data-protection@open.ac.uk
HAROKOPIO UNIVERSITY	dpo@hua.gr
ANAPYXIAKI DIADIMOTIKI ETERIA PSIFIAKES POLIS KENTRIKIS ELLADAS AE OTA	https://dccg.gr/%ce%95%cf%80%ce%b9%ce%ba%ce%bf%ce%b9%ce%bd%cf%89%ce%bd%ce%af%ce%b1/
PANEPISTIMIO PATRON	dpo@upatras.gr
SATEGI EVGIRIAS ARCHAGGELOS MICHAEL KAIMAKLIOYY	Info.archangelosmichael@gmail.com
PAGKYPRIOS SYNDESMOS KARKINOPATHON KAI FILON 1986	
IBERMATICA SA	rgpd@ibermatica.com
ASOCIACION CENTRO DE	kronikgune@kronikgune.org

EXCELENCIA INTERNACIONAL EN INVESTIGACION SOBRE CRONICIDAD	
EIP ON AHA REFERENCE SITES COLLABORATIVE NETWORK	info@rscn.eu
BIOBEAT TECHNOLOGIES LTD	privacy@bio-beat.com
FONDAZIONE CASA SOLLIEVO DELLA SOFFERENZA	privacy@operapadrepio.it

5.4 Personal data protection compliance support: communications approach

This section showcases the communications approach that is to be pursued as part of the project's actions towards compliance support and coordination with relevant partners[36].

The various stakeholders involved in the Gatekeeper project have selected Slack as an additional means of communication to be used alongside physical and online meetings in the project. Slack is a messaging app for business that connects people to the information they need. By bringing people together to work as one unified team, Slack transforms the way organizations communicate. Slack helps teamwork in a more connected, flexible, and inclusive way.

We can model the pilot as Slack channel where pilot representatives raise their question. Each Category points to specific person that filters the request (for instance pilot manager

[36] For transparency purposes it is important to note that the proposed partner-specific assessment actions (reported on Section 4.6) were severely disrupted during the COVID-19 pandemic by lack of response to the proposed actions from the diverse project partners despite multiple reminders at various levels (including two express requests during Plenary meetings). This communications and compliance support action is aimed towards addressing the risks generated by this situation.

for Budget transfer process). The relevant person will know how to solve the issue or redirect to who will know it within the GATEKEEPER actors.

Pilot representatives post questions in the channel by using the "mention" functionality they can notify directly to the relevant actor related to the topic of the question that will act only on post where he has been mentioned. The relevant actor looks at the post and if he/she can solve the issue provides a response otherwise he/she will use the "share" functionality to redirect the question to who is responsible of taking care of the issue and will post the response in the channel

The proposed approach will enable more flexible communication and resolution of pending issues throughout the consortium and will be of particular relevance to the project's compliance-related actions. The following images showcase the stakeholder mapping on a per-pilot basis, however it is important to remember that the solution will be available across the consortium, which will enable more flexible communications with all partners and further support to the Policy, Legal, and Ethics Board.

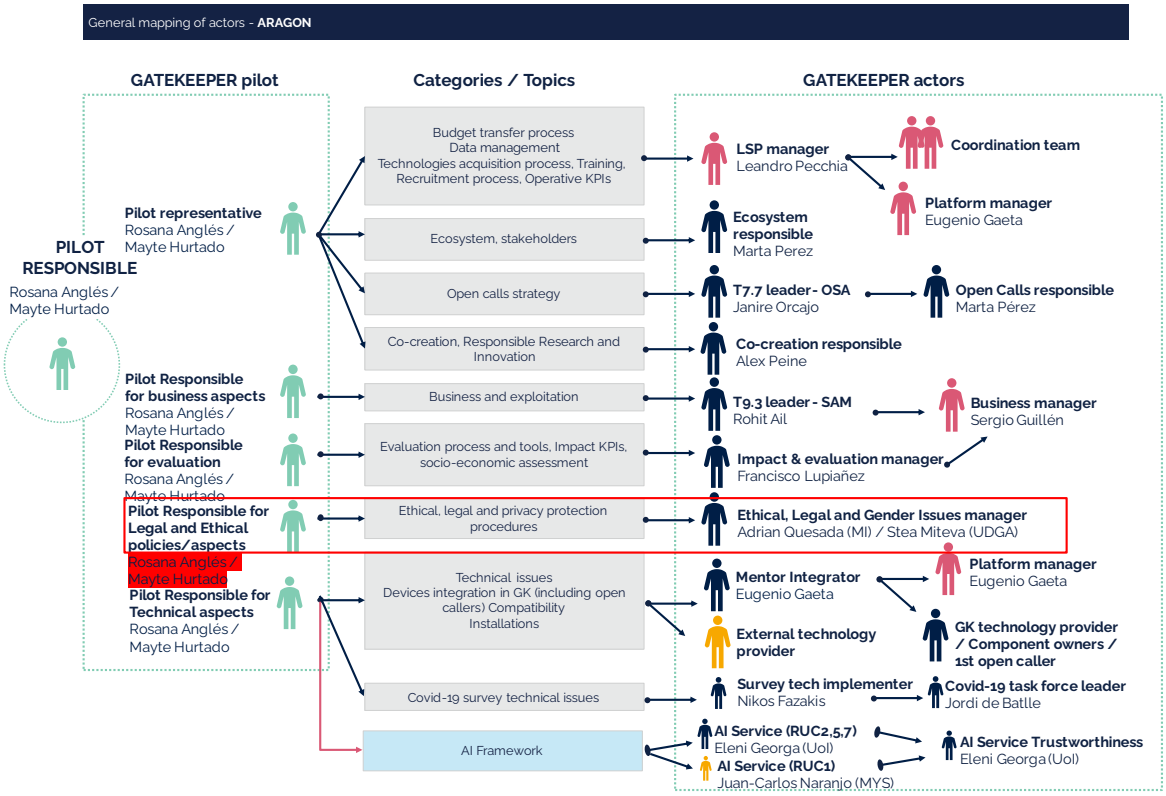


Figure 7: General Mapping of Actors: Aragon

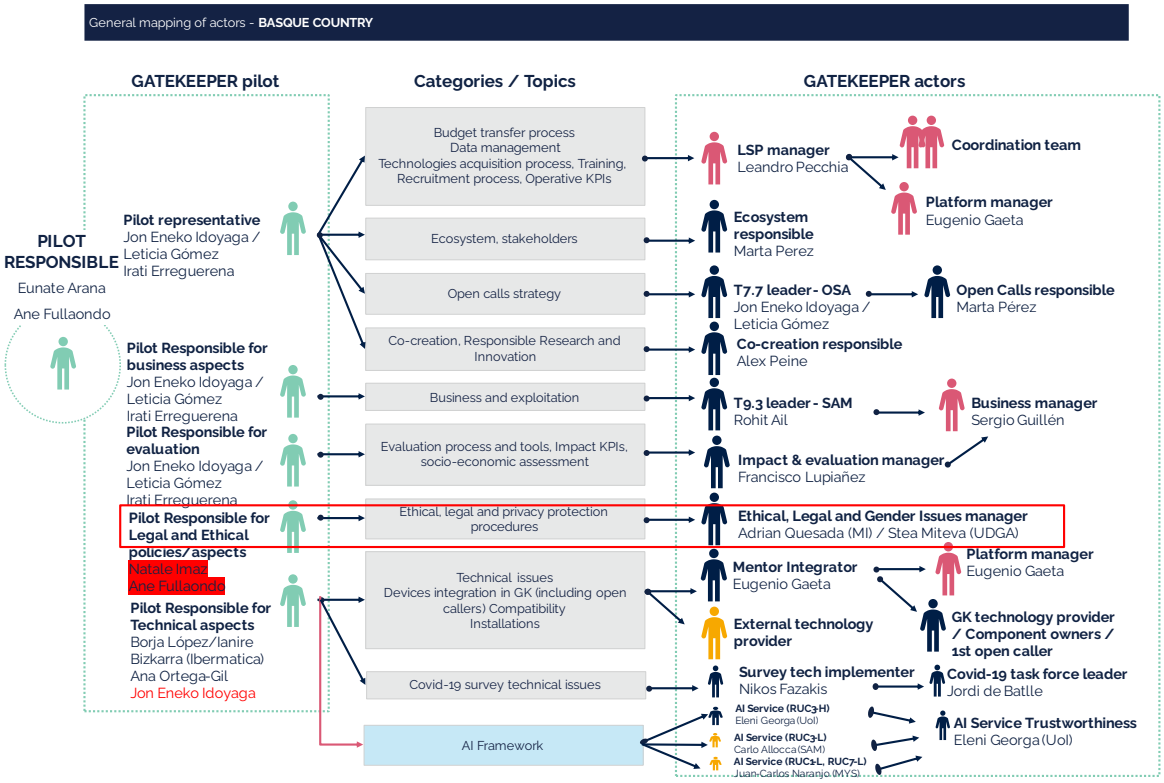


Figure 8: General Mapping of Actors: Basque Country

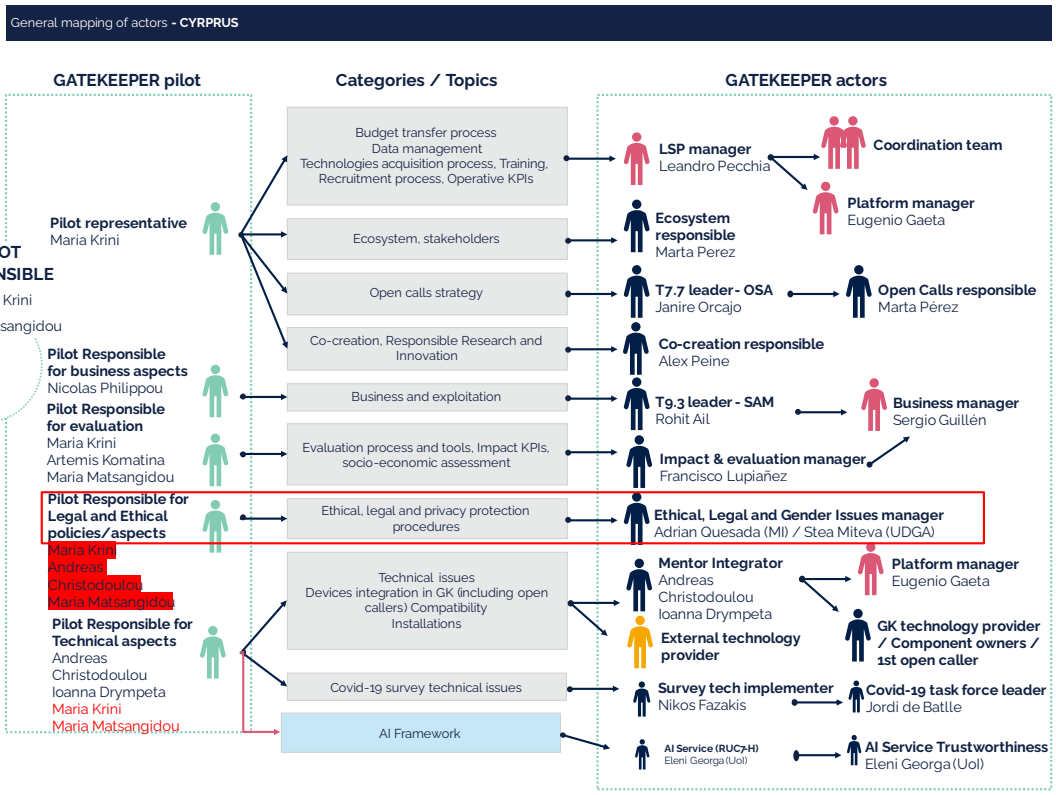


Figure 9 General Mapping of Actors: Cyprus

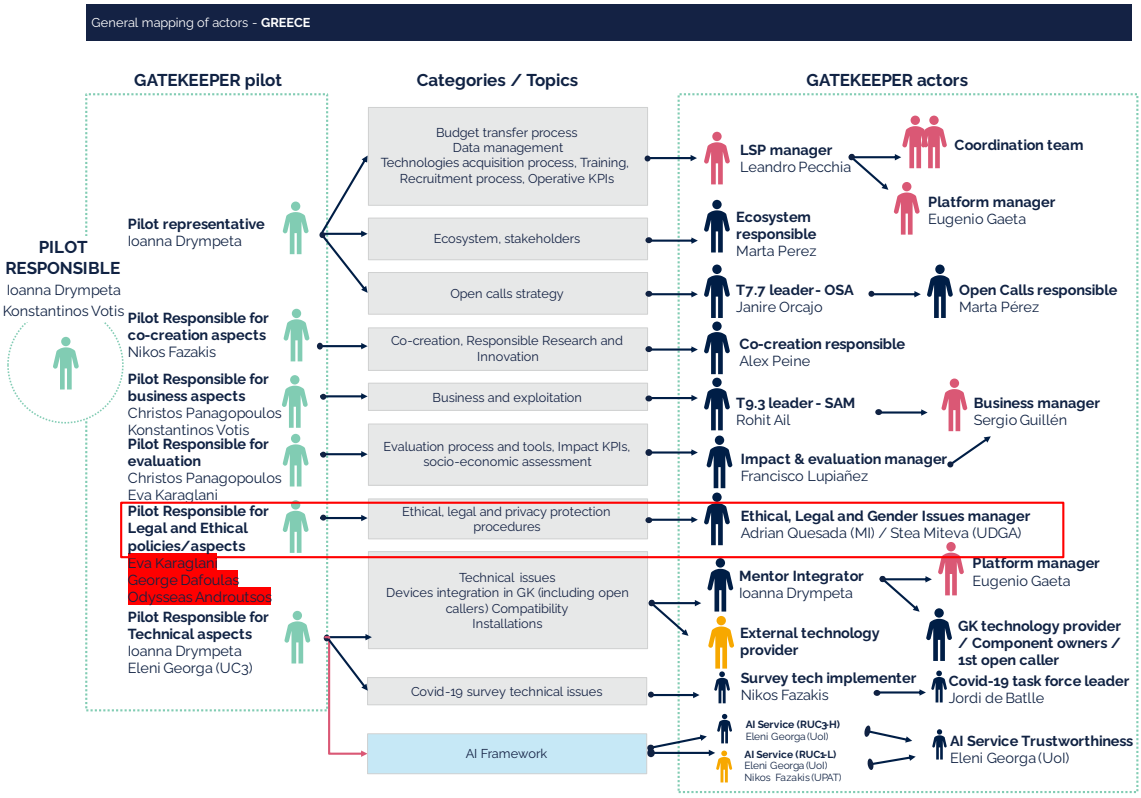


Figure 10: General Mapping of Actors: Greece

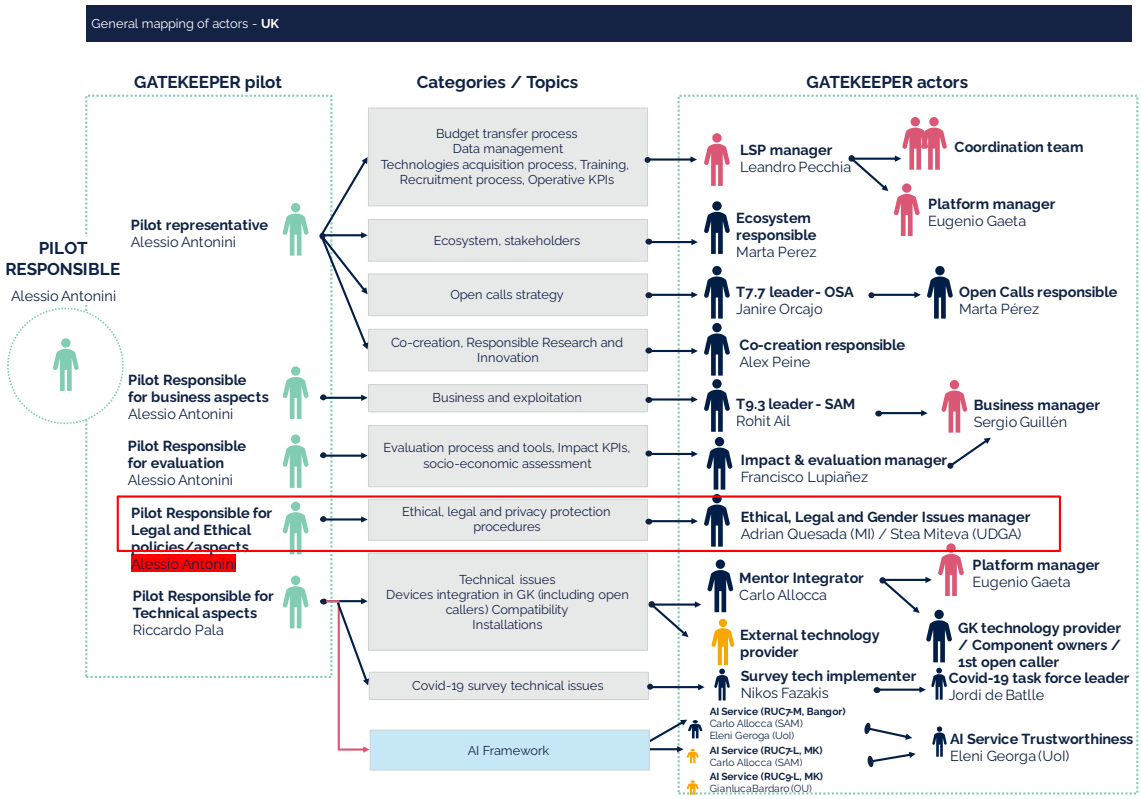


Figure 11: General Mapping of Actors: UK

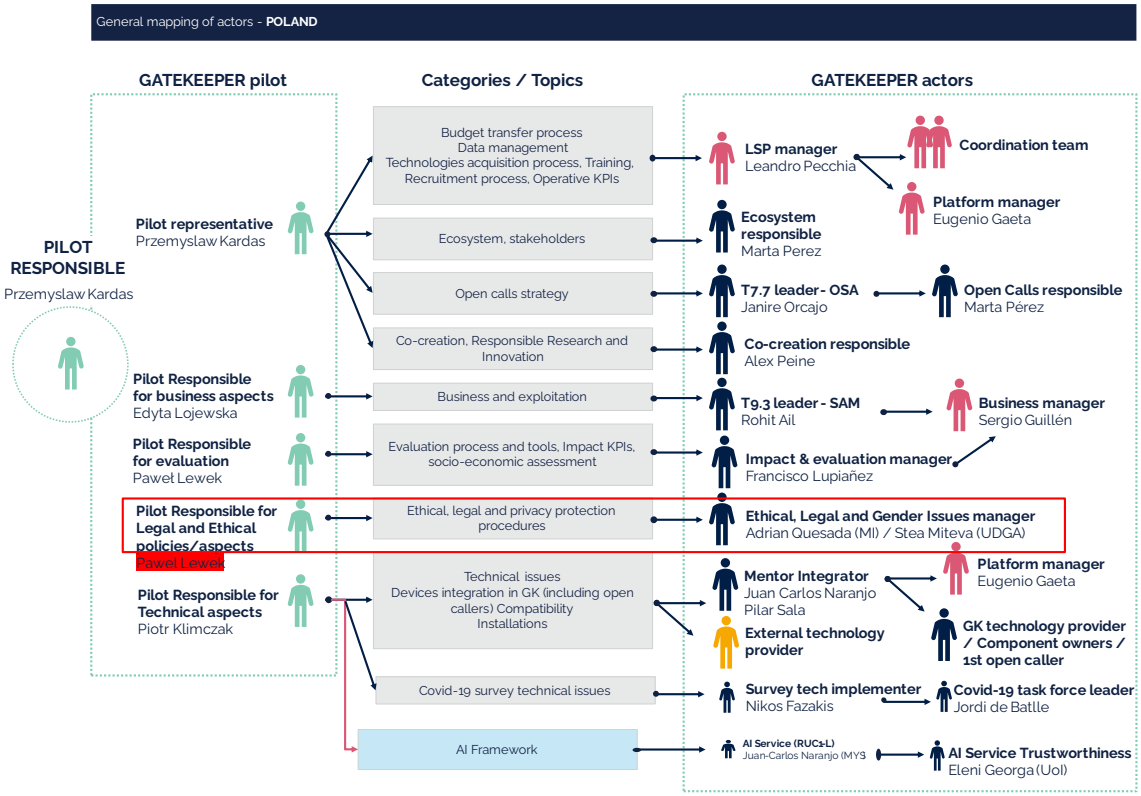


Figure 12: General Mapping of Actors: Poland

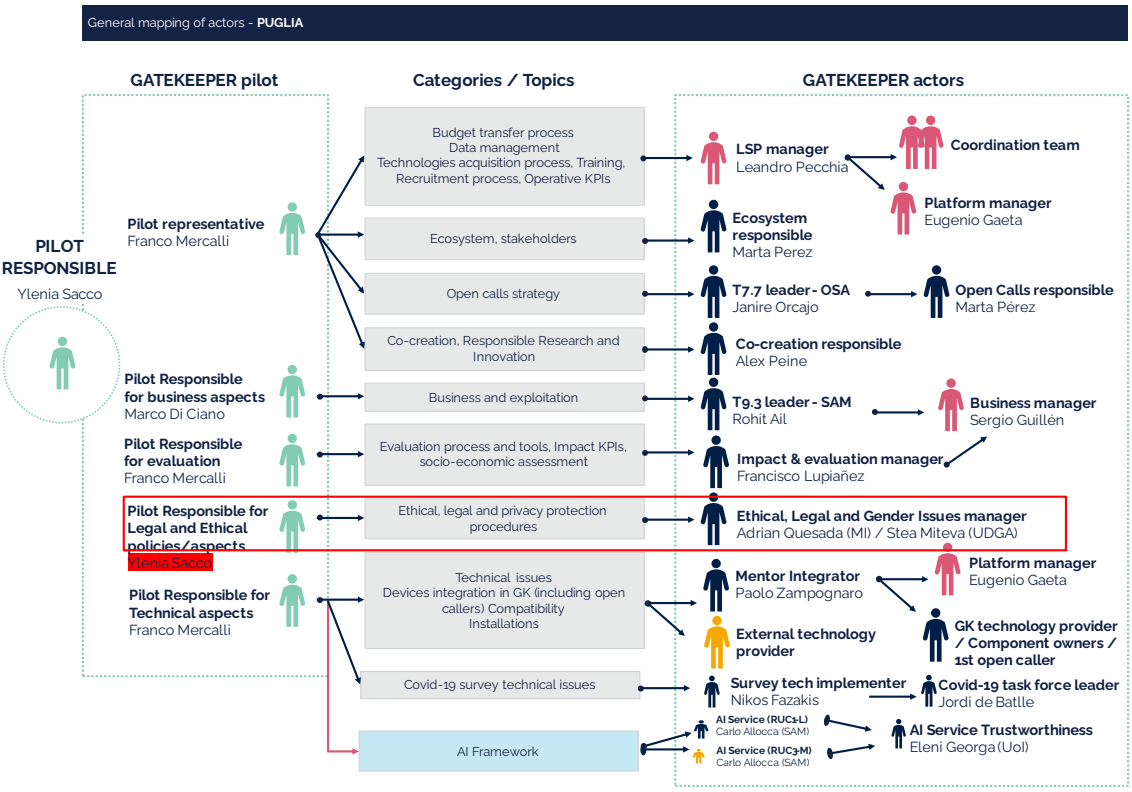


Figure 13: General Mapping of Actors: Puglia

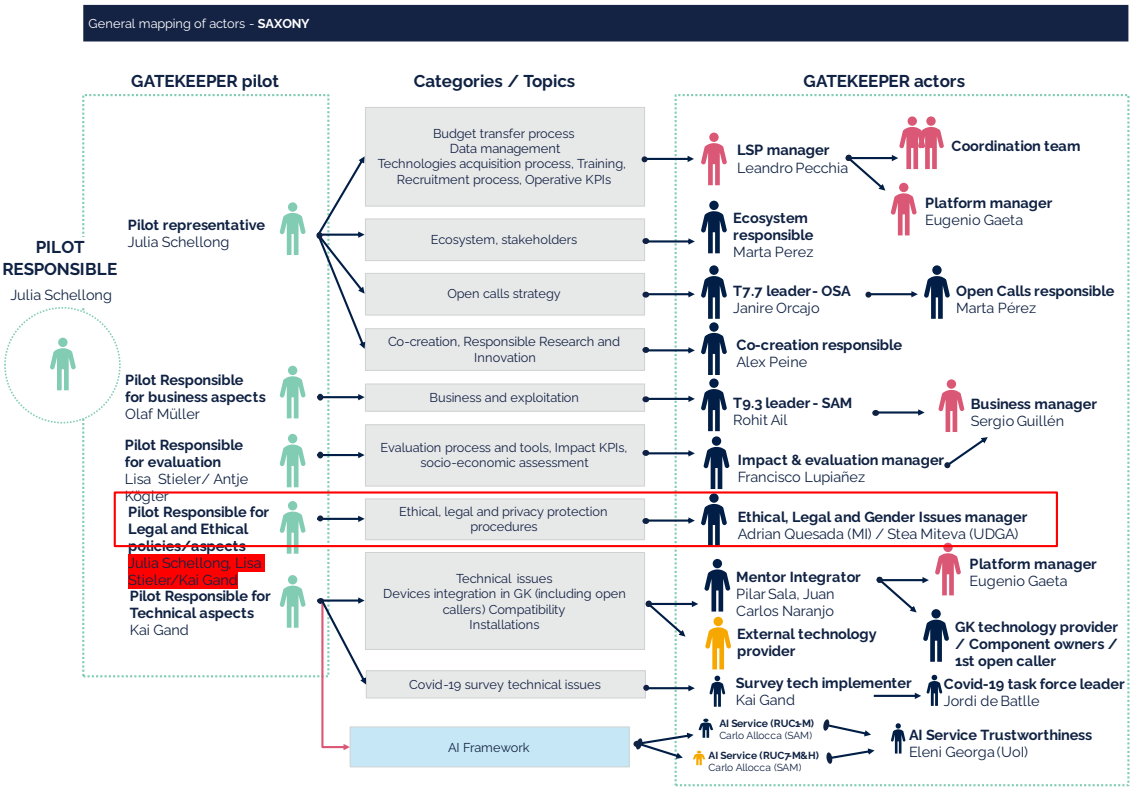


Figure 14: General Mapping of Actors: Saxony

6 Conclusion and Future Work

The GATEKEEPER project deals with important ethical and legal issues which need to be properly tackled to facilitate the deployment of e-health solutions which will gain the trust of the end-users.

The current deliverable pays particular attention to data protection and ethical compliance of procedures and deployments of the pilots and their relations with the other consortium partners in regard to access and sharing of personal data and special categories of data. It presents the state of the art of the project and reports on important actions, such as: evaluation of ethics compliance questionnaires provided by pilots, assessment of dataflows and aggregation of datasets in repositories both in terms of pilot's tenants and GATEKEEPER Data Federation.

The deliverable identifies recommendations for mitigation of potential risks, as well as best practices for compliance with data protection regulations and ethical guidelines to shape the deployment of the project and provide solid grounds for governance and sustainable deployment beyond the lifetime of the project.

This second iteration of the LEEP provides clarifications on the pilot's state of the art, paving the way towards the project's sustainability and data governance approach on multiple levels.

A substantial part of the work done by the Policy, Legal and Gender board in the framework of T1.2 related to pilot consultation, stakeholder mapping, preparation of templates for Data Processing Agreements will be presented in the following iteration of the Data Management Plan, to reason the guidelines and principles on data management, anonymization, pseudonymization, tokenization, synthetic data, etc., that will be introduced.

The work of the PLGB will continue to support pilots and partners on monthly basis to discuss legal compliance and ethical issues which might arise in the context of the project.

Finally, the work will continue to leverage developments in the field of certification and standardisation which will be highlighted in the context the tasks and deliverables in WP8.

Following the identified milestones in the first iteration of this deliverable, it can be highlighted that:

- The mapping of relevant legal and ethical measurements in place by pilots have been completed, evaluated and mitigation actions have been proposed
- The former identified basic principles and checklists have been validated and a further tailoring will be provided, considering the received feedback and the identified needs of pilots and consortium partners
- The previously identified pilots' issues have been further and in-depth explored, and more needs have been identified towards whose mitigation the next efforts of the task will be focused
- The results have inspired discussions and join efforts by the consortium and its leaders to interact in parallel and propose new governance structures and models for sustainability and efficiency
- The Ethical dimension of AI and the involvement of vulnerable individuals have been taken into account, assessed and guidelines and actions for further consideration have been proposed