O{P}ERANDO

online privacy enforcement, rights assurance & optimization

D3.1 Guidelines on legal aspects

Author(s):	Matthias Pocs
Responsible Partner:	STL
Version:	V2.0
Date:	27/09/2016
Distribution level (CO, PU):	PU

Project Number:	H2020 - 653704
Project Title:	OPERANDO

Title of Deliverable:	Guidelines on legal aspects
Due Date of Delivery to the EC:	31/10/2016 (revised version)

Work Package:	WP3
Contributor(s):	Rachael Bartholomew OCC, Luigi Clivati PDI, Juncal Alonso TCN, Gorka Benguria TCN, Leire Orue-Echevarria TCN, Sauro Vicini FCSR, Zeev Pritzker AVO Brian Pickering ITI
Reviewer(s):	Reynold Greenlaw OCC, Rachael Bartholomew OCC
Approved by:	All Partners

Document Revision History

Version	*Date*	*Modifications Introduced*	
		Modification Reason	*Modified by*
0.1	07 July 2015	Document started	Matthias Pocs (STL)
0.2	15 July 2015	1st round of contributions	Rachael Bartholomew (OCC)
0.3	15 July 2015	1st round of contributions	Zeev Pritzker (AVO)
0.4	15 July 2015	1st round of contributions	Luigi Clivati (PDI)
0.5	15 July 2015	1st round of contributions	Juncal Alonso Ibarra (TCN), Gorka Benguria Elguezabal (TCN), Leire Orue-Echevarria Arrieta (TCN)
0.6	15 July 2015	1st round of contributions	Sauro Vicini (FCSR)
0.7	22 July 2015	Review legal / ethical considerations	Brian Pickering (ITI)
0.8	23 July 2015	2nd round of contributions	Juncal Alonso Ibarra (TCN)
0.9	27 July 2015	Technical review of contributions	Matthias Pocs (STL)
1.0	31 July 2015	Quality assurance, finalised, submitted	Rachael Bartholomew (OCC)

1.1	26 Sep 2016	Modified following review report	Matthias Pocs (STL)
2.0	30 Sep 2016	Finalised and submitted	Rachael Bartholomew (OCC)

OPERANDO Consortium Partners and Acronyms

OCC	Oxford Computer Consultants
AVO	Arteevo Technologies
PDI	Progetti di Impresa
STL	Stelar
RMS	RomSoft
TCN	Tecnalia
ITI	IT Innovation Centre, University of Southampton
UPRC	Piraeus University Research Center
FCSR	Fondazione Centro San Raffaele

Glossary of Terms and Abbreviations

ASL	Azienda Sanitaria Locale
B2C	Business to consumer
DRS	Disaster resilient societies
G2C	Government to citizen
OSP	Online Service Provider
PA	Privacy Authority
PbD	Privacy by Design
PDR	Personal Data Repository
PSP	Privacy Service Provider
TFEU	Treaty on the Functioning of the European Union
UPP	User Privacy Policy
WP29	ARTICLE 29 Working Party on Data Protection

Table of contents

Executive Summary

This Deliverable outlines the first phase of work package WP3 for the legal data protection aspects in the OPERANDO project, preparing the WP3 Privacy-by-Design approach and method (Deliverable D3.2 and Task T3.2, respectively). In particular, WP3 aims to solve the extreme difficulty of translating the protection of fundamental rights into concrete indications for technology design.

As it happens with the use cases defined in D2.1 [1] and D2.2 [2], legal aspects are also dependent on the respective market segments supported by the OPERANDO platform. Consistently, we consider the legal data protection aspects of the OPERANDO project used for the market segments of business-to-consumers (B2C) online services (such as social networks like Facebook and LinkedIn) and government-to-citizen (G2C) online services. Privacy regulations for the two market segments of B2C and G2C are different both in nature and in enforcement practices.

For B2C environments, the nature of the personal data to be shared and how it is used is less complex and defined in advance in the OSP's contractual terms and conditions. With G2C market segments, however, the situation is different as personal data, including sensitive data, may have to be used and shared in less clearly anticipated ways motivated by duty-of-care responsibilities of public authorities. Consistently, legal aspects will differ according to the societal challenges to protect: the health of diabetes patients, gambling addicts, children in a hospital, and the security of domestic violence victims or flood victims. It is for the various market segments that WP3 will assess the legal data protection obligations and implications of the OPERANDO algorithms and architecture. WP3 will translate this society-focused approach of the law (different set of legal rules for the societal challenges) to the OPERANDO project and specify technological features across the use cases as far as possible.

Moreover, WP3 will show how the OPERANDO project promotes security technologies and services in the meaning of the EU Horizon 2020 security pillar (e.g. technologies for disaster resilient societies (DRS)) [3]. This is with a view to taking the opportunity to contribute our standardisation proposal planned in WP3, to the work programme of the EU standards bodies which are working on the European Commission standardisation request M/530 on Privacy by Design for the security industry [4], at the same time as the OPERANDO project.

At this stage, WP3 carried out the first iteration of the technical, legal and ethical analysis with leaders of work packages WP4 to WP7. We developed first examples of technical proposals concerning the OPERANDO use cases, which show the relevance of the ethical and legal values and requirements. We developed the preliminary legal requirements for the project definition phase which will serve as input to the marketing requirements definition in Month M6. This Deliverable will be used to verify the Milestone "MS4 2nd prototype – Minimal Viable Product (MVP)" and contribute to the basic working implementation of OPERANDO design, databases, core engines, mechanisms and algorithms.

This deliverable demonstrates that partners organisations of T3.1 have internally initiated the legal Privacy-by-Design process in order to feed the development and integration processes during each phase of the OPERANDO project with ad-hoc consultation of those partners. It is structured according to the various normative levels of ethical values and fundamental rights, legal principles of data protection law and privacy goals of anonymisation, pseudonymised data mining and decentralised systems. In each case, legal and ethical guidance and regulation is summarised along with the specific position that OPERANDO takes with regard to such regulation and guidance.

Whereas WP3 focuses on research about a Privacy-by-Design method for the development of online privacy services for innovative technological concepts, as a societal responsibility of PSPs, WP8 will cover the legal and ethical aspects concerning OPERANDO trials and system deployment fulfilling legal and ethical obligations as data controllers and data processors.

1 Introduction

1.1 Abstract

In the framework of an innovation action, WP3 will address legal data protection aspects that are specific to the OPERANDO technology/service design and development. While customers of the cybersecurity industry bear the legal responsibility relating to technology operation and personal data processing, WP3 focuses on the legal aspects of the early technology design lifecycle stages as a societal responsibility to be met by providers [4].

The purpose of analysing the fundamental rights to privacy and data protection and the other legal aspects in this deliverable is to develop innovative technological concepts which we will use in the OPERANDO project. The strategy of OPERANDO is to reduce the possibility of privacy violations by innovative technology design as a societal responsibility of online services in addition to the conventional technical and organisational mechanisms of enforcement of the current legal requirements.

In general, this approach promotes the legal principle of "Privacy by Design" (PbD) [5] which will probably (during the lifetime of the project) become a legal obligation [31]. Hence, WP3 will focus on the design of appropriate technical proposals for the algorithms and architecture to be developed in the framework of WP4 to WP7.

In addition to the use cases, WP3 will also cover auditing-related aspects. It is important to oversee and verify the processes in the organisations of PSPs and their federations for implementing the high-level legal requirements. This work will be used for checking OSPs and PSPs, for procurement of their services, and supervision by data protection authorities. Subsequent deliverables will also consider the EU regulation aspects for policymakers, DPAs, consumer organisations, and standards bodies.

Concepts developed on the basis of WP3 will be implemented in addition to the algorithms and architecture under the other technical work packages. This aims to create flexibility for consumers and OSPs to set design options appropriate to their individual use case (full functionality) and OPERANDO platform to provide relevant oversight mechanisms in support of possible legal obligations. This will be done through the creation of the Individual User Privacy Policy (UPP) that will be automatically computed from several relevant information including applicable privacy laws. Technical conditions for compliance with privacy laws will be transparently enforced by the Privacy Authority (PA) through the modules of the OPERANDO platform. Whereas in the case of G2C development of middleware for each deployment is needed for a tight integration between the PSP and the OSP, in the case of B2C a stable version of OPERANDO can be deployed as a service to consumers without tight integration with the supervised OSP services.

1.2 July 2016 reviewers' resubmission remarks

The following remarks were made by the reviewers concerning D9.3 in the July 2016 Athens review meeting:

- *The purpose of the deliverable could be served by a more structured presentation, outlining technical proposals/examples per use case.*
- *Furthermore, the methodology used in order to identify legal requirements and their applicability to OPERANDO is not adequately presented.*
- *Hence, a revised version of this deliverable should be produced, in order to describe/reflect the way/methodology the legal requirements were collected, evaluated and finally were selected for the project's purposes.*

Following the review of the first year of the project, we described the methodology for the legal requirements definitions and revised D3.1 to include this description. Consistently, we planned an action item to put the review's recommendations into practice. Additionally, we inserted several new subsections starting with "1.1 Methodology for legal requirements definitions" in the introductory section of D3.1.

After the first review meeting, the Commission recommended the consortium to "resubmit the deliverables D1.6, D2.5, D3.1, D4.2, D8.2, D8.3, D9.2, D9.3, D10.2 following the comments/ recommendations in the consolidated review report". Moreover, the Commission recommended "an action plan on how the consortium will effectively address the review's findings in general, and all the recommendations in particular". In the review report, the Commission requested "a revised version of this deliverable should be produced, in order to describe/reflect the way/methodology the legal requirements were collected, evaluated and finally were selected for the project's purposes". This request was extended in an additional email by the Project Officer to the project coordinator, which is aimed at providing further help to the revision of D2.5 and D3.1, so that D3.1 should not only describe the methodology the legal requirements were collected, evaluated and finally selected, but also how they were finally "applied" for the project's purposes.

In the additional email by the Project Officer, the consortium was also asked to "provide, when applicable, relevant information (results of surveys and/or interviews and any other evidence) on how [it] elicited opinions and feedback (for example in the form of brainstorming or focus groups). The goal [would be] to share how [the consortium] involve the relevant stakeholders in the requirements definition procedure by asking appropriate questions".

Besides, the additional guidance by the Project Officer's email referred to the "new General Data Protection Regulation (GDPR) that will be in force as of May 2018 (http://ec.europa.eu/justice/data-protection/) [which] should be also taken into consideration". Finally, in the additional help provided in the Project Officer's email, the project's reviewers advise the consortium to consider to follow a "similar approach to D3.1 […] for the D2.9 concerning the update of 1st reporting period's D2.6".

1.3 Methodology for legal requirements definitions

The Privacy-by-Design objective of OPERANDO uses a legal approach to enable the assessment against Article 25 of the EU General Data Protection Regulation that will apply from May 2018. This legislative obligation includes the promotion of fundamental ethical and legal values as defined in the EU Charter of Fundamental Rights and the legal principles of data protection. The expected potential social, competitive and economic impact is pursued with the internal informal as well as the external formal standardisation activities. Therefore, the methodologies used for the processing of legal requirements include three layers: the legal methodology and internal stakeholder procedure – on which the consortium focussed in the first project year - and the preparation of formal stakeholder involvement, which has started with year one and will be carried out until and possibly beyond the end of the project's lifetime.

1.4 Legal methodology for OPERANDO

The consortium developed legal requirements in D3.1 and D3.2. In particular, the legal approach is described in the introductory section concerning legal compliance and the subsection on legal principles promoted by the privacy goal in D3.2. In contrast to stakeholder involvement, legal methodology is based on a review of legislation, state constitutions, opinions by regulators and rulings by court as well as papers and commentaries by legal scholars and similar literature. Using established legal methodology, we collected, evaluated, selected and applied relevant rights and freedoms as well as legal data protection principles.

We followed principle of "Data Protection by Design" as defined by the GDPR. The definition in Article 25 GDPR as entered into force on 24 May 2016 (and applicable from 25 May 2018) does not differ from the definition we took into account in D3.2 (submitted on 31 March 2016). D3.2 is based on the GDPR as as politically agreed on 28 January 2016 between the EU co-legislators (see citation of legislation in D3.2, page 8 ("time of determination of means", etc.), as well as references to the GDPR in footnote 1). Since the objective of the principle of "Data Protection by Design" refers to the design and development of technologies, the legal requirements definitions were collected, evaluated, selected and applied having regard to whether and to what extent they have an impact on technology design. The legal data protection principles outlined in D3.1 are based on the provisions of the GDPR. The following table illustrates how the relevant sections 3.1 to 3.9 in D3.1 correspond to the GDPR provisions:

3.1 Lawfulness	• Article 5(1)(a) "lawfulness, fairness", and • Article 6 "Lawfulness of processing"
3.2 Profiling prohibition	• Article 4(4) "profiling", • Article 5(1)(d) "accuracy", • Article 22 "Automated individual decision-making, including profiling"
3.3 Data availability	• Article 1(3) "free movement neither restricted nor prohibited"
3.4 Purpose limitation	• Article 4(13), etc. "genetic/biometric/health data", • Article 5(1)(b) "purpose limitation"; and • Articles 9 and 10 special categories of personal data"
3.5 Data security	• Article 5(1)(f) "integrity and confidentiality", • Article 32 "Security of processing", • Articles 33/34 "data breach"
3.6 Data subject rights	• Article 4(11/24) "consent/objection"; • Article 5(1)(a) "transparency"; • Articles 7 and 8 "Conditions for consent"; • Articles 12 to 21 "rights of the data subject"
3.7 Anonymity	• Article 1(1) "Subject-matter", • Article 2(1) "Material scope", • Article 4(1/5) "personal data/pseudonymisation", • Article 5(1)(c/e) "data minimisation/form which permits identification", • Article 11 "not require identification", • Article 25 "Data protection by design and by default", • Article 89(1) "data minimisation/pseudonymisation"
3.8 Responsibility	• Article 4(7 to 10) "controller, processor, recipient, third party"; • Article 5(2) "responsible"; • Article 24 "Responsibility of the controller"; • Article 26 "Joint controllers"; • Article 28 "Processor"; • Articles 29 and 30; • Articles 44, etc. "transfers"
3.9 Accountability	• Article 5(2) "accountability"; • Article 24(3) "demonstrate compliance"; • Article 31 "Cooperation with the supervisory authority";

	• Article 35 “Data protection impact assessment”; • Article 36 “Prior consultation”; and • Article 37 “Data protection officer”

Moreover, the OPERANDO project took as a starting point the goals defined by the European data protection authorities (see references in D3.1), in the light of which the legislative requirements should be applied. Besides, the only example of a technical measure for compliance that Article 25 mentions, is pseudonymisation. This Privacy-by-Design approach (D3.2) is in line with this EU legislative incentive for privacy innovation projects. Another criterion of the legislative duty of data protection by design is to meet take into account the “rights and freedoms” of individuals. We addressed this criterion with our deliverable on ethical guidelines in D3.1, in particular, using the EU Charter of Fundamental Rights. In addition, the legal methodology also covers the exploitation of the legal work as an accountability measure. In order to demonstrate compliance with the legal obligation of data protection by design in line with Articles 5(2), 24(3) and 31 GDPR, WP3 deliverables will document the project’s management concerning the above-mentioned criteria of data protection by design. They will enable public procurers and other responsible organisations to demonstrate compliance with Article 25 GDPR.

1.5 Internal stakeholder involvement

In the first project year, the objectives of WP3 focussed on the legal methodology as planned in Annex I. Beyond that, we carried out the first iteration of the technical, legal and ethical analysis with leaders of work packages WP4 to WP8. The planned methodology for feedback between lawyers and engineers (Annex I, Part B, p. 14), which entails a scientific multi-disciplinary approach with contributors in their expert capacity irrespective of any formal delegation by stakeholders (see also [7]). This includes the project’s partners who contributed expertise on various relevant technological domains, that is, expertise on: privacy technologies and identity management solutions, security threat analysis, technology sectors such as cloud computing, technology applications in market segments such as healthcare as well as ethics in computer science. Indirectly project partners also represent several stakeholder groups: SMEs, academia, research organisation, lawyers, IT consultants, etc.

The methodology for this internal stakeholder involvement was used to evaluate and finally select and apply the legal requirements definitions previously processed using the legal methodology to OPERANDO. In order to implement legal requirements, the WP3 leader requested, coordinated and consolidated contributions by partners, as described in the document revision history and the subsection on alignment with use cases of trials partners in D3.2 as well as the revision history, executive summary and introduction of D3.1.

Moreover, he distributed a survey on data types and processing logic for inputs by partners. This was done using Excel spreadsheets, which were structured according to the project partner’s competence (e.g., privacy-enhancing cryptography) and use cases (Online advertisement, Food Coach, West London Alliance, etc.). Questions were drafted using the individual use-case descriptions, to ensure that each partner receives so specific requests that only that individual partners can answer.

The WP3 leader coordinated contributions from OCC, PDI, TCN, UPRC, FCSR, AVO and ITI using the JIRA project management system and the OwnCloud document management system. Moreover, he actively participated in the consortium’s fortnightly progress teleconference calls by proposing the legal requirements definitions on the agenda for discussion. In order to protect the interests of internal stakeholders involved, the WP3 leader marked draft documents “confidential”.

1.6 External stakeholder involvement

The process of evaluation, selection and application of legal requirements definitions would be repeated externally in any formal stakeholder forum, which is beyond the control of the consortium. As demonstrated in the first year through meetings with the European consumer organisations and the application by the OPERANDO project for liaison with the official European Standardisation Organisations, we started to prepare our contributions to the formal stakeholder involvement in the legal requirements definitions procedure. This aims to convince European standardisers to re-use the requirements definitions that have been accepted by means of the procedure of the OPERANDO consortium, for the standardisation of European online privacy services in general.

In particular, the legal requirements definitions in D3.1 were presented to the only officially recognised European consumer organisations ANEC and BEUC for feedback in the User Advisory Board meeting in Bologna (September 2015). Moreover, we discussed D3.1 in the annual meeting of ANEC's Digital Society WG in Berlin (May 2016).

An action plan on how the consortium will effectively involve the relevant stakeholders in the legal requirements definition procedure will be defined in T3.3. For developing a standardisation proposal, we will initiate a dialogue with consumer privacy stakeholders. That task will run during the second half of the project's lifetime. In particular, the results will be assessed against its ease of use by industry and the priorities of the standards committee, to which we will contribute our standards proposal.

To help demonstrate consumer protection to ANEC, the legal approach described in the previous subsections uses a methodology defined by ANEC in their comments to the consultation by the European Commission on the standardization request addressed to the European Standardisation Organisations CEN, CENELEC and ETSI, in support of the implementation of a privacy management in the design and development and in the production and service provision processes of security technologies (ANEC-ICT-2014-G-020final, http://www.anec.eu/attachments/ANEC-ICT-2014-G-020final.pdf). This methodology was accepted by the competent Commission DG and finally included as requirements for the development of standards on "privacy by design" for delivery by 2019 (see identical wording in M/530).

Furthermore, we aligned D3.1 with standardisation developments concerning "privacy and data protection by design" of the European Committee for Standardization (CEN) and the European Committee for Electrotechnical Standardization (CENELEC). For this, the OPERANDO project applied as a liaison organisation according to EU Standardisation Regulation 1025/2012, for approval by the CEN-CENELEC Joint Working Group 8 "Privacy management in products and services" and participation in that standards committee. This will allow us to provide input to the committee as we develop our standard proposal. The WP3 leader uses experience he gained as ANEC Representative and his experience as ANEC Head of Delegation in that committee.

At the same time, we also propose to act as a communication channel for other DS-1 projects with this committee, consolidating contributions to JWG 8 drafted by the DS-01-2014 projects. It is important to build alliances that support privacy innovation in the standards committees. Interested stakeholders from the 33 member countries of European standardisation (EU28, EFTA, Turkey, Macedonia), can influence the standardisation activity on data protection by design. Privacy innovators are just one of the many stakeholders represented in the standards committee. Therefore, it will be important to enable standardisers to consider contributions for online privacy services as new "products" in the market, as opposed to more conventional business models of the privacy consultants (e.g., on privacy in human resource management).

1.7 Reflection of methodology

One of the features of the methodology for legal requirements definitions collection, evaluation, final selection and application for OPERANDO's purposes is the legal methodology. The legal approach

taken in OPERANDO entails the benefits of efficient translation of fundamental rights into technology design. Moreover, it promises to guarantee a high level of privacy and personal data protection for citizens, supported by technical measures. However, where the legal framework is vague or not specified yet, political approaches of stakeholder involvement can add to the legal approach. That is why the project is managed to include contributions to the legal requirements definitions procedure by different internal stakeholders and in the second half of the project, in external formal stakeholder fora.

Another feature of the methodology of requirements definitions is the project's focus on the principles of data protection by design, instead of planning work concerning all the provisions of the GDPR or any other piece of data protection legislation. This emphasis has the advantage that the strength of the consortium's composition, that is, the ability to design and develop technology, is made use of. However, the project's approach also means brings about dependency on a certain provision of the legislation and the way it is enforced by the supervisory authorities. In order to compensate for any disadvantages, we enriched the approach by having included work on other provisions of the new GDPR such as the rules for certification and accountability.

2 Normative ethics

WP3 analyses ethical issues as covered by European fundamental rights and freedoms that are associated with the OPERANDO objectives. As theories that prescribe how people ought to act towards one another and their environment, ethical norms are in particular defined in constitutional law such as the European Charter of Fundamental Rights [5]. As a yardstick, we take the fundamental rights of the citizens to specify what they mean for privacy of citizens in online services (see on the concept of legal technology design [7]).

2.1 Fair decision-making

According to paragraph 2 of Article 8 of the EU Charter data must be processed fairly. This is specified by the fundamental right to an effective remedy according to Article 47 of the EU Charter which entitles everyone whose rights and freedoms guaranteed by the law are violated to an effective remedy before a tribunal. Everyone has a right to a fair hearing by an independent and impartial tribunal and to the possibility of being advised, defended and represented. This right includes the need to resolve false system decisions as an anticipated fair trial.

For the OPERANDO use cases, we developed first examples of technical proposals, in particular, concerning OPERANDO data analytics that support fair decision-making for the online services provided to citizens and consumers. In the UK public administration use cases, professionals providing care will still make the decisions for services provided to a citizen before the data (personal data, financial data) is stored in OPERANDO-enabled systems. The big data analytics used for local authorities will be used to guide decision making of humans, for example, forecasting budgets for the area. The analytics would be used to look at how much care or services were going to be needed for the next time period, and how much of these services the local authority need to fund. This decision is made in a similar way currently, just without such comprehensive analytics to guide them.

In the Food Coach use case at Ospedale San Raffaele, fair decision-making will be promoted by helping users check the accuracy of the analysis of their habits and preferences. Personal data are analysed in order to find patterns that can help isolate key variables such as nutritional and lifestyle habits and food preferences structured in four sections (Profile, Diary, Diet and Planner). The semantic-ontological engine will automatically find patterns with the user's preferences or a questionnaire which can be verified by the users.

The ASL Bergamo and Istituto Pediatrico Giannina Gaslini use cases will support fair decision-making using organisational measure. They clearly define a supervisor responsible of the service and the owner of the substitutive power. In case that the supervisor does not act as requested by the user for the defence of his rights, the owner of the substitutive power will reply to the request of the user acting as requested or explaining the omission of the supervisor.

2.2 Privacy & data protection

According to Articles 7 and 8 of the EU Charter people have the right to protection of their privacy and personal data. The right to privacy entitles everyone to respect for his or her private and family life, home and communications. The right to data protection entitles everyone to the protection of personal data concerning him or her. According to Article 8 (2) ersonal data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. The Charter also guarantees that everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Article 8(3) stipulates that compliance with these rules shall be subject to supervision by an independent authority.

European data protection legislation, most notably the EU Data Protection Directive [27], is made up of a broadly recognised set of principles: lawfulness, profiling prohibition, data availability, purpose

limitation, data security, data subject rights, anonymity, responsibility and accountability. The data protection principles are used to prepare justifications for and inspire certain technological design decisions in OPERANDO.

Moreover, privacy is specified by legislation protecting confidentiality and security of electronic communications. In the context of B2C online services, EU ePrivacy Directive [29] extends the scope of legal protection beyond the processing of personal data to also include the integrity of equipment and services used for consumer communications (cookies, spyware, viruses, etc.) as well as traffic data (IP address, connection start/end times, etc.) and information stored in the consumer's equipment which are both broader notions than the concept of personal data.

Legal data protection principles in the OPERANDO context will be specified in the subsequent section 3 of this deliverable.

As mentioned above, the strategy of OPERANDO is to reduce the possibility of privacy violations by innovative technology design as a societal responsibility of online services in addition to the conventional technical and organisational mechanisms of enforcement of the legal requirements. For the B2C case this means, for example,

- automatic lockdown of privacy settings of Facebook to their most stringent values,
- automatic watchdog of privacy setting possibilities and advising the user when a new privacy setting option becomes available, and
- blocking 3rd-party tracking of users as they surf the web.

2.3 Consent & autonomy

Article 8(2) of the EU Charter requires personal data to be processed on the basis of consent of the person concerned or some other legitimate basis laid down by law. Consent is defined in Article 2 of the Data Protection Directive 95/46/EC (soon Article 4 of the EU Data Protection Regulation, see COM(2012) 11) and by European data protection authorities [22] (informed, explicit and freely given consent). For example, consent is not freely given and thus unlawful if an OSP ties it to the conclusion of the service contract. The requirement of consent stems from the autonomy of citizens which is also guaranteed by Article 6 ("everyone has the right to liberty"). In particular, consent is one of the two prerequisites to lawful data processing.

Moreover, online services are required to ask for "opt-in" consent by the EU ePrivacy Directive [29] and its Article 5(3) amended by the EU Cookie Directive [28]. Accordingly, consumers' consent limits data processing to what is necessary (in a legal sense) to provide the service requested by users. This limitation is particularly relevant for 3rd party advertisement, 1st party analytics, social plug-in tracking cookies in the social network services context [16] [20] [23] [24] [25]. Concerning the opt-in approach, some national laws that are in line with the EU ePrivacy Directive such as the German Telemedia Act [30] promote OSPs pseudonymising online profiles, by relaxing the requirement of consent to the right of users to opt out of cookies and other online data processing. Such legislation is particularly beneficial to PSPs developing PbD solutions such as OPERANDO.

For the OPERANDO use cases, we developed first examples of technical proposals, in particular, concerning the OPERANDO dashboard ensuring that users stay in control and set their own privacy policies. Details are set out in the use cases document D2.2 [2]. In the UK public administration use cases, service users who have their details stored in OPERANDO-enabled systems will be able to use an OPERANDO dashboard. This dashboard ensures that these citizens stay in control of their data, by allowing the user to set their own user privacy policies by answering simple, understandable questions. These privacy policies are then used to control access to the service users' data. The dashboard also shows the user a log of requests for access to their data, both accepted requests and denied requests. In this way, the dashboard demonstrates to the service user how their privacy policy is being met. Users' control over their data is particularly important in the use case of a

domestic violence victim, as information about their location for example needs to be protected. In this case, the ability to control release of this information is key.

Similarly, in the disaster resilience (DRS) use case, when the user sets their user privacy policy via the dashboard, they will be asked questions and given the opportunity of consent by marking a checkbox labelled “I consent for OPERANDO to release my address and health status to emergency services in case of a large scale incident such as flooding”. Only if they consent, the locations of vulnerable adults will be used to alert the emergency services in the event of a disaster like a flood.

In the Food Coach use case, the information engine will ask the end user for a specific informed consent. It will inform, involve, offer choices with consent as a way to protect confidentiality and security from harms that could result from data disclosure. Users will be able to grant access of their data to other users such as doctors, family members, caregivers, pharmacists, etc.

Concerning the ASL Bergamo and Gaslini use cases, the users will be able to check and define which kind of data are stored, who can view it, and which kind of use they will be subject to. For example, in the ASL Bergamo Gambling service, a user can decide if his own data (amount of money played, if he drinks while he plays, how often he plays, etc.) can be anonymized and used by different departments of ASL for a reason other than the gambling addiction cure process.

All in all, the OPERANDO PA platform will enable the delivery of privacy services to end users through the enforcement of the User Privacy Policy (UPP) (set up by the user) and the logging and reporting of access to the personal data. This will allow the user to get reports about the use of this personal data and where relevant, partake in its monetisation. The UPP concept will be validated under the conditions of the various use cases, with their own specificities and needs.

2.4 Non-discrimination

The EU Charter also prohibits unjustified discrimination of citizens. This would contravene the equality rights enshrined in Article 21 of the Charter. Article 24 relates to the rights of the child and provides that the EU recognises and respects the right of children to protection and care as is necessary for their well-being and that in all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration. In particular, the rights of children are protected in EU data protection law [14] [15] [20].

Article 23 of the Charter guarantees that the equality between women and men must be ensured in all areas including measures providing for specific advantages in support of domestic violence victims. Similarly, Article 33 of the Charter relates to the right of family life and grants the family social protection. In Article 34 the EU recognises and respects the entitlement to social security benefits and social services providing protection. In addition, Article 38 of the Charter relates to the protection of consumers and provides that the EU recognises and respects that its policies must ensure a high level of consumer protection.

For the OPERANDO use cases, we developed first examples of technical proposals ruling out discrimination of vulnerable categories of data subjects. In the Hestia use case, domestic violence victims are referred to receive support services. Information about them is shared in situations of emergency, e.g., to the police. For this, the OSP asks for consent to such an information sharing mechanism and carries out case-by-case assessments of lawfulness and proportionality, before emergencies are communicated to the police or similar recipients to ensure acting in the best interest of vulnerable categories of data subjects.

With regard to health, OPERANDO will not diagnose or advise on any health (mental or physical) issue, but simply provide alerts and information if appropriate. OPERANDO further undertakes, within the constraints of the law and individual consent, to alert users of any potential health or other issues which they should then pursue with the relevant experts.

The Food Coach use case will support the rights of vulnerable citizens, for example, in relation to clinical data. Moreover, the system will prevent the potential of discrimination based on group profiling. The use of algorithms and advanced data analytics will be carefully monitored for potential discriminatory outcomes for disadvantaged groups. An extreme example would be that data is disclosed about a child that is overweight or obese. This form of information discovered by data analysis could result in stigmatisation, cause injustice and reduce opportunities of the child. Investigation will be done to identify practical ways of protecting data that could lead to harmful forms of disclosure to vulnerable individuals.

In the ASL Bergamo and Istituto Pediatrico Giannina Gaslini use cases, all information about categories of users in need of special protection (i.e., children) will be managed and controlled by a supervisor that is legally authorised to access the specific information (the parents of a child).

Compared to B2C online services, in the use cases mentioned above, there are particular benefits to local authorities using OPERANDO to store and access the data for vulnerable individuals. With regard to emergencies, within the constraints of agreed consent and data usage, OPERANDO will undertake to support the time-limited sharing of data in pursuit of the safe management and resolution of specific crises with emergency services on a need-to-know and by-consent basis.

All in all, the OPERANDO platform will provide appropriate audit and reporting tools to be able to report access to services and any automated decision making to demonstrate non-discriminatory treatment of users. The platform will provide means to classify personal data by their sensitivity (low to extreme), economic value (low to extreme) and the type of online service allowed to access the personal data (e.g., health data only accessed by healthcare institutions).

2.5 Human dignity

Article 1 of the EU Charter defines human dignity as an inviolable human right. In contrast to other fundamental rights that are not automatically violated if an action interferes with them, human dignity must not be restricted. With regard to the processing of personal data this means that profiling of citizens using unique personal identifiers to connect databases related to them, must be avoided [26].

For the OPERANDO use cases, we developed first examples of technical proposals, in particular, concerning the OPERANDO PA preventing personal data from being used as unique personal identifiers to connect databases creating a comprehensive personality profile. This is particularly important in the UK public administration use cases where service users receive social care and support services. The OPERANDO's access restriction will uphold their dignity by preventing others knowing about the care they receive.

The ASL Bergamo and Ospedale Gaslini use cases will prevent profiling and strengthen dignity by means of automatic anonymisation linked to the medical purpose for which citizens' data are collected. Only the authorised medical personnel can identify a person and only for processing of the information needed for the pre-defined medical purposes. In particular, in Ospedale Gaslini, the automatic system of anonymisation ensures that only the doctor authorised by the user can identify that user.

In the B2C uses cases of social networks, OPERANDO will prevent the tracking and to a certain extent, the profiling of the users.

All in all, the OPERANDO platform strives to significantly enhance user control over personal data and support the commented situations in each use case. It will enable the user to refer the OSP to the PA for getting only the specific personal data allowed in the UPP. This will mitigate the risk of OSPs harvesting large amounts of personal data that could otherwise finally lead to creating a unique personal identifier.

2.6 Health care, public security & online business freedoms

According to the first paragraph of Article 168 of the Treaty on the Functioning of the European Union (TFEU), a high level of human health protection shall be ensured in the definition and implementation of all European Union policies and activities. As an expression of solidarity the Charter guarantees in Article 35 the fundamental right of access to preventive health care and the right to benefit from medical treatment under the conditions established by national laws and practices.

Moreover, citizens have a fundamental right to security from domestic violence, natural disasters and other threats according to Article 6 of the Charter. Concerning domestic violence, Article 8 of the TFEU stipulates that the EU must aim to eliminate inequalities between men and women which according to the Declarations to the Treaty of Lisbon of 13 December 2007, includes the combatting of domestic violence and support of victims. In relation to disaster resilience, pursuant to Article 196 of the TFEU, the EU must ensure civil protection by encouraging cooperation between Member States in order to improve the effectiveness of systems for preventing and protecting against natural disasters. EU action must support Member States' action at national, regional and local level in responding to natural disasters within the EU.

These EU freedoms and values include the right of diabetes/obesity patients, gambling addicts, children in hospitals, domestic violence victims, and flood victims to access technology.

With regards to eGovernment, in some countries, services are provided through a broker which holds personal data in a secure central data vault where the broker manages information and protects it for the user from uncontrolled release to public service agencies [21].

Concerning social networks, consumers benefit from the additional service such businesses provide. PSPs, social network service providers, ad network providers and advertisers are protected according to Article 16 of the Charter that recognises the freedom to conduct a business. For example, the EU ePrivacy Directive [29] explicitly recognises the consent-based economic exploitation of data for value-added services.

OPERANDO will help OSPs provide more efficient and improved online services by making available data and services to the users, creating tremendous opportunity to improve EU public goods such as health care, public security and online privacy services, and helping European economy grow. In the Hestia use case, OPERANDO will enable more effective support services for service users such as domestic violence victims. The availability of the data store and the easy-to-set UPP and consents allows access to the user's data and more coordinated care for the service user, with service providers able to access the right data at the right time. Equally, in the DRS use case concerning wide-spread emergency situations (e.g. flooding), access to the location data of vulnerable adults (where they have given consent) for the emergency services allows an improved and informed response.

In the Food Coach use case, OPERANDO will increase secure access to information for a variety of users with emphasis on the ability to correct or suppress inaccurate information. The system will integrate, analyse and generate reports (for personal use only) with summaries of patients nutritional history and physical activity. In addition, OPERANDO will promote personal well-being and self-empowerment through technology. The platform tools will make personal data actionable, discoverable and meaningful with real-time queries that will guide personalised healthy food choices to improve users' quality of life. Moreover, the user will be free to opt for releasing his or her data and reports for public health surveillance.

The services of ASL Bergamo and Ospedale Gaslini will provide a new way to keep in touch with the two authorities. For example, it will be easier for a potential patient to subscribe to the gambling addiction services of ASL Bergamo and to safeguard his or her privacy more efficiently, thanks to the online system instead of going physically to the offices.

All in all, the concept of classification of the personal data in the OPERANDO platform will provide the means to adopt these additional data and service availability support by evaluating the value, in a technical meaning, of the "sensitivity" attribute of its specific personal data type for the purposes of OPERANDO. This way, the OSP can provide more value added services offered by the PA. This will derive in a more effective support of the delivered services.

2.7 Proportionality & mission creep

Since information and communication technologies interfere with the fundamental rights and freedoms mentioned above, one must respect the principle of proportionality as defined in national constitutions and the EU Charter. For example, Article 52 of the Charter stipulates that any limitation on the exercise of the rights and freedoms recognised by the Charter are subject to the principle of proportionality and limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. Accordingly, the benefits for health care, public security and online business freedoms must be balanced with the impact on users' rights and freedoms.

The principle of proportionality includes the prevention of mission creep, also referred to as "function creep". In consequence, service providers must take measures against misuse of technology originally intended for the legitimate uses of health care, public security, and online business freedoms. This applies to EU data protection law and the context of security authorities and detection technologies [19].

For the OPERANDO use cases, we developed first examples of technical proposals, in particular, concerning the OPERANDO Private Data Repository where data will be irreversibly transformed in a way that they can only be used for the original purposes for which auxiliary data are available. Moreover, OPERANDO promotes proportionality by introducing the concept of the privacy guarantee, where if a request is made against the data of a service user, the requestor must provide a guarantee of how this data will be used. This can be checked by regulators and the service user would have access to this guarantee, to understand how their data is being used. This guarantee prompts the requestor to only ask for the data required, and to detail the reasons for this. The user is also able to set their privacy policy from a dashboard (by answering simple questions) which gives pre-defined responses to most requests made against their data.

In the Food Coach use case, the principle of proportionality will be promoted ensuring that personal data are used to the extent necessary for the intended purpose of dietary advice for optimal health. OPERANDO will provide access to the minimum amount of data that is sufficient for a personalised food and nutritional plan reducing the possibility of mission creep beyond what is needed to communicate healthy behaviours and nutritional needs.

With regard to the B2C use cases of social networks, OPERANDO will provide appropriate tools to support the monitoring of data usage and will inform users of any changes which may affect them. This way, they can reconsider their privacy settings. As planned in the OPERANDO Grant Agreement, for the sensitive and exceptional case of criminal investigations, OPERANDO platform will provide mechanisms that enable PSPs to avoid full data disclosure to law enforcement agencies optionally transforming particularly sensitive information such as biometric data to protect consumers.

3 Legal data protection principles

Privacy and data protection law is made up of broadly recognised legal principles. This section analyses the legal requirements for the OPERANDO market segments. Since the legal requirements are too generic to give guidance for engineering, the ethical values outlined in the previous section help specify privacy law and develop technical requirements.

3.1 Lawfulness

The principle of lawfulness covers several aspects of legal requirements which in addition to consent, require PSPs to distinguish several degrees of health, security and other objectives [8] [12] [13] [14] [16] [17] [20].

They should distinguish the various degrees of health and security protection. From other threats to the health of patients and security of victims, they have to distinguish threats to a user's life. This is necessary to enforce the balance between the ethical values of health care/public security and privacy/data protection. In addition, they have to distinguish threats that will realise immediately (where time does not allow checking lawfulness in advance), from other threats. The knowledge about the medical/security history and health/security-related behaviour and interactions can either rest on facts or mere assumptions which the service provider has to distinguish before they can get more data about users. In internal and external data sources, the service has to distinguish according to the degrees of reliability of those sources. Using personal data for the threat prediction should only be allowed if PSPs establish a high reliability of data originating in external sources. The PSPs have to distinguish between the data subjects to avoid third parties of being involved in notifications to caregivers in the patient's social environment and social care/security personnel in the victim's social environment. Since independent auditors need to verify whether OSPs meet the legal requirements the PSP should assist health and security OSPs and in giving the auditor the information he or she needs to check the lawfulness of the data processing.

Accordingly, these criteria apply to social network services and their business freedom. For example, from a risk of reduced advertisement revenues of such a service provider, the PSPs has to distinguish the loss of any revenues which would in effect prohibit the operation of social network services as such. In addition, they have to distinguish data processing that is needed for the technical provision of the service requested by the user from the processing for legitimate business interests. Besides, they should distinguish communication that is set by users to be publically available to an infinite number of recipients from more intimate communications. Moreover, they should distinguish cookies that are more persistent from very volatile ones; cookies from major ad network providers with a high number of publishing OSPs from niche ad networks with a lower number of/smaller OSPs as recipients of personalised advertisement [25].

For the OPERANDO use cases, we developed first examples of technical proposals for users to set their privacy policies indicating the impact of allowing or denying data access. In the Hestia use case, social care emergencies are treated in a special way. For example, on referral of domestic violence victims to receive support services, the "information sharing without consent form" (to which those victims consent) defines the categories of data and data subjects, statutory justifications for data processing, criteria for the proportionality test and consultation of colleagues, authorities and data subjects. This allows their information to be shared in a situation of emergency to stated organisations (e.g., police) to protect their physical security in contrast to other social care cases where the full process concerning privacy and data protection has to be carried out in advance. Similarly, OPERANDO will ask users to set their privacy policies, to determine access to their data, with clear indications of the impact of allowing/denying access to data. In addition, we will implement a method that ensures that access to data and services in emergency situations is granted in a lawful way. In the DRS use case, OPERANDO will implement an option to allow the emergency services access to the locations of vulnerable individuals in the event of a disaster by setting their

preference questions through their privacy policy. Rapid access to this information would enable more efficient management of an emergency situation.

Social networks will be forced to design their services and business to stay economically sustainable and protect user rights and user control at the same time. They will be forced to give users the choice of complete privacy, exchange of privacy for benefit, or some customised setting in the middle – and make money only on the users who consent to some relaxation of their privacy in exchange for free use of the service or other benefits. OPERANDO will facilitate enabling such customised settings.

3.2 Profiling prohibition

According to the principle of profiling prohibition, OSPs, PSPs and 3rd parties such as ad network providers must not deploy algorithmic decision-making without sufficient human verification if it entails significant disadvantages for users. It covers several aspects of legal requirements [8] [12] [26]. In particular, the PSP should enable OSPs and 3rd parties to correct inaccuracy factors of data about user behaviour and interactions. Moreover, users have a right to know the logic behind such profiling so that the PSP should help OSPs describe that logic. PSPs should enable auditors which have to verify that OSPs meet the legal requirements, to look for potential adverse effects of automatic decision-making for users in real-life operation. Moreover, automatic decisions with significant implications for users need to be double-checked manually by OSP personnel in advance, so that PSPs should offer tools assisting in this task and improving the OSP personnel's ability to verify automatic decisions.

For the OPERANDO use cases, we developed first examples of technical proposals to aid more effective decision-making by drawing professionals' attention to relevant information. In the Food Coach use case, dietary advice will be automatically provided by the Food Coach engine based on a person's profile. With this profiling, the users have a right to know the logic behind automatic decisions that are based on adopted nutritional guidelines and physician analysis for prescribing a personalised diet. Moreover, there will be an interface with third parties interested in publicising their healthy food products. OPERANDO will offer information about the logic for both categories of profiling.

WP3 will consider the special situation of social networks and other B2C market segments where the main income is generated from automatic profiling. In return for giving up a certain degree of achievement of this data protection principle within the legal limits, OPERANDO will compensate it with a higher level of protection of other ethical and legal requirements such as consent and data subject rights (see sections 2.3 and 3.6) by giving consumers the choice concerning the level of privacy that they prefer. WP3 will need to investigate how OPERANDO could promote the prohibition of OSPs of automatic profiling while pursuing marketing purposes. The OPERANDO platform will provide several mechanisms to minimise the possibility of profiling from PSPs, providing only specific personal information and controlling the information provided to the PSPs.

All in all, OPERANDO will provide tools to ensure that any aggregated or summary information about service users has been checked by human agents before use in any automated service or process; and that they are available to service users as part of their personal data.

3.3 Data availability

The principle of data availability covers several aspects of legal requirements [8] [12]. A lack of personal data has to be avoided in order to ensure that OSPs can achieve their legitimate purposes of health, security or business freedoms. PSPs should make available the data to several OSPs and OSP departments with equivalent tasks. Although data availability is a legal data protection principle, it also serves the technical requirement of a high system performance. Moreover, it supports OSPs in collecting data related to the user's environment from all available sources as well as "soft" data which are not necessary in a strict health, security or other business sense. Moreover, users should

not be forced to cooperate with the OSP in order for it to collect data. The service should collect data without influencing the behaviour or interactions of users. Concerning data loss, the PSP should protect the data, communication channels and user interfaces.

Similarly to the ethical requirements mentioned in the previous section, data availability comes into conflict with the other principles. This means that its limitation will have to be specified using its interaction with the other legal principles such as anonymity, as well as the ethical requirements mentioned above.

OPERANDO will help OSPs ensure that data are available at the right time and is shared with the right organisations. In the Barnsley Borough Council use case, concerning vulnerable adults, availability of data at the right time is crucial. For example, if a vulnerable adult were to visit an Accident and Emergency (A&E) department, the A&E professional has no access to their social care and support information, so even though an individual might be monitored 24/7 and provided care, they could be admitted to hospital unnecessarily (and increasing cost unnecessarily) due to lack of information available to the health professional. OPERANDO is key for sharing this information effectively, as data available about a service user needs to be stored securely in order for many organisations to access it, without risking the privacy of the users' data due to security breaches. This is particularly necessary as in the UK, legal obligations require the health sector, e.g., to set up an information sharing scheme and to restrict but not block access to citizens' medical data (e.g., by their GP) if a citizens opts out of the scheme. OPERANDO will ensure data availability as required by the scheme, while reducing the impact of this opt-out and non-blocking approach on citizens. We will offer options for access restriction on sharing the medical information.

In contrast to B2C use cases, certain cases of health and social care will require citizens to be registered in an OPERANDO-enabled system, for example, when visiting an A&E or a GP practice. In those cases, citizen data needs to be available medical and social care professionals so that the users' set of preferences will be opted in by default, as far as required by legal provisions, enabling citizens to monitor data use in their dashboard and use it to opt out or restrict access.

All in all, WP3 will assess the principle of data availability and specify it using the ethical requirements such as proportionality and prevention of mission creep as well as the other legal data protection principles such as purpose limitation.

3.4 Purpose limitation

The principle of purpose limitation covers several aspects of legal requirements [8] [12] [13] [14] [16] [18] [19] [20]. It requires PSPs to transform the collected user data so that nobody can link them with external databases or with the location where the service collects them. Moreover, the principle of purpose limitation requires the PSP to transform personal data so to rule out the possibility to extract excessive sensitive data (related to health, ethnic origin, sexual orientation, crimes, etc.) about the user from the data (see e.g., Article 8 of the EU Data Protection Directive [27]). Serving a specific purpose, the collected data should only be available to the OSP and category of personnel in charge. Others, such as the OSP's cloud operators, should not be able to use the data for secondary purposes, e.g., to concentrate all behaviour and interactions of users in a single place. PSPs should apply specific technologies and data formats in order to achieve such purpose limitation. In addition to enabling OSPs to separate user data from earlier data collections, PSPs should separate sensing devices, databases, data analytics systems and management systems from systems that can be accessed by other employees or organisations. Besides, they should label user data with the intended purpose.

For the B2C use cases, the purpose limitation principle prohibits social networks as publishers of advertisement and ad network providers, in particular, those that are part of a group of companies, to use personal data for advertisement that is not published on the social network whose services the consumer uses [24].

For the OPERANDO use cases, we developed first examples of technical proposals to prevent OSPs from linking data to external databases and to deploy techniques that stop re-identification. In the Food Coach use case, the health, behaviour and preferences data will be collected used and/or disclosed only to the extent necessary to accomplish a specified purpose. The information engine will safeguard identifiability and only link information from the clinical database. The user data will not be linked to external databases. Techniques will be deployed to stop re-identification and will not link data with outside sources.

In the ASL Bergamo and Ospedale Gaslini use cases, OPERANDO will ensure that the data will be stored in a way that blocks direct linking with other databases that are not protected by OPERANDO, not even within the same organization. In addition, organisational measures will strengthen purpose limitation. The data will be managed by the same department that will use it for the medical activities. For example, in the gambling addiction service run by the ASL Bergamo, the data will not be managed by the external department for information and communication technology, but will be controlled directly by specialized personnel of the same unit.

All in all, the OPERANDO platform will provide a Personal Data Repository (PDR) that along with the Gatekeeper allows controlled release of personal data to OSPs. Multiple Gatekeeper and PDR nodes can be implemented in order to strategically distribute personal data locations. These PDR nodes can be also located at the premises of corporations or public administration agencies supervised by an external or internal PA.

3.5 Data security

Independently from the engineering requirements of IT security, the legal data protection principle of data security requires OSPs, PSPs and 3rd parties to take various measures [12] [8] [13] [14] [16] [20]. Although the technical and the legal aspects overlap (authentication, access control, cryptography, platform security, secure communications, Public Key Infrastructure, security management, etc.), the legal principle focuses on the citizens' interests of the fundamental rights to privacy and data protection. The PSP's design decisions on the basis of The PSP's engineering requirements can lead to other design choices than those based on legal considerations, for example, if they come into conflict with business secrets.

The legal principle of data security requires controllers and processors to limit the data access to types and extent of access on a need-to-know basis. Accordingly, the system has to tailor access rights to the task of the individual workplace of personnel and auditors. It must limit user interfaces so that only the right personnel can obtain knowledge of user behaviour, interactions and automatic decisions. The system should facilitate supervision of data transfer, especially, to countries outside the EU. The system should make unauthorised data access more difficult, by splitting up databases among OSPs, PSPs and 3rd parties. It should employ state-of-the-art encryption for storage and in transit as well as a secure data format.

OPERANDO will provide tools in support of access control, encryption and auditability. In the Hestia use case, professionals will access data on a need-to-know basis. Limiting access to data is especially important in the example of a domestic violence victim, where their medical and location data are sensitive data. It is crucial that only social care and health professionals who need to know this information have access to the service users' data. For OPERANDO to be a trusted platform, the users' data will be stored securely and only accessed in the ways which they have consented to, set in their UPP.

In the Food Coach use case, a set of administrative, physical and technical actions will be taken to protect the confidentiality, availability and integrity of personal data with a view to the ethical aspects. The use of information technology mechanisms such as firewalls, encryption, passwords, and security compliance as well as the restriction of access to raw data that could directly identify an individual will be implemented. Concerning data transfer, the Food Coach system will provide a geo-

tagging scheme to prevent moving data across national borders from violating the law. Furthermore, the ASL Bergamo and Ospedale Gaslini use cases will maintain the high level of security already guaranteed for all the other online services run by the two administrations with the help of PDI.

All in all, data security will be supported by the PSP-controlled user data vault for G2C and (to a less enforceable extent) for B2C use cases. With respect to user access, it is envisioned that the OPERANDO platform provides security aware mechanisms and tools through Task T6.3 Security aware mechanisms and tools. This task will design and develop server-side solutions for (1) user authentication which ensures access only by legitimate system users and for the protection of end-users identity, and (2) user authorisation which enables access control to PA tools and services. Personal data delivery to the OSP will be (optionally) performed by the PA. The PA will release the data to the OSP based on the UPP and with strict judicious safeguards. This will allow revocation of access rights for specific users and OSPs.

Moreover, concerning the splitting of databases, WP3 will investigate which data should be processed in the cloud and which data should merely reside in the local systems of the OSP/PSP. We will assess how that can be decided and which module / component is in charge of that.

3.6 Data subject rights & user control

The principle of data subject rights covers several aspects of legal requirements [8] [12] [14] [17] [20] [21] that also aim to enhance user control. Concerning transparency, OSPs have be able to tell users who possesses whose data when and why. This can be enforced by engaging a trusted third party from which OSPs have to request data. Moreover, OSPs should inform users about the existence of rights, for which PSPs can be helpful. At all stages of data processing, they have to access logging has to include the following information for the respective stages of data processing (collection, transformation, transfer, etc.): employees, identity of controller/processor, their access/user rights, date/time of process, and (electronic) consents of users and their content. Concerning data breaches, they have to log the category of data subjects and data categories; to count the number of data subjects and number of datasets; and record the remedial actions taken, to be able to notify relevant authorities, staff and users.

Concerning participation of data subjects, PSPs should support OSPs to ensure that users can access their data; ask OSPs to assess data correction or deletion; configure the services using of data; and access the content of their consents and withdraw them for the future. In addition, the PSPs should assist OSPs in setting up and running a complaint handling system. PSPs should offer OSPs watermarks or similar technologies as well as sophisticated logging to help OSPs detect unlawful disclosure of user data and fulfil their data breach notification duties.

As mentioned, the legal data protection principles come into conflict. In particular, the logging duties both for transparency and participation reasons will be balanced with the other principles such as purpose limitation, data security and anonymity that aim to avoid the collection of additional personal data.

One of the OPERANDO project's main objective is to support user control over their data. OPERANDO will provide tools to support the control and management of data along with audit and reporting capabilities for data subjects and system administrators. The users of OPERANDO will be able to view the data held about them on their dashboard, and update them as necessary. The dashboard will allow the user to keep these administration functions in one place. With this collection of their data, there is also information about who has accessed their data and when, provided by the OSPs. This dashboard is therefore very important to reassuring users about the processing of their data. Furthermore, we will investigate the possibility to extend the currently planned OPERANDO architecture to include a module in charge of management where the data is located.

For example, users of the Food Coach platform will have opportunities to review who has accessed their individually identifiable health and preferences information. The user will be able to understand what individually identifiable health and preferences information exists about them, how the data is collected, used, and disclosed and whether and how they can exercise choice over such collections, uses, and disclosures to their doctor, personal trainer, and caregiver. In addition, it will provide mechanisms to allow the deletion of data upon a user's request. In the ASL Bergamo and Ospedale Gaslini use cases, transparency will be assured by PDI's "Lamiacittà Software" that guarantees logging and supports data subjects in exercising their rights.

3.7 Anonymity

The legal principle of anonymity covers several aspects of legal requirements [8] [13] [14]. The PSP should generalise datasets of users so that nobody can single out a person from larger groups of users. As planned in the OPERANDO Grant Agreement, this section particularly explores the requirement that users should be given the opportunity to consult their online data without having to reveal to OSPs, PSPs or 3rd parties that they are the same users of previous online consultations. In addition, the PSP should split them up so that an OSP and a PSP or a 3rd party can only jointly identify a person, by using sophisticated data transformation algorithms. The rationale behind this separation is to ensure that any such cooperation will not occur and thus compromise the anonymity of the individual involved. PSPs should protect data against de-anonymisation, for example, by using cryptographic measures that are effective for a sufficiently long time period (e.g., 10 years). In order to anonymise data, PSPs should collect additional context information and multiple degrees of generalisation or other representations of the same datasets. The PSP should avoid data storage and transfer by using index data where possible and reduce data categories needed for applications.

PSPs should add policies for user data to keep the retention periods as short as possible. Some data are only needed for intermediary technical reasons, the PSP should delete these by-catch data immediately. Moreover, log data should be minimised. Properties of the service that can be configured by OSPs should be set privacy-friendly by default.

As mentioned, the legal data protection principle of anonymity (e.g., short data retention period) will be balanced with the other principles such as logging requirements of the principle of data subject rights. Another example is the principle of lawfulness. The conflict will be resolved, e.g., by enabling OSPs to make the anonymity of users conditional upon the extent to which the application in question promotes the health of users, their security or legitimate business interests.

For the OPERANDO use cases, we will develop first proposals of innovative anonymisation techniques for OPERANDO components such as data analytics throughout the lifetime of the project to promote trust of users in PSPs.

In the Hestia use case, this could apply during brokerage (see D2.2 [2] for this process) when local authorities may provide a selection of service providers with anonymous data about a service user in order to ascertain estimated costs for the services they could provide to the citizen in their situation. This data provided would only include a minimum of information about the service user in order to detail services offered and a cost.

Anonymity will be handled in the B2C use cases of social networks, by generating substitute identities and preventing 3rd party use tracking.

All in all, OPERANDO will fully anonymise data, and provide protections that guarantees the data anonymity by limiting the processing of data. User requirements will be constructed in a way to protect individual and group anonymity taking on full consideration of reports that are generated by the system. All data will be anonymised and obfuscated such as to make it useless outside the information engine. In particular, the following tasks of the OPERANDO will tackle the challenge of meeting the legal principle of anonymity:

- T4.3: Innovations in privacy aware data publication & mining (ITI, PRS, STL);
- T6.1: Cloud-based Privacy Authority platform architecture (TCN, AVO, PRS, STL);
- T6.2: Privacy enhanced mechanisms and tools (ITI, OCC, AVO, RMS, TCN, PRS).

3.8 Responsibility

The principle of responsibility covers several aspects of legal requirements [8] [10] [12] [14] [17] [20]. PSPs should enforce that OSPs can only jointly exercise system administration and use with a PSP or another trusted third party ("system protection"). This way by default nobody can re-configure an online service to identify users without authorisation, e.g., by changing the algorithms for the innovative anonymisation techniques. The system should also detect irregular allocation of user rights, disabling of encryption or logging, and other irregular administrative activities. A management or automatic process to check software updates should be introduced. In the cloud environment, PSPs must ensure that access to data is limited to the OSP in charge of the particular online service. In the B2C use cases of social networks, the principle of responsibility requires PSPs to separate the roles of ad network providers and publishers [24].

In addition, PSPs should assist them to reveal their identity as a data controller concerning data transfers. Concerning 3rd parties, OSPs need to communicate their identity, e.g., to ad network providers so that they can inform users in addition to their own identity, about the source of data collection where users can verify the existence of their consent.

Moreover, PSPs should support the right to be forgotten and ensure that if data are corrected or deleted, this is also effective in the cloud environment, on devices of personnel and at third parties as recipients. In order to prevent unlawful disclosure, PSPs should choose, where possible, a service architecture based on index data instead of access to full data. Besides, they should carry out decentralised analytics and decision making. To ensure compliance with all of these requirements, PSPs should assist OSPs in setting up a privacy management system.

OPERANDO will provide tools in support of service providers' compliance with the requirements of responsibility. In the Hestia use case, the log of data use by local authorities and service providers (kept by PSPs) will aid auditors to follow the trail of data usage to determine whether the data was used responsibly by these OSPs. The service user will also be able to see a simple access log in their dashboard, so that they are able to understand who has viewed and used their data and the purpose.

In the Food Coach use case, responsibility will be promoted by the OPERANDO platform for the proper allocation of user rights, encryption, and software updates involving policies and procedures that include providing controls and limitations for the end-user, doctor, personal trainer, and caregiver. The ASL Bergamo and Ospedale Gaslini use cases will promote responsibility by means of PDI's legally compliant quality procedure. For example, in the Ospedale Gaslini use case, only the two supervisors together (one for the PSP and one for the OSP) can have the permissions and powers to totally reconfigure the system. Otherwise, they only have the power to manage their own part.

Concerning the upcoming "right to be forgotten" obligation, we will investigate the possibility of extending the currently planned architecture to include effective data tracking in the cloud environment. Such an audit trail would reveal where the data may have been copied, so that all such copies could be removed if needed. In the B2C use cases of social networks, for example, this mechanism would enable users to set the date by which their data will be erased.

3.9 Accountability

The principle of accountability covers several aspects of legal requirements which require OSPs to introduce mechanisms for verification of compliance with the law [9]. These mechanisms should reveal hardware, software, development tools and service configuration as far as they are ethically or legally relevant, e.g., concerning automatic decision-making. PSPs' public website and other product

material serve to inform related documentation. For cooperation with auditors and data protection authorities, PSPs should facilitate reviews, audits and inspections sufficiently independent from the OSP in question.

Moreover, the principle of accountability requires OSPs, PSPs and 3rd parties to ensure that the service remains adjustable to recommendations from in-house data protection officers and data protection authorities. PSPs should guide OSPs in carrying out privacy impact assessments which are the basis of possible adjustments required by data protection authorities. This guidance will also help OSPs oblige their employees to respect data secrecy and provide in-house training.

OPERANDO will provide tools in support of service providers' compliance with the accountability requirements. If there is a change in the law, it is costly to change systems and processes to keep up to date. However, using a PSP and OPERANDO-enabled systems will help them to stay up to date with the latest legislation and change their staff's practices accordingly. For example, in the Food Coach use case, we will perform a privacy impact assessment following the guidelines that apply to the demographic, clinical, behaviour and preferences data.

All in all, we will investigate the possibility of extending the currently planned architecture to include audits and trailing or the allocation of accountability aspects in the module "OSP enforcement".

4 Conclusion

Future work of OPERANDO will focus on providing a more complete set of examples of technical proposals for G2C and B2C use cases aiming to fulfil the EU societal responsibility of Privacy by Design. Moreover, we will monitor the EU legislative developments and take opportunities with regard to upcoming legal obligations concerning Privacy by Design [31] to create a credible privacy service platform.

Moreover, OPERANDO will study informal standards created by the ARTICLE 29 Working Party on Data Protection that are mentioned throughout this document. We will use the legally justified design decisions in OPERANDO to actively contribute to technical standardisation, for example, on occasion of the European Commission standardisation request M/530 on Privacy by Design for the security industry [4] to strategically prepare the marketing of OPERANDO as a viable business model.

5 References

1. OPERANDO D2.1 Consumer Use Cases Document, AVO Report Public 31/07/2015.
2. OPERANDO D2.2 OSP Use Cases Document, AVO Report Public 31/07/2015.
3. European Commission, Decision C(2014)4995 "Horizon 2020 Work Programme 2014-2015, 14. Secure Societies - Protecting freedom and security of Europe and its citizens", Brussels 22/07/2014.
4. Commission Implementing Decision C(2015) 102 final, Standardisation Request M/530, retrievable at http://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=548
5. Charter of Fundamental Rights of the European Union, European Union Official Journal C 364, 18/12/2000 p. 1, retrievable at http://www.europarl.europa.eu/charter/pdf/text_en.pdf
6. ARTICLE 29 Data Protection Working Party and Working Party on Police and Justice, "The Future of Privacy - Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data (WP 168)," Brussels 2009.
7. M. Pocs, "Will the European Commission be able to standardise legal technology design without a legal method?," Computer Law & Security Review 28 (2012) pp. 641-650.
8. ARTICLE 29 Working Party on Data Protection (WP29), "Working Document on the processing of personal data relating to health in electronic health records (EHR) (WP 131)," Brussels 2007.
9. WP29, "Opinion 3/2010 on the principle of accountability (WP 173)," Brussels 2010.
10. WP29, "Opinion 1/2010 on the concepts of 'controller' and 'processor' (WP 169)," Brussels 2010.
11. WP29, "Opinion 15/2011 on consent (WP 187)," Brussels 2011.
12. WP29, "Working Document 01/2012 on epSOS (WP 189)," Brussels 2012.
13. WP29, "Opinion 05/2014 on Anonymisation Techniques onto the web (WP 216)," Brussels 2014.
14. WP29, "Opinion 02/2013 on apps on smart devices (WP 202)," Brussels 2013.
15. WP29, "Opinion 2/2009 on the protection of children's personal data," Brussels 2009.
16. WP29, "Opinion 02/2012 on facial recognition in online and mobile services (WP 192)," Brussels 2012.
17. WP29, "Opinion 13/2011 on Geolocation services on smart mobile devices (WP 185)," Brussels 2011.
18. WP29, "Opinion 03/2013 on purpose limitation (WP 203)," Brussels 2013.
19. WP29, "Opinion 1/2007 on the Green Paper on Detection Technologies in the Work of Law Enforcement, Customs and other Security Authorities (WP 129)," Brussels 2007.
20. WP29, "Opinion 5/2009 on online social networking (WP 163)," Brussels 2009.
21. WP29, "Working Document on E-Government (WP 77)," Brussels 2003.
22. WP29, "Opinion 15/2011 on the definition of consent (WP 187)," Brussels 2011.
23. WP29, "Working Document 02/2013 providing guidance on obtaining consent for cookies (WP208)", Brussels 2013.
24. WP29, "Opinion 2/2010 on online behavioural advertising", Brussels 2010.
25. WP29, "Opinion 4/2012 on cookie consent exemptions (WP194)", Brussels 2012.

26. WP29, “Advice paper on essential elements of a definition and a provision on profiling within the EU General Data Protection Regulation”, Brussels 2013.
27. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, European Union Official Journal L 281, 23/11/1995 p. 31.
28. Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, European Union Official Journal L 337, 18/12/2009 p. 11.
29. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), European Union Official Journal L 201, 31/07/2002 p. 37.
30. Telemediengesetz (TMG) as amended on 17/7/2015, Bundesgesetzblatt (BGBl.) 2015 I 1324, retrievable at http://www.gesetze-im-internet.de/tmg/
31. European Commission Proposal of a Data Protection Regulation COM(2012) 11 final, retrievable at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf