<table>
<thead>
<tr>
<th><strong>Project Number:</strong></th>
<th>GA 727301</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Project Title:</strong></td>
<td>SHIELD</td>
</tr>
<tr>
<td><strong>Title of Deliverable:</strong></td>
<td>Report on legal requirements</td>
</tr>
<tr>
<td><strong>Due Date of Delivery to the EC:</strong></td>
<td>30/06/2017</td>
</tr>
<tr>
<td><strong>Workpackage responsible for the Deliverable:</strong></td>
<td>WP3</td>
</tr>
<tr>
<td><strong>Editor(s):</strong></td>
<td>Matthias Pocs</td>
</tr>
<tr>
<td><strong>Contributor(s):</strong></td>
<td>Brian Pickering</td>
</tr>
<tr>
<td><strong>Reviewer(s):</strong></td>
<td>Derick James</td>
</tr>
<tr>
<td><strong>Approved by:</strong></td>
<td>Xabier Larrucea</td>
</tr>
<tr>
<td><strong>Recommended/mandatory readers:</strong></td>
<td>All WP’s</td>
</tr>
</tbody>
</table>

**Abstract:**

This deliverable reports on the analysis of legal requirements and design proposals for SHiELD.

**Keyword List:**

GDPR, data protection by design, health information, pseudonymisation, epSOS, privacy, security, law

**Disclaimer**

This document reflects only the author’s views and neither Agency nor the Commission are responsible for any use that may be made of the information contained therein.
## Document Description

### Document Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Modifications Introduced</th>
<th>Modified by</th>
</tr>
</thead>
<tbody>
<tr>
<td>v0.1</td>
<td>05/06/2017</td>
<td>First draft version</td>
<td>Matthias Pocs</td>
</tr>
<tr>
<td>v0.2</td>
<td>06/06/2017</td>
<td>Consolidated after working session</td>
<td>All partners</td>
</tr>
<tr>
<td>v0.3</td>
<td>23/06/2017</td>
<td>Contributed to main sections</td>
<td>Brian Pickering</td>
</tr>
<tr>
<td>v0.4</td>
<td>24/06/2017</td>
<td>Consolidated partner contributions, added introduction and conclusion</td>
<td>Matthias Pocs</td>
</tr>
<tr>
<td>v0.5</td>
<td>28/06/2017</td>
<td>Changed after quality review</td>
<td>Derick James</td>
</tr>
<tr>
<td>v1.0</td>
<td>28/06/2017</td>
<td>Optimised, submitted to EC</td>
<td>Xabier Larrucea</td>
</tr>
</tbody>
</table>
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terms and abbreviations</td>
<td>6</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>8</td>
</tr>
<tr>
<td>1 Introduction and methodology</td>
<td>9</td>
</tr>
<tr>
<td>2 General legal requirements</td>
<td>10</td>
</tr>
<tr>
<td>2.1 Lawfulness</td>
<td>10</td>
</tr>
<tr>
<td>2.1.1 Law or consent</td>
<td>10</td>
</tr>
<tr>
<td>2.1.2 Vital interests</td>
<td>11</td>
</tr>
<tr>
<td>2.2 Data accuracy and profiling prohibition</td>
<td>11</td>
</tr>
<tr>
<td>2.2.1 Accuracy</td>
<td>11</td>
</tr>
<tr>
<td>2.2.2 Profiling</td>
<td>12</td>
</tr>
<tr>
<td>2.3 Data availability</td>
<td>12</td>
</tr>
<tr>
<td>2.4 Purpose limitation and sensitive data</td>
<td>12</td>
</tr>
<tr>
<td>2.4.1 Purpose limitation</td>
<td>12</td>
</tr>
<tr>
<td>2.4.2 Sensitive data</td>
<td>13</td>
</tr>
<tr>
<td>2.5 Data security (in the sense of data-protection law)</td>
<td>13</td>
</tr>
<tr>
<td>2.6 Data subject rights, portability, right to be forgotten</td>
<td>15</td>
</tr>
<tr>
<td>2.6.1 Transparency (in the sense of data-protection law)</td>
<td>15</td>
</tr>
<tr>
<td>2.6.2 Participation</td>
<td>16</td>
</tr>
<tr>
<td>2.7 Data minimisation</td>
<td>16</td>
</tr>
<tr>
<td>2.7.1 Amount of data</td>
<td>16</td>
</tr>
<tr>
<td>2.7.2 Retention period and anonymised data</td>
<td>17</td>
</tr>
<tr>
<td>2.7.3 Pseudonymisation</td>
<td>18</td>
</tr>
<tr>
<td>2.8 Responsibility</td>
<td>19</td>
</tr>
<tr>
<td>3 Design and management requirements</td>
<td>20</td>
</tr>
<tr>
<td>3.9 Risk-based approach</td>
<td>20</td>
</tr>
<tr>
<td>3.9.1 Technical and economic aspects</td>
<td>20</td>
</tr>
<tr>
<td>3.9.2 Processing scope and purposes</td>
<td>20</td>
</tr>
<tr>
<td>3.9.3 Rights and freedoms of natural persons</td>
<td>21</td>
</tr>
<tr>
<td>3.10 Data protection by design</td>
<td>21</td>
</tr>
<tr>
<td>3.10.1 Measures at design time</td>
<td>21</td>
</tr>
<tr>
<td>3.10.2 Pseudonymisation for data minimisation</td>
<td>21</td>
</tr>
<tr>
<td>3.10.3 Other elements in support of ‘data protection by design’</td>
<td>21</td>
</tr>
<tr>
<td>3.10.4 Updating of ‘data protection by design’</td>
<td>22</td>
</tr>
<tr>
<td>3.10.5 Effectiveness and integration of ‘data protection by design’</td>
<td>22</td>
</tr>
<tr>
<td>3.11 Accountability, data protection officer, impact assessment</td>
<td>22</td>
</tr>
<tr>
<td>3.11.1 Demonstration of legal compliance</td>
<td>22</td>
</tr>
</tbody>
</table>
3.11.2 Elements in support of accountability ................................................................. 23
3.11.3 Updating of accountability measures ................................................................. 23
3.12 Certification .................................................................................................................. 24

4 Fundamental-rights requirements .................................................................................. 25
4.13 Fair decision-making ................................................................................................. 25
4.14 Privacy and data protection ....................................................................................... 25
4.15 Autonomy and lawfulness .......................................................................................... 25
4.16 Non-discrimination .................................................................................................... 26
4.17 Human dignity ............................................................................................................ 26
4.18 Public health and access to health care ..................................................................... 26
4.18.1 Access to health care ............................................................................................. 26
4.18.2 Public health ........................................................................................................... 26
4.19 Proportionality and mission creep ............................................................................. 26
4.19.1 Proportionality ....................................................................................................... 27
4.19.2 Mission creep ......................................................................................................... 27

5 Conclusions ..................................................................................................................... 28

6 References ...................................................................................................................... 29
### Terms and abbreviations

<table>
<thead>
<tr>
<th>Personal data</th>
<th>Any information relating to an identified or identifiable natural person.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive data</td>
<td>Special category of personal data such as those concerning health, the processing of which is in principle prohibited. “Data concerning health” means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.</td>
</tr>
<tr>
<td>Anonymised data (subjects)</td>
<td>Data rendered anonymous so that the data subject is not or no longer identifiable. Data-protection law does not apply to anonymised data or its processing, including for statistical or research purposes. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.</td>
</tr>
<tr>
<td>Pseudonymisation</td>
<td>Processing of personal data so that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to a data subject. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. The application of pseudonymisation to personal data is an element of legal compliance but it is not intended to preclude any other measures of data protection.</td>
</tr>
<tr>
<td>Data subjects</td>
<td>An identified or identifiable natural person</td>
</tr>
<tr>
<td>Identifiability</td>
<td>Ability to identify a data subject, direct or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.</td>
</tr>
<tr>
<td>Processing</td>
<td>Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.</td>
</tr>
<tr>
<td>DPA</td>
<td>Data protection (supervisory) authority</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>EHR</td>
<td>Electronic health record</td>
</tr>
<tr>
<td>NCP</td>
<td>National contact point</td>
</tr>
<tr>
<td>eADC</td>
<td>epSOS Automatic Data Collector</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standardization for Organization</td>
</tr>
<tr>
<td>TS</td>
<td>Technical Specification (a type of standardisation deliverable)</td>
</tr>
<tr>
<td>CD</td>
<td>Committee Draft</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>CEN</td>
<td>European Committee for Standardization</td>
</tr>
<tr>
<td>TC</td>
<td>Technical Committee</td>
</tr>
<tr>
<td>BSI</td>
<td>British Standards Institution</td>
</tr>
<tr>
<td>PAS</td>
<td>Publicly Available Specification</td>
</tr>
<tr>
<td>WP29</td>
<td>ARTICLE 29 Working Party on data protection. The WP29 is the EU advisory body on data protection composed of the European DPAs (one per Member States of the European Union and the DPA of the European Union) created by Article 29 of Directive 95/46/EC. The WP29 will be renamed into European Data Protection Board based on Article 68 of the General Data Protection Regulation 2016/679/EU.</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>GP</td>
<td>General practitioner</td>
</tr>
</tbody>
</table>
Executive Summary

This deliverable reports on the analysis of legal requirements for SHiELD. It specifies the GDPR’s classic ‘data protection principles’ and innovative ‘data protection by design’ and accountability obligations. For the latter, WP3 suggests introducing a SHiELD scenario on “GDPR design and management requirements”.

In this document, WP3 proposes a pseudonymisation mechanism for privacy-by-design procedures, for discussion among SHiELD technical and trial partners.

This deliverable identifies the documents by the WP29, such as those on epSOS and EHR, as relevant guidance for SHiELD to consider.

It also includes the description of the ethical values enshrined in the European Charter of Fundamental Rights, which are elements of legal compliance and possible sources for proposals for technical and organisational measures.
1 Introduction and methodology

In the first task of WP3, legal requirements were analysed in collaboration between Stelar and IT Innovation. This work aims to prepare the more comprehensive procedural guidance which will be elaborated in SHIELD task T3.2.

In the following sections, the design considerations currently being reviewed by the technical work packages are summarised in connection with individual aspects of existing EU regulation.

The document is to be seen in the light of the concept of ‘data protection by design’. In contrast to guidance on data-protection agreements between healthcare organisations, this report primarily targets the relationship between healthcare providers and technology providers. This is because that relationship effectively concerns the design of the product or service (SHIELD task T3.1: “specify legally and ethically compatible design patterns”).

This deliverable is structured into sections on general legal requirements, design and management requirements and fundamental-rights requirements. In particular, the general legal requirement of data minimisation is complemented by WP3 pseudonymisation proposals. Each (sub-)section defining a legal requirement is subdivided into the requirement and the preliminary application to the case of SHiELD.

Concerning the methodology, this document takes into account SHiELD deliverable D2.1 on challenges for security in health data exchange. It focusses specifically on legal data-protection requirements as identified for epSOS and other EHR-based data exchange. It also mentions relevant OpenNCP and e-SENS specifications (D2.1 Table 3). Moreover, the editor of this deliverable requested feedback from all SHiELD partners in the working session of the Liverpool consortium meeting, on how expected results from SHiELD work packages and tasks could support the respective legal requirements.

The legal requirements are derived from the GDPR. Compared to its predecessor (the Data Protection Directive 95/46/EC) the GDPR has a new kind of impact on systems for health data exchange. It is a single piece of legislation directly effective in all Member States of the European Union and thereby unifying legal obligations that are currently defined at national level; applicable to any organisation in the world that purchases or uses applications, services, products processing data or based on data; which introduces dissuasive sanction and more efficient regulation (see SHiELD deliverable D7.1). This means that the general legal requirements (data protection principles) and the fundamental-rights requirements (ethical values) to which the general requirements refer, have a new quality of impact. Moreover, the GDPR introduces a new kind of design and management requirements of ‘data protection by design’, accountability, risk-based approach, certification, data protection impact assessment, etc.

Additional guidance on legal data-protection requirements by the WP29 is referenced where relevant (documents referred to with a “WP” identifier in this document, e.g. “WP189”, can be found at [1]). In some instances guidance from international and European health-informatics standards and industry are mentioned as well.

The scientific methodology follows from the multi-disciplinary bridging approach between legal research and the different disciplines of computer science, for legally compatible technology design in the field of data protection [2] [3]. Accordingly, the very high-level fundamental rights and data-protection principles, on the one hand, as well as very specific preliminary technological proposals, on the other, are approximated in an iterative process.
2 General legal requirements

The data-protection principles are defined as general legal requirements in this section.

2.1 Lawfulness

The legal basis for processing of personal data may be law, consent, vital interests and others (GDPR Articles 5(1)(a)(1), 6, 7, 8).

2.1.1 Law or consent

Data processing must be based on law or consent.

WP3 recommends SHIELD to consider the WP29 in their Opinions on epSOS and EHR (WP189, WP131). In the epSOS case it seems that processing will probably take place outside the specific purposes of medical treatment, which would otherwise qualify as a legal basis for the health-data exchange. Another possible legal basis - the public interest exemption - is also ruled out by the WP29 as a legal basis for the use of health data transferred from another health care provider within the EU.

Therefore the Working Party is of the opinion that the explicit consent and the vital interest of the data subject can serve as an appropriate legal basis for the processing of personal data in the framework of the epSOS project, in its current shape. As regards consent, the WP29 suggests a two-step explicit consent.

Firstly an explicit consent should be given to the participation of the data subject in the epSOS project or parts of it (for example in the form of modular access rights for health care providers, see below). This first consent in country A would allow the health care providers to prepare specific data with the intention to make them available in future to other health care providers in the framework of epSOS. The first consent would be required only once at the point where (actually before) the data subject’s data are prepared or made available to the system. Therefore it follows, that the first consent necessarily has to be given before the second consent. If there, following the first consent, are any major changes in the processing of data within epSOS, a new consent will be required.

In order to facilitate making the benefits of epSOS available to data subjects who need treatment in country B but have not previously given consent in country A, the epSOS project could investigate the possibility of allowing patients to give also their first consent for instance in a secure way over the Internet in country B.

The second consent shall be given explicitly for the processing of health data in the case of actual treatment in country B.

In addition to the WP29 guidance on epSOS and EHR, WP3 recommends SHIELD to consider details about the legal requirement in this subsection that can be found in WP29 Opinions on consent (WP187) and legitimate interests (WP217).

The technical specifications of OpenNCP components have direct relevance for the requirements covered in this subsection. For example, the epSOS Automatic Data Collector in the OpenNCP project [5] [6] is designed to flexibly extract any information that is contained in any epSOS transaction and its enclosed consumer documents. The eADC may only be used after the prior authorisation of the affected data protection assignees of the organisation that is operating the NCP. It may also be necessary to document a prior authorisation of the
affected data subject (patient) under certain circumstances or regulatory settings, depending on the specific configuration and extent of the actual data extraction and collection.

SHiELD: The sensitivity finder tool will be developed to analyse PDFs and tables, and tag and sort them into "identifiable", "quasi-identifiable" and other categories of data. Its output will be used at design time to prepare informed consent. Modular consent (and withdrawal of consent) is an element of data processing under consideration. It would also minimise the impact on validation in or beyond the project if consent is design in a modular way. However, the granularity of modular consent depends on the source technology (free-text PDFs versus structured patient summary).

2.1.2 Vital interests

Data processing may be based on ‘vital interests’ (i.e., data processing is essential for a data subject’s life or that of another natural person) if consent cannot be manifestly based on consent (or another legal basis such as ‘public interest’ in cases of disasters, epidemiology, etc.). No national deviation is permitted.

WP3 recommends SHiELD to consider the WP29 in their Opinions on epSOS and EHR (WP189, WP131). Processing of personal and sensitive data can be justified without second consent in country B if it is necessary to protect the vital interests of a data subject or of another person if in the emergency case the data subject is physically or legally incapable of giving his consent. The GDPR sets out that the processing of sensitive personal data can be justified if it is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent.

The processing must relate to essential individual interests of the data subject or of another person and it must in the medical context be necessary for a life-saving treatment in a situation where the data subject is not able to express his intentions (emergency case). Accordingly, this exception could be applied only to a small number of cases of treatment and only where the first consent of the two-steps-model has been given. It is of great importance that the scope of this exception should be narrowly defined as to when and how it can be applied. Also, technical measures should be employed in order to prevent misuse of the emergency case.

SHiELD: Additional safeguards may include notification of trusted third parties (such as a caregiver trusted by the data subject, the DPA) about the occurrence of the ‘break glass circumstance’. For example, there is currently an internal discussion about reporting to data subjects of attempts to access their data. On DPA notification, the legal requirement under the GDPR would suggest that only one DPA would be informed, namely the DPA of the member state where the service is hosted. However, SHiELD is also considering whether any such mechanism should be extended to include notification to the relevant DPA for the member state where the data subject resides.

2.2 Data accuracy and profiling prohibition

Personal data and related decisions must be accurate or verified.

2.2.1 Accuracy

Data must be accurate and regularly updated (GDPR Article 5(1)(d)).

SHiELD: There are tools for checking document quality (plausibility, e.g., for census data) and maturity level of data inputs to clinical systems. Document provenance should also be tracked.
For GPs, national systems may be more mature than those for hospitals. In the long run, there should be a data quality management team for a central repository.

2.2.2 Profiling

Automatic decisions must not be taken for granted without sufficient human verification (GDPR Article 22).

SHiELD: There is no such data analytics planned in SHiELD.

2.3 Data availability

The free movement of personal data in the European Union must not be restricted for reasons of data protection.

SHiELD: One of the main objectives of SHiELD is to support cross-jurisdiction data sharing where there is a clear need in connection with the vital interests of the data subject.

2.4 Purpose limitation and sensitive data

Personal data are subject by the purpose of processing and special categories of data are subject to further conditions and safeguards.

2.4.1 Purpose limitation

Data must be processed only for specified and non-incompatible purposes (GDPR Article 5(1)(b)).

WP3 recommends SHiELD to consider the WP29 in their Opinions on epSOS and EHR (WP189, WP131). In order to properly assess how this requirement should be put into place in practice it is necessary to clearly identify the legitimate purpose or purposes for which the epSOS-based system intends to process personal data. As stated earlier, purposes must be specific and explicit, that is, determined in a precise and well-defined manner, so generic approaches could not be sufficient. The “provision of care or treatment” and “the prescription and dispensation of medicines” are, of course, legitimate purposes, but the WP29 wonders whether they are sufficiently and precisely describing the aims and activities of epSOS. Moreover, any other envisaged purposes must be defined prior to any processing, in order to warrant that no more personal data than is necessary will be processed, and therefore to properly comply with the legal requirements.

Moreover, data must in practice only be processed for the legitimate purpose. Therefore, each query for personal data available through the epSOS system should be based on the existence of a real need to access specific data related to the care or treatment to be provided or the medicine to be prescribed or dispensed in a particular case.

In addition to the WP29 guidance on epSOS and EHR, WP3 recommends SHiELD to consider details about the legal requirement in this subsection that can be found in WP29 Opinion on purpose limitation (WP203).

The technical specifications of OpenNCP components have direct relevance for the requirements covered in this subsection. For example, the epSOS Automatic Data Collector in the OpenNCP project [5] [6] is designed to flexibly extract any information that is contained in any epSOS transaction and its enclosed consumer documents. The eADC may only be used for enabling the designated evaluation task force to fulfil its assigned task as agreed by the epSOS
decision bodies and in full compliance to the epSOS framework agreements and the individual regulatory setting at the point of operation.

Additional guidance to the WP29 Opinions and the OpenNCP specifications, is given by health-informatics standard ISO/TS 14265 ‘Classification of purposes for processing of personal health information’.

SHiELD: The purpose specification is done partly in use cases but not, e.g., for 3rd-party uses for the improvement of services (data-protection services, etc.). To implement purpose limitation support, design is based on policies and user rights definition.

2.4.2 Sensitive data

Conditions and safeguards for special categories of information must be observed or taken. The European Union and/or Member States may maintain or introduce further conditions for data processing (GDPR Articles 9(2), (4), 10).

WP3 recommends SHiELD to consider the WP29 in their Opinions on epSOS and EHR (WP189, WP131). Accordingly, all data contained in medical documentation, in electronic health records and in EHR systems are “sensitive personal data”. Therefore, they are not only subject to all the general rules on the protection of personal data, but also subject to the special data protection rules on the processing of sensitive information.

SHiELD: All exchanged data are considered to be sensitive (special category) personal data, including metadata such as the existence of records in certain categories of healthcare organisation.

2.5 Data security (in the sense of data-protection law)

Data must be processed with a level of security appropriate to the risks for the patients and other data subjects (GDPR Articles 5(1)(f), 32).

WP3 recommends SHiELD to consider the WP29 in their Opinions on epSOS and EHR (WP189, WP131). All staff implementing the project should be provided with clear-cut, written instructions on how to appropriately use the epSOS system in order to prevent security risks and breaches. Suitable arrangements should be made in using the Patient Summary and e-Prescription storage and archiving systems to protect the data against unauthorised access, theft and/or partial or total loss of storage media. User rights should be defined. For this, the WP29 refers to an example from a different sector: Commission Decision 2008/49/EC of 12 December 2007 concerning the implementation of the Internal Market Information System as regards the protection of personal data.

Concerning encryption, for data exchanges, secure communication protocols and end-to-end-encryption must be adopted based on encryption standards for securing electronic communications. This has to be done in order to prevent acquisition/disclosure of the information in the presence of any intermediaries not controlled by the patient or the authorised healthcare organisations. Endpoints of the encryption must be located within environments either controlled by the patient directly or by the professional healthcare organisations authorised by the patient for processing his/her medical data. Where communications of health data take place by way of applications that rely on publicly available networks (e.g. the Internet) for data exchanges, the system should envisage the use of reliable digital certificates for both the server systems delivering the service and the client devices accessing the data. An unbroken chain of digital evidence must be preserved to safeguard the integrity and authenticity of the health data in an end-to-end manner.
As regards authentication, special attention must be paid to adopting a reliable and effective electronic identification system that provides strong authentication. This applies equally to both participating staff members and patients. Additionally, procedures should be put in place to regularly verify the authentication credentials and the authorisation profiles allocated to the staff. The data controller should devise specific procedures to prevent online access and consultation by data subjects where there are possible data confidentiality threats – whether detected directly by the data controller or reported by the data subjects (e.g. in case of theft/loss of authentication credentials, unauthorised access to the system and other data breaches, etc.).

In terms of auditability, the system must be capable to correctly record and track in an auditable way the individual operations that make up the overall data processing. This applies, in particular, to data access requests and any handling of the data. The system should also include regular internal checks and controls on authenticity of authorisations. Accordingly, appropriate internal and external controls should be used in the way of audit log systems to verify database accesses, whilst there should be specific alerts where risky and/or non-standard behaviour is identified. To ensure that this all works the system should be audited on a regular basis.

With respect to back-ups, unauthorised data access and/or changes should be prevented when the back-up data are transferred and/or stored (e.g. by means of encryption). It should be ensured that all epSOS operators must be subject to professional secrecy or similar rules of practice - as is the case in respect of health care practitioners.

Specifically regarding the e-Prescription system, additional measures should be deployed in order to ensure that pharmaceutical operators can only access digital prescriptions for providing the medicines prescribed and they should prevent any kind of epSOS related prescription database from being set up at the pharmacy.

In emergency situations, if it proves necessary to access any information without the required authorisations, that and any subsequent access (including any data processing operations) should be logged and subject to audit; records should also be kept concerning the reasons for the particular data access.

The technical specifications of OpenNCP components have direct relevance for the requirements covered in this section. For example, the Evidence Emitter powered by e-SENS [7] enables NCPs to generate and emit electronic evidence used for non-repudiation purposes.

There are two examples given in [7]. First, in e-Prescription, the patient returns to the home country and claims reimbursement of 3 packages of the drug purchased abroad. The dispensation only shows that 1 package was dispensed. The organization of NCP A now needs to prove that erroneous information was received from NCP B and was not generated while processing the dispensation information. A similar case arises when the patient claims they only purchased 1 package out of 3, and there should be still some available amount on the prescription. The NCP A needs to show that the information received from NCP B was wrong.

Second, in Patient Summary, a drug is administered to the patient, and the patient suffers a severe allergic reaction. The allergy to the drug was mentioned on the patient summary, but the doctor claims that this information was not delivered and shown to them. Now NCP B wants to demonstrate that this information was indeed not received from Country A.

Another OpenNCP component with direct relevance for the requirements covered in this subsection is the epSOS Automatic Data Collector in the OpenNCP project [5] [6], which is...
designed to flexibly extract any information that is contained in any epSOS transaction and its enclosed consumer documents. The eADC result data sets and persistent data storage facilities within the relational database management system must be adequately protected from unauthorised access. The configuration and extraction rules must be adequately integrity protected.

Additional guidance to the WP29 Opinions and the OpenNCP specifications, is given by health-informatics standard ISO 27799 ‘Security management in health using ISO/IEC 27002’.

SHiELD: There will also be tools to identify potential and actual attacks. For example, in the “knowledge base”, availability such as protection against data loss and reliable and fast algorithms, will be considered (e.g., Denial of Service attacks on epSOS service by redundancy and caching). Other security measures under consideration are protection against data destruction, theft and manipulation. In addition, there is some discussion within the project relating specifically to the application and initialisation of risk models not least to provide access for technical components to the perceived risks which individual data subjects may have identified.

2.6 Data subject rights, portability, right to be forgotten

Transparency and participation elements constitute data subjects rights.

2.6.1 Transparency (in the sense of data-protection law)

Data must be processed in a transparent manner (“who processes what when”; GDPR Articles 5(1)(a)(2), 11(1), 12 to 14).

WP3 recommends SHiELD to consider the WP29 in their Opinions on epSOS and EHR (WP189, WP131). One of the preconditions for a valid consent is that the data subject has received information (from the controller or his representative) which satisfies the legal requirements.

The information should contain a comprehensive, clear and understandable description of the epSOS-based project, mentioning at least the categories of data that would be transferred by which health care providers to which other health care providers and other institutions. This includes the institutions involved in the further processing of the data in country B for other purposes than to provide and manage health care. Information must also be provided about the purpose of the transfer and how long the data would be stored. Finally it must be made clear that there is the option of withdrawing consent at any time. The data subject should also be informed about the right of access and rectification of data concerning him/her. This information would be included in the first consent following the two-step consent suggested by the WP29.

Moreover, the information given must at least contain the explanation which health care provider and other institution will process which categories of data and for which purpose. This would be included in the second consent following the two-step consent suggested by the WP29.

With regards to the exchange of data in emergency cases in the epSOS project, the data subject should be informed about it in the general information concerning the epSOS-based project (first consent). In this situation it is especially important that the patient is given access to information about the transmissions that have taken place.

SHiELD: This will be addressed by audit trails (logging) in the security-monitoring assurance-tool and the OpenNCP component that checks this in relation to NCP and data requestor.
2.6.2 Participation

Patients and other data subjects must be able to access (and receive/transmit as defined in the GDPR), correct and/or delete their data (even across controllers as defined in the GDPR). Member States may restrict data subject rights by enacting proportionate legislation (GDPR Articles 15 to 21, 23).

WP3 recommends SHiELD to consider the WP29 in their Opinions on epSOS and EHR (WP189, WP131). All data controllers who handle epSOS data, no matter on what level or in which role (e.g. as health care provider, dispenser of e-prescriptions, National Contact Point, and so forth) must give data subjects the right to access to and the right to the rectification, erasure and blocking of his or her own data, regardless of whether the data subject is a national or resident of another Member State and regardless of whether the relevant data derives from data controllers in other Member States. No data controller who processes data in the epSOS project can refuse access or the rectification, erasure and blocking solely on the ground that the data controller itself did not introduce the data to epSOS.

A data subject should be able to address questions about access and demands for rectification, erasure and blocking to any of the controllers as well as to any other body involved in the exchange of information within epSOS. A demand to access or for the rectification, erasure and blocking of data which is given to an epSOS partner who does not handle data about the data subject, should be forwarded to the data controller in charge within the epSOS system even if this relevant controller is established in another Member State.

For the epSOS project the WP29 recommended to investigate the possibility of granting the data subject direct (electronic) reading access to his/her own data. The epSOS project should investigate the possibility of giving to data subjects direct (electronic) reading access to their own data. The data protection right of access need not necessarily always mean direct access. Direct access might, however, contribute considerably to trust in the epSOS system. From a data protection point of view a precondition for granting direct access would be secure electronic identification and authentication in order to prevent access by unauthorised persons.

Another recommendation by the WP29 was for a common epSOS website to be constructed to inform on the specific rights of data subjects according to the different legislations of all the participating states. The information on the website should clearly specify the rights, conditions and practicalities according to the national legislation of each Member State.

SHiELD: Notifications will be handled in connection with the consent management (“I would like to be notified if data are shared”). OpenNCP does not allow correction or deletion, not even for healthcare professional (read only). In any case, measures will be taken to guarantee the rights of any trial participant to access and delete their data.

2.7 Data minimisation

Data minimisation refers to the amount of data, retention period and anonymised data as well as to pseudonymisation.

2.7.1 Amount of data

The amount of data (data categories) must be reduced as much as possible given the specified purposes (GDPR Article 5(1)(c)).
WP3 recommends SHiELD to consider the WP29 in their Opinions on epSOS and EHR (WP189, WP131). The processing of personal data must be strictly limited to the minimum which is necessary for the fulfilment of the epSOS purposes which must be specified, explicit and legitimate.

The patient should also have the possibility to give his/her consent only to the transfer and processing of certain categories of health data (modular access rights for health care providers in another country). Finally it must also be made clear that there is the option of withdrawing consent at any time. The data subject should also be informed about the right of access and rectification of data concerning him/her.

As it has been explained above the explicit consent of data subjects, or an action to protect their vital interest, could serve as an appropriate legal basis for the processing of health-related personal data in the framework of the epSOS project. However the processing of such data must be strictly limited to the minimum necessary to the fulfilment of the epSOS purposes. Only relevant information in relation to the epSOS purposes should be recorded into the Patient Summary and e-Prescription.

In addition to the WP29 guidance on epSOS and EHR, WP3 recommends SHiELD to consider details about the legal requirement in this subsection that can be found in WP29 Opinions on proportionality (WP211).

SHiELD: Identification of data categories will be done, e.g., by the data sensitivity tool, which will be enforced by policies and the consent management.

### 2.7.2 Retention period and anonymised data

Data must be deleted - or data subjects must be (effectively) anonymised - as soon as possible, given the specified and non-incompatible purposes (retention period; GDPR Article 5(1)(e)).

WP3 recommends SHiELD to consider the WP29 in their Opinions on epSOS and EHR (WP189, WP131). In order to safeguard that data are not kept longer than is necessary in the epSOS system, a maximum retention period should be decided as well as a common procedure as to what shall happen to the data at the end of the retention period.

Only those healthcare professionals and authorised personnel who are involved in the patient’s treatment may access medical records, and therefore the epSOS Patient Summary and e-Prescription information. From the wording of the documentation provided to the Working Party, there does not seem to be a requirement for the NCPs to store medical information for the fulfilment of the epSOS purposes, so the retention of such data by the NCPs should be avoided. However, in case personal data has to be stored, for example at the NCP, the epSOS project should decide on a maximum retention period and also on a common procedure as to what shall happen to the data at the end of the retention period.

In addition to the WP29 guidance on epSOS and EHR, WP3 recommends SHiELD to consider details about the legal requirement in this subsection that can be found in WP29 Opinions on anonymisation techniques (WP216), the concept of personal data (WP136), the ePrivacy legislation (WP247, WP240), device fingerprinting (WP224), the Internet of Things (WP223), trusted computing (WP86) and the Internet (WP16). For example, in WP247 the WP29 proposes technical solutions for deletion and anonymisation of MAC addresses for statistical counting (as hashing is not sufficient for anonymisation).

The technical specifications of OpenNCP components have direct relevance for the requirements covered in this subsection. For example, the epSOS Automatic Data Collector in...
the OpenNCP project [5] [6] is designed to flexibly extract any information that is contained in any epSOS transaction and its enclosed consumer documents. The eADC is potentially collecting and storing a redundant data set (copy of medical information) in relation to its individual configuration. Without manual intervention, the eADC is potentially storing the collected data sets for an indefinite period of time.

In addition to the WP29 Opinions and the OpenNCP specifications, the draft privacy-technologies standard ISO/CD 20889 'De-identification techniques' will be monitored.

SHiELD: Data management will also include an “expiry date”, which will be used by appropriate data management tools to identify when data should be deleted, including any associated notification. Moreover, SHiELD will progress beyond the state of the art by exploring technological aspects of right to be forgotten, e.g., enabled by distributed management of pseudoidentifiers and auxiliary data, as well as anonymisation, e.g., for health data used in Big Data subject to inference attacks.

### 2.7.3 Pseudonymisation

Concerning the retention period only for non-incompatible purposes such as research and statistics, an element of compliance may be the implementation of pseudonymisation in order to safeguard the rights and freedoms of data subjects (GDPR Article 89(1)).

Details about this legal requirement can be found in WP29 Opinion on anonymisation techniques (WP216) and the concept of personal data (WP136).

Additional guidance is given by health-informatics standard ISO 25237 'Pseudonymization’ (as amended in ISO/TC 215/N2016090).

SHiELD: Technical partners will review existing anonymisation tools with a view to what tooling can be made available within the platform.

To this end, patient data should be subject to the following proposed pseudonymisation mechanism. Patient data should be transformed into irreversible representations, in addition to storage in its original state, in order for the healthcare provider to choose whether or not to use the pseudonymisation mechanism in a particular case.

Accordingly, the transformed representations must be designed in a way that they cannot be used to allow or confirm the unique identification (authentication) of a natural person (e.g. link records about the same data subject), without the knowledge of the original data and auxiliary data. This adds to the system the possibility of enforcing another check by relying on the cooperation between entities chosen to hold those auxiliary data and those who have the knowledge about the original data.

This proposal is not limited to data categories such as name and address (direct identifiers) but may be applied to the respective modules of the health record containing the history of drugs prescriptions, treatments, etc. and even to a combination of those modules. This is because they could technically also be used to allow or confirm the unique identification (authentication) of a natural person even if they are considered anonymous or anonymised data or data having undergone pseudonymisation.

For example, this would enable healthcare providers to give patients the opportunity to consult their health data without having to reveal their identity to cloud operators in a way that they link them to previous consultations.
2.8 Responsibility

System user rights must be enforced per “controller” and “processor”. Controllers are the ones who determine the purposes of data processing (not only the means of data processing). They may be any natural or legal persons, public authorities, agencies or other bodies involved in the processing of the personal data such as hospitals, GPs, dentists, and pharmacies. For responsibility it needs to be considered whether or not

- two or more controllers are involved in the determination of the purposes and means of personal data processing (joint controllers).
- the separation of roles and responsibilities for personal data processing is clearly defined, comprehensive and up to date (GDPR Article 26)
- any (part of the) personal data processing is outsourced (processors) and if so,
- sufficient guarantees are provided by the (sub-)processor and conditions for processing are met as well as whether or not those guarantees and conditions are regularly reviewed and updated (GDPR Article 28-31)
- any personal data is transferred to a third country or an international organisation (export) and if so,
- the conditions for that personal data export are met as well as whether or not those conditions are regularly reviewed and updated (GDPR Articles 44-50).

WP3 recommends SHiELD to consider by the WP29 in their Opinions on epSOS and EHR (WP189, WP131).

In relation to the NCPs, it appears that the NCP in country A is controller for the disclosure of the patient data, and the NCP in country B is controller for the retrieval of the patient data. However, the WP29 found that there might be a different national reality. There is also a certain regulatory role at an EU level because of the delivery of central services by the epSOS project and the security and communication standards; however this is not an EU role of direct involvement in the data processing. Other issues are the acceptance of new participants and the provision of information to data subjects.

Moreover, the healthcare providers are controllers for the creation of the medical records from which the epSOS datasets are derived and sent abroad. In certain EU Member States all participating healthcare providers are also supposed to be jointly controlling the NCP processing, the NCP acting as a processor. In some countries, each health care provider is supposed to be joint controller - together with the NCP - of the NCP processing. Accordingly, if all participating healthcare providers in a country are supposed to be jointly controlling the NCP processing, such a scattered control can raise serious doubts. These doubts might be mitigated by appropriate measures to safeguard patients’ rights (e.g. pseudonymisation for data minimisation) and to guarantee transparency.

In addition to the WP29 guidance on epSOS and EHR, WP3 recommends SHiELD to consider details about the legal requirement in this subsection that can be found in WP29 Opinions on controller and processor (WP169) and cloud computing (WP232, WP196).

For example in WP169, the WP29 gives the following example for platforms for managing health data: In a Member State, a public authority establishes a national switch point regulating the exchange of patient data between healthcare providers. The plurality of controllers - tens of thousands - results in such an unclear situation for the data subjects (patients) that the protection of their rights would be in danger. Indeed, for data subjects it would be unclear whom they could address in case of complaints, questions and requests for information, corrections or access to personal data. Furthermore, the public authority is...
responsible for the actual design of the processing and the way it is used. These elements lead to the conclusion that the public authority establishing the switch point shall be considered as a joint controller, as well as a point of contact for data subjects’ requests.

SHiELD: The technical implications of the legal requirements will need further investigation, but will at least be implemented as part of an overall consideration of role-based data access management. There might be useful guidance on profiles for the roles of hospitals, internal units, cloud operators, and national health services.

3 Design and management requirements

The legal obligations introduced by the GDPR are defined as design and management requirements in this section.

WP3 recommends the SHiELD project to introduce a scenario or use case in a suitable document (e.g. SHiELD deliverable D6.1). This scenario should focus on the legal data-protection design and management requirements outlined in this section.

3.9 Risk-based approach

The risk-based approach refers to technical and economic aspects, processing scope and purposes, as well as rights and freedoms of natural persons.

WP3 recommends SHiELD to consider details about the legal requirement in this subsection that can be found in WP29 Opinion on the risk-based approach (WP218).

3.9.1 Technical and economic aspects

Controllers must take into account the state of the art and the cost of implementation.

SHiELD: As mentioned above ("data security"), technical partners are considering how best to provide a meaningful risk calculation to support data subject consent decision making, but also potential consequences for the data subject of any data breach. In SHiELD deliverable D2.1 the consortium analysed the challenges for security and privacy in health data exchange. This informs the assessment of the state of the art and costs of implementation.

For example, it will show that SHiELD will progress the state of the art by adding to epSOS-based systems tools and procedures for design time, explaining how to implement default privacy safeguards in health data exchange and possibly leading to innovative privacy-enhancing technical concepts (privacy-by-design paradigm).

3.9.2 Processing scope and purposes

Controllers must take into account the nature, scope, context and purposes of processing.

WP3 recommends SHiELD to consider by the WP29 in their Opinions on epSOS and EHR (WP189, WP131). Accordingly, data-protection measures should take into account the highly sensitive nature of the data to be processed, the central role of ICT within the framework of the project, and the cross-border dimension of the data transfers through the epSOS project. As a result, it is appropriate to implement a high level of personal data protection that should be adequate to the risks arising from the epSOS system.
3.10 Data protection by design

‘Data protection by design’ refers to the requirement to take measures as soon as at design time, pseudonymisation for data minimisation, other certain elements that help meet that requirement, regular review and updating, as well as the demonstration of the effectiveness and integration of the privacy-enhancing technical and organisational measures.

3.10.1 Measures at design time

Controllers must implement appropriate (risk-based approach) technical and organisational measures at the time of the determination of the means for data processing (at design time) and at runtime, for meeting the legal requirements (GDPR Article 25(1)).

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 (GDPR Recital 78).

The principles of data protection by design and by default should also be taken into consideration in the context of public tenders (GDPR Recital 78).

SHiELD: The design methodology for SHiELD is based on agile processes, and includes review by a legal researcher (WP3), by potential adopters (the trial partners), and the ethics adviser from IT Innovation. As such those processes are iterative. The WP3 procedures and SHiELD tools related to WP3 (e.g., risk modelling, data sensitivity, data hiding) are for design time, aiming to lead to re-configuration or even re-design of a systems for health data exchange.

3.10.2 Pseudonymisation for data minimisation

An element of compliance may be the implementation of pseudonymisation designed to implement data-protection principles such as data minimisation (GDPR Article 25(1)).

Details about this legal requirement can be found above (section “data minimisation”, subsections “anonymised” and “pseudonymisation”).

SHiELD: As mentioned above (“data minimisation”), the technical partners are currently evaluating different approaches to anonymisation. For example, related work could be addressed by the identifiability analysis in the ‘data sensitivity tools’.

3.10.3 Other elements in support of ‘data protection by design’

Other elements of demonstration of compliance may be:
— 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

(GDPR Recital 78)

The project results should enable healthcare professionals and providers to choose between different privacy-enhancing options; for example, between options to delete health data after use, to activate the pseudonymisation and to deactivate the use of certain EHR modules.

SHiELD: These specific elements are being considered within the design of platform management and audit capabilities, as well as related components for data management.

3.10.4 Updating of ‘data protection by design’

Measures for ‘data protection by design’ must be regularly reviewed and updated (GDPR Articles 25(1), 24(1)(2)).

SHiELD: These recommendations will be addressed in the iterative review via the agile software development process during the lifetime of the project. SHiELD will create guidelines to be used by potential adopters such that they know how to maintain currency and compliance.

3.10.5 Effectiveness and integration of ‘data protection by design’

Controllers must be able to demonstrate (‘assess or verify’, GDPR Recital 74) the effectiveness of the implementation and integration of the measures for ‘data protection by design’ (GDPR Article 25(1)).

Details about this legal requirement can be found in WP29 Opinion on apps on smart devices (WP202).

In addition, UK standard BSI/PAS 277 for consideration by CEN/TC 251 ‘Health informatics’ and the mHealth Code of Conduct on privacy for endorsement by the European Commission will be monitored.

SHiELD: This recommendation is part of the design and implementation, as stated above, of appropriate management and audit tools to be developed as part of the SHiELD tool set.

3.11 Accountability, data protection officer, impact assessment

Accountability comprises the requirement to demonstrate legal compliance, certain elements that help meet that requirement, as well as regular review and updating.

3.11.1 Demonstration of legal compliance

Controllers must implement appropriate (risk-based approach) measures to be able to demonstrate compliance with the legal requirements (GDPR Articles 5(2), 24(1)).

SHiELD: As mentioned above, it is suggested to create a new SHiELD scenario concerning design and management requirements including the ‘demonstration of compliance’.
**3.11.2 Elements in support of accountability**

Elements of demonstration of compliance may be:

- Implementation of data protection policies
- Implementation of data protection by design
- Adherence to codes of conduct or certification schemes
- Maintenance of a record of processing activities under the controller’s or processor’s responsibility
- Performance of a data protection impact assessment
- Cooperation with the supervisory authority concerning the personal data processing
- Monitoring by a data protection officer

(GDPR Article 24(2), Recital 78, Recital 81, Recital 82, Recital 84)

**SHiELD:** This is part of the design and implementation of reporting capabilities. The elements for compliance listed above provide the basis against which the design of such reporting will be done.

For WP3 ("privacy by design"), the suggested SHiELD scenario mentioned above, will cover the demonstration of compliance concerning the implementation of ‘data protection by design’ as a source for future WP3 reports. In relation to WP7 (exploitation including standardisation), a contribution to certification or conformity-assessment schemes is planned. The suggested SHiELD scenario will cover the demonstration of compliance concerning the adherence to codes of conduct or certification schemes.

As regards the data protection officers, and in view of possible exploitation of the project results, WP3 recommends SHiELD trial partners and their data protection, legal or IT-security officers to collaborate with the SHiELD legal researcher and ethics adviser. This would enable the project to consolidate the legal requirements definition and technical and organisational solutions in response, across the partners’ organisations.

Concerning data protection impact assessments, as mentioned above (“data security”), exploiting risk models within the project is being discussed among the technical partners. This should include the risks for the effectiveness of the legal requirements defined in this document.

In relation to the cooperation with the DPA, WP3 recommends SHiELD to consider the WP29 in their Opinions on epSOS and EHR (WP189, WP131). Accordingly, all data controllers handling epSOS data must cooperate as defined in the GDPR with the DPA, regardless of whether the data subjects are nationals or residents of another Member State and irrespective of whether the data handled originate from data controllers in other Member States. There is currently no DPA for the whole epSOS processing. Each DPA supervises his own NCP. Because of the trans-border character of the epSOS processing, co-operation between national DPAs in supervising the epSOS project is strongly recommended by the WP29.

**3.11.3 Updating of accountability measures**

Measures for demonstration of compliance must be regularly reviewed and updated (GDPR Article 24(1)). For this a process for continuous improvement of data-protection management should be implemented.
SHiELD: As well as data expiry dates (see above “data minimisation”), technical partners are currently discussing how to provide automatic alerts to service providers that review is necessary.

3.12 Certification

An approved certification mechanism may be used as an element of ‘demonstration of compliance’ (see above ‘accountability’).

According to the GDPR Articles 42 and 43, certification is a voluntary mechanism that is available via a process that is transparent and does not reduce the responsibility of the controller or the processor for legal compliance or affect the tasks and powers of the DPAs. A certification is issued by certification bodies or DPAs on the basis of criteria approved (and made public) by a DPA or by the European Data Protection Board.

Certification is issued to a controller or processor for a maximum period of three years and may be renewed, under the same conditions, provided that the relevant requirements continue to be met, or are to be withdrawn otherwise. The European Data Protection Board is obliged to collate all certification mechanisms in a publicly available register.

Certification bodies are responsible for the proper assessment leading to the certification or the withdrawal of such certification, without affecting the responsibility of the controller or processor for compliance with the GDPR. The GDPR requires “certification bodies” to

- have an appropriate level of data-protection expertise,
- inform the DPA,
- demonstrate their independence and expertise in relation to the subject-matter of the certification to the satisfaction of the DPA,
- undertake to respect the approved data-protection criteria,
- establish procedures for the issuing, periodic review and withdrawal of data protection certification,
- establish procedures and structures to handle complaints about infringements of the certification or the manner in which the certification has been, or is being, implemented by the controller or processor, and to make those procedures and structures transparent to data subjects and the public,
- demonstrate, to the satisfaction of the DPA, that their tasks and duties do not result in a conflict of interests, and to
- provide the DPAs with the reasons for granting or withdrawing the requested certification.

The GDPR also requires Member States of the European Union to ensure the accreditation of certification bodies either by DPAs or by the national accreditation body (named in accordance with Regulation 2008/765/EC) following standard EN-ISO/IEC 17065/2012 and any additional requirements set by the DPA. The accreditation of certification bodies is also subject to the criteria approved by the DPA or by the European Data Protection Board, as far as they complement Regulation 2008/765/EC and the technical rules that describe the methods and procedures of the certification bodies (in the case of national accreditation).

SHiELD: Partners envision a kind of certification approach using OpenNCP as an example that can promote SHiELD-compliant tools and SHiELD-compatible apps. Currently there is no common European Data Protection Seal in the meaning of the GDPR. Therefore, the conditions for the creation of certification schemes are relevant in order to identify opportunities for the SHiELD project to contribute to the creation of any European certification scheme for legal
data-protection requirements in health data exchange. This may be done through by participating in the

- development of any criteria for approval by the European Data Protection Board
- activities related to data-protection certification of the national accreditation bodies
- preparation and execution of any relevant delegated act adopted by the European Commission for additional requirements or any Commission implementing act for technical standards
- setting up of a data-protection certification body or scheme

For example, the Directive 2011/24/EU on the application of patients’ rights in cross-border healthcare created the ‘eHealth network’ to discuss the requirements for the exchange of information among Member States. A member of the eHealth network is CEN/TC 251 ‘Health informatics’, which we plan to approach in the course of the standardisation activities in WP7.

4 Fundamental-rights requirements

The ethical values enshrined in the European Charter of Fundamental Rights [4] are defined as fundamental-rights requirements in this section.

4.13 Fair decision-making

Data must be processed fairly (Charter [4] Article 8(2); see above ‘data subject rights’).

SHiELD: There is no plan currently to develop any automated profiling and decision making on that basis. All SHiELD held data will be managed in accordance with features exposed to data subjects as part of the informed consent process.

4.14 Privacy and data protection

Individuals have the right to protection of their privacy and personal data (Charter, Articles 7 and 8, see above ‘data protection principles’).

Details about this legal requirement can be found above (section “data minimisation”, subsections “anonymised”).

From a legal perspective, privacy protection and data protection do not have an identical scope. For example, privacy protection - currently under legislative revision - adds to data protection by covering the protection against the intrusion into a (mobile) IT system and therefore being applicable even if no data are processed or if data are anonymous or anonymised. An example of a measure of ‘data protection by design’ suggested in the draft ePrivacy Regulation (see http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=41241) is to provide online service users the ability to configure cookie options for accepting no cookies at all, no 3rd-party cookies or all cookies.

SHiELD: SHiELD software will comply with relevant legislation, but it will also allow data subjects (or an appropriate care giver) to reach informed decisions about access to and the use of their data.

4.15 Autonomy and lawfulness

Data processing must be based on the consent of the person concerned or some other legitimate basis laid down by law (Charter [4] Article 8(2); see above ‘lawfulness’).
SHiELD: The default legal basis for processing of data within a SHiELD managed environment is based on explicit and informed consent from the data subject or an appropriate care giver.

4.16 Non-discrimination

Individuals must not be treated unequally without legitimate reasons (Charter [4], general and specific non-discrimination requirements).

SHiELD: All data subjects will be treated in accordance with the user choices made available to individuals whose data is managed by SHiELD. All such users will be presented with the same choices.

4.17 Human dignity

Human dignity is inviolable and must be respected and protected (Charter [4] Article 1).

SHiELD: Personal data managed by SHiELD will be released only under strictly controlled circumstances, by default in accordance with data subject consent, or in pursuit of the vital interests of the data subject. There will therefore be guarantees to avoid human dignity of any individual to be compromised.

4.18 Public health and access to health care

This subsection covers the fundamental rights to access to health care and the public-health objectives of the European Union.

4.18.1 Access to health care

Individuals have the right of access to preventive health care and the right to benefit from medical treatment under the conditions established by national laws and practices (Charter [4] Article 35).

SHiELD: As directed by the project trials, SHiELD might provide appropriate tools to raise alerts in connection with a specific data access request if and only if any such alert could lead to preventive intervention. What constitutes such an intervention will be determined by the trial partners.

4.18.2 Public health

A high level of human health protection must be ensured in the definition and implementation of all European Union policies and activities (Treaty on Functioning of the European Union, Article 168). For example, the Directive 2011/24/EU on the application of patients’ rights in cross-border healthcare was introduced by the European Union legislator. The Directive offers a possible legal basis for health data exchange (WP189).

SHiELD: The entire premise for the SHiELD project is to ensure that in respecting the wishes (“informed consent”) of the data subject, any exceptional cases (solely) related to the vital interests of that data subject will be carefully managed. All non-consent-based data access requests will be logged and alerted to the data subject when convenient and/or to an appropriate person or body (e.g., the DPA).

4.19 Proportionality and mission creep

This subsection describes the legal requirements of proportionality and protection against mission creep.
4.19.1 Proportionality

Any limitation on the exercise of the rights and freedoms of individuals must be proportionate. Limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the European Union or the need to protect the rights and freedoms of others (Charter [4] Article 52). Accordingly, the benefits for the various health and care services must be balanced with the impact on the rights and freedoms of data subjects and other natural persons.

Details about this legal requirement can be found above (section “data minimisation”, subsection “amount of data”).

SHiELD: Any healthcare intervention to result from access to data other than via explicit and informed consent will only be permitted on SHiELD if the vital interests of the data subject would otherwise be compromised. What constitutes a balanced approach will be determined by the trial partners.

4.19.2 Mission creep

Precautions must be taken against misuse of technology originally intended for a legitimate use (“mission creep”, “function creep”). Special attention should be given to the centralised aspects of an epSOS-based system. The epSOS interfaces require NCPs to comply with a certain structure, behaviour and security policy. In addition there are a number of information sources which are relevant for every NCP and must be in the same state for every NCP. Examples for this are common taxonomies, schemas, and web service endpoint addresses of NCPs. This shared data is centrally managed in order to avoid inconsistencies and version conflicts in a generalisation process of epSOS [8].

SHiELD: SHiELD management and audit tools will be implemented to ensure that data can only be accessed and used within strict constraints, typically and by default in respect of data subject consent. For example, SHiELD might make use of the UK de-centralised architecture, which is based on index data (MPIX), record types and references (as opposed to more centralised systems e.g. in Austria), and the OpenNCP, which is designed in an even more de-centralised way.
5 Conclusions

This report analysed the legal requirements related to data-protection law and fundamental rights relevant to the SHiELD project. The new legal nature (a single EU law) and obligation of ‘data protection by design’ and accountability introduced by the GDPR bring about challenges for the SHiELD project.

Whereas the consortium is free to choose what specific technical and organisational measures are taken, they will need to offer a satisfactory level of protection (risk-based approach) using pseudonymisation for data minimisation and other kinds of measures. Other solutions than the ones suggested in this report, which might become apparent during the ongoing project and covered in the next WP3 report, may also qualify as satisfying the legal obligations.
6 References


