Deliverable
D8.1 Privacy Implications

<table>
<thead>
<tr>
<th>Workpackage</th>
<th>WP8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lead beneficiary</td>
<td>FIZ</td>
</tr>
<tr>
<td>Due date</td>
<td>30th November 2016</td>
</tr>
<tr>
<td>Submission date</td>
<td>30th November 2016</td>
</tr>
<tr>
<td>Type</td>
<td>R, PU</td>
</tr>
<tr>
<td>Author(s)</td>
<td>Diana Dimitrova, Francesca Pichierri, Franziska Boehm</td>
</tr>
<tr>
<td>Abstract</td>
<td>Privacy, data protection, health data, privacy by design/default</td>
</tr>
</tbody>
</table>

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 689947.
# History of changes

<table>
<thead>
<tr>
<th>Rev. N</th>
<th>Description</th>
<th>Author(s)</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>First draft of TOC</td>
<td>Diana Dimitrova, Francesca Pichierri</td>
<td>29&lt;sup&gt;th&lt;/sup&gt; September 2016</td>
</tr>
<tr>
<td>2</td>
<td>First draft of the document</td>
<td>Diana Dimitrova, Francesca Pichierri</td>
<td>5&lt;sup&gt;th&lt;/sup&gt; October 2016</td>
</tr>
<tr>
<td>3</td>
<td>Review</td>
<td>Franziska Boehm, FIZ</td>
<td>2&lt;sup&gt;nd&lt;/sup&gt; November 2016</td>
</tr>
<tr>
<td>4</td>
<td>Final version review</td>
<td>Jordi Rovira, TID</td>
<td>14&lt;sup&gt;th&lt;/sup&gt; November 2016</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table of contents

List of Abbreviations ............................................................................................................................................. 3

Abstract .................................................................................................................................................................. 4

1. Introduction ..................................................................................................................................................... 7

2. The EU Privacy and Data Protection Framework and STARR ...................................................................... 7

   CHAPTER 1: The Right to Privacy and Data Protection and Applicable Law ..................................................... 8

   CHAPTER 2: Relevant Definitions .................................................................................................................. 15

   CHAPTER 3: Legal grounds for processing .................................................................................................. 27

   CHAPTER 4: Key principles of personal data processing ............................................................................. 32

   CHAPTER 5: Data subjects rights .................................................................................................................. 37

   CHAPTER 6: Transfers to Third Countries .................................................................................................. 46

   CHAPTER 7: Data Protection Impact Assessment ....................................................................................... 49

3. Conclusion ...................................................................................................................................................... 55

4. Bibliography .................................................................................................................................................... 56
List of Abbreviations

CFREU – Charter of Fundamental Rights of the European Union
CJEU – Court of Justice of the European Union
CoE – Council of Europe
DPIA – Data Protection Impact Assessment
ECHR – European Convention of Human Rights
ECtHR – European Court on Human Rights
EDPS – European Data Protection Supervisor
GDPR – General Data Protection Regulation
MS – Member State
TC – Third Country
TEU – Treaty on the European Union
TFEU – Treaty on the Functioning of the European Union
Abstract

The present deliverable, the first one on privacy and data protection in STARR, presents an analysis of the EU privacy and data protection requirements and principles as they apply to the STARR project at the present stage of its development. With the elaboration of the technology in the future months this legal analysis will also be deepened and extended. Therefore, the analysis should not be regarded as finalized. It is rather an overview of the applicable legal rules and a first application to the current version of the STARR technology.

Data protection is given a special focus in the project since the core of the planned STARR technology is the processing of personal data, i.e. data relating to identified or identifiable natural persons. More precisely, STARR will process stroke survivors’ data which relates to their blood pressure, physiological data, medication, physical performance, etc. More importantly, such personal data are considered to be sensitive data due to the rich information it could reveal about particular individuals, e.g. about their health and habits. Therefore, STARR should comply with the EU data protection law and the national specifications on data protection as research activities are not exempt from these data protection provisions. Many of the recommendations in this deliverable would be also applicable to the exploitation of the STARR application if it becomes operational.

The requirements and principles which the deliverable analyses and applies have been derived mainly from the following legal acts:

- Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU).
- Article 8 of the European Convention on Human Rights (ECHR).
- Directive 95/46/EC on the protection of personal data and its free movement within the Union and its successor – the General Data Protection Regulation (GDPR), which will be applicable as of May 2018.

Further requirements have been derived from the case-law of the Court of Justice of the EU (CJEU) and the European Court of Human Rights (ECtHR) and from authoritative opinions of expert groups such as the Article 29 Working Party.

More precisely about the requirements and their application to STARR, the project should define the purposes of the selected personal data processing operations of the STARR technical solution, both in the research/validation phase and in the actual operation of the STARR application in real life. The same applies also to the STARR research activities, e.g. carrying out interviews with stroke survivors. This would fulfill both the requirement on legitimate aim for interference with the rights to privacy and data protection (Article 52 (1) CFREU) and on purpose specification (Article 6 (1) (b) Directive 95/46/EC and Article 5 (1) (b) GDPR).

The project should then assess whether the planned technology is necessary and proportionate to the actual achievement of the said objective(s). When assessing the compliance with these two principles, one should look at the appropriateness and effectiveness of the measure, e.g. the STARR app, for achieving the aim, e.g. assist rehabilitation and/or prevent secondary stroke, and demonstrate that there are no other less intrusive means of achieving the aim, e.g. there are no other similarly effective solutions in achieving this purpose which process fewer personal data or process it in a more privacy-friendly way.
Once the necessity and proportionality are demonstrated, the STARR solution should satisfy the following requirements and principles:

- **Legal basis** – the STARR solution itself and the STARR research activities should have a basis in law. For example, the consent of the users of the STARR app/platform seems to be the most likely candidate for legal basis as the STARR project would give stroke survivors the opportunity to voluntarily participate in the STARR research and test activities after having informed them of the implications for their personal data.

- **Purpose specification** – the deliverable has made a suggestion of possible legitimate purposes and the limitation of the legitimate use of the data. For example, a legitimate purpose would be researching/testing the performance, acceptance and accuracy of the STARR solution for purposes of facilitating the rehabilitation of stroke survivors while excluding the usage of health data for marketing purposes.

- **Data minimization** – the deliverable has made suggestions on the proportionate categories of personal data which can be used by the STARR platform, e.g. collecting and further processing only the data which are necessary for rehabilitation and not collecting more data, e.g. collecting information about habits which are not relevant for stroke survivors’ rehabilitation.

- **Data accuracy** – since working with accurate data is crucial for the success of the treatment of stroke survivors, the deliverable recommends ensuring that the quality of the data can be monitored and corrected easily if inaccuracies are detected.

- **Limitation on data storage** – data in principle should not be stored for longer than necessary. Thus, personal data not needed any more during the course of the project or at latest at the end of the project should either be deleted or permanently anonymised.

- **Data security** – while the definition and implementation of the technical measures for ensuring the security of the personal data are the responsibility of the technical partners, the deliverable extracts the legal requirements on data security to ensure that patient data is not compromised when processed by the STARR solution.

- **Privacy by design and by default** – the deliverable has made a set of recommendations on how to integrate the privacy requirements in the design on the technology, e.g. by allowing STARR users to have more control over the processing of their personal data by giving them the opportunity to choose with whom their STARR data is shared.

- **Data Protection Impact Assessment (DPIA)** – the deliverable sets the framework for carrying out this assessment by providing a preliminary list of data protection risks and initial suggestions for mitigating these risks. This framework, presented in the form of a table, should be elaborated on in the next months of the project together with the technical partners.

Another aspect discussed in the deliverable is the issue of data transfers outside the European Union. The analysis of the procedures for such transfers could be relevant for STARR as one of the partners in STARR, i.e. RT-RK, is established in Serbia. However, since their role in the data processing tasks in STARR is not clear yet, a more in-depth analysis on data transfers would be provided in the next deliverables if necessary.

Last but not least, the respect of data subject rights is of paramount importance. This refers to the rights to information, access to own personal data, rectification, erasure (or right to be forgotten), data portability, blocking or objection. Having procedures in STARR to allow the STARR data subjects to exercise these rights is
the best way for ensuring that these rights are respected. The deliverables recommends what procedure should be followed in STARR to help data subjects exercise these rights. An example of such a recommendation is what information should be provided to STARR volunteers before they consent to participate in the STARR research activities and use the STARR solution.
1. Introduction

The amount of personal data processed in the health and research context continues to rise every year. New tools and services using information and communication technologies (ICTs) can improve prevention, diagnosis, treatment, monitoring and management but they can also extend the possibility of collecting, storing, sharing, disseminating and editing personal data considered to be “sensitive data”, such as health data and biometric data, at a very low cost. While methods, technics and volume of data processing are increasing, the control over data is decreasing and this may consequently lead to a misuse of data, compromising the privacy of individuals. A misuse of sensitive data may be irreversible and could have severe and long-term consequences on the individual’s fundamental rights; a misuse of personal health information, for example, can have strong consequences for the patient such as financial and psychosocial harms.

In order to prevent that, as the STARR project will involve the design, testing, and possible operational exploitation of such technology and the processing of large and various amounts of personal data, especially health data, it is paramount that all the technical partners comply with the European legal framework designed to protect the privacy and the personal data of individuals, in this specific case of stroke survivors and health professionals. Especially, we encourage the partners to integrate the privacy requirements in the design of the technology.

The aim of the deliverable is to guide the partners through a general overview of the existing European regulatory system. In the first chapter, a brief analysis of the applicable law for the planned STARR platform (from a European perspective) is provided. Relevant concepts and the legal grounds for processing are explored respectively in the second and in the third chapter. The fourth chapter analyzes key-principles of personal data processing while the fifth is dedicated to the data subject rights. The transfer to third countries and the data protection impact assessment are investigated in the last two chapters of the present deliverable.

2. The EU Privacy and Data Protection Framework and STARR

The purpose of the present section is to examine the currently applicable EU data protection framework and give examples of its application to the STARR technology and research activities, which involve the processing of personal data. It will provide a brief background on the rights to privacy and data protection. Then it will go on to examine the basic principles and requirements, which stem from the EU secondary data protection legal acts. They will be applied as much as possible to STARR. This application will be elaborated on in the future deliverables. The present section will also make a first sketch of the possible data protection risks in STARR and propose measures to mitigate them. The authors of the deliverable are aware that currently both Directive 95/46/EC and the GDPR are in force but the GDPR will be applicable only as of 25 May 2018. Thus, while those who process personal data and are subject to the EU data protection framework currently have to satisfy the conditions of Directive 95/46/EC, they should start adjusting to the new requirements stemming from the GDPR.

---

Therefore, both of these legal acts will be examined, in addition to other legal acts such as the e-Privacy Directive.

CHAPTER 1: The Right to Privacy and Data Protection and Applicable Law

The notion of “private life” is rather broad. Depending on the circumstances, the concept may extend to the moral and physical integrity of an individual. Following the jurisprudence of the European Court of Human Rights (ECtHR), the right to protection of personal data forms part of the rights protected under Article 8 of the European Convention on Human Rights (ECHR), an international treaty adopted by the Council of Europe (i.e. the right to respect for private life and family life, home and correspondence). Under the European legal system, the right to privacy and the right to the protection of personal data are regarded as fundamental rights, protected by a number of instruments passed by both the Council of Europe and the European Union. The EU, while often following the jurisprudence of the ECtHR, treats the rights to privacy and data protection as separate rights, although they often overlap. In the STARR context, for instance, when tests are performed with stroke survivors to evaluate the developed solution, non-consensual or compulsory medical treatment or examination of any kind will certainly fall within the protective scope of private life under Article 8 ECHR and the Charter of Fundamental Rights of the European Union (CFREU).

The regulatory instruments provided by both institutions (Council of Europe and European Union), however different, are in fact overlapping and they express common principles in the field. These will be examined below.

The Council of Europe

The European Convention on Human Rights

Article 8 of the European Convention on Human Rights (ECHR), adopted by the Council of Europe in 1950 and entered into force in 1953, guarantees the right to respect for private and family life, home and correspondence. It also lays down the conditions under which restrictions of this right would be justified. No interference by a public authority with the exercise of this right is allowed except if it pursues a legitimate aim and it is “in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others”.

The European Court of Human Rights (ECtHR) specified that the word “in accordance with the law” requires the impugned measure both to have “some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual - if need be with appropriate advice - to regulate his conduct”. Therefore, the ECtHR examines also the “quality of the law” and this means that the legal rules that do not have the relevant quality are not

---

1 ECtHR, Costello-Roberts v. the United Kingdom, No. 13134/87, March 25, 1993.
2 See, e.g.: ECtHR, Malone v. the United Kingdom, No. 8691/79, August 2, 1984; ECtHR, Copland v. the United Kingdom, No. 62617/00, April 3, 2007; ECtHR, Klass and Others v. Germany, No. 5029/71, September 6, 1978; ECtHR, Uzun v. Germany, No. 35623/05, September 2, 2010; ECtHR, Leander v. Sweden, No. 9248/81, March 26, 1987; ECtHR, S. and Harper v. the United Kingdom, Nos. 30562/04 and 30566/04, December 4, 2008.
5 Article 8 (1) ECHR.
6 Article 8 (2) ECHR. Emphasis added.
7 ECtHR, Gillan and Quinton v. The United Kingdom, No. 4158/05, January 12, 2012, par. 76.
“law” in terms of the ECtHR, not even if they serve a “legitimate aim” (e.g., national security, public safety, public order, etc).9

Regarding the term “necessary”, the word itself implies that the legitimate aim that is pursued by the interference on the rights cannot be achieved by less restrictive measures.10 Assessing the necessity requirement implies also a proportionality test; an interference would be considered “necessary in a democratic society” for a legitimate aim if it answers a “pressing social need”, if it is reasonably proportionate to the fulfilment of that need and if the reasons adduced by the national authorities to justify it are “relevant and sufficient”.11 Any interference with Article 8 will not be considered, in principle, disproportionate if it is “restricted in its application and effect, and is duly attended by safeguards in national law so that the individual is not subject to arbitrary treatment.”12

Convention 108

As a consequence of the emergence of information and communication technology in the 1960s, new and more detailed rules were needed in order to safeguard individuals’ personal data. Taking as a point of reference the Article 8 of the ECHR, the Committee of Ministers of the Council of Europe started to adopt various resolutions on the protection of personal data.13 In 1981, the Council of Europe enacted the Convention for the protection of individuals with regard to the automatic processing of personal data (Convention 108)14, which was, and still remains, the only legally binding international instrument dealing specifically with data protection. In STARR, every partner is established in a Member State of the Council of Europe15, which has ratified the Convention.16 Participation in the Convention 108 is not exclusively limited to Member States of the Council of Europe. The Convention, in fact, is open to accession by non-member States, even non-European countries, such as Serbia, which has already ratified it. In 1999, the EU became a Party of the Convention.17

Conventio 108 applies to all data processing carried out by both the private and public sector and it sets out minimum standards aimed at protecting individuals against abuses connected with the processing of personal data. The important principles established by the Convention 108 concern, in particular, fair and lawful collection and automatic processing of personal data, storage for specified and legitimate purposes, not for use for ends incompatible with those purposes, nor kept for longer than is necessary. Furthermore, they concern the quality of the data, in particular that data must be adequate, relevant, accurate and not excessive (proportionality); the confidentiality of sensitive data such as person’s race, politics, health, religion, sexual life or criminal record; the individual’s right to know that information is stored on him or her (information of the data subject); and his/her right of access and rectification. These principles will be examined in depth in the following chapters.

---

10 Ibid.
12 CoE, Committee of Ministers (1973), Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, September 26, 1973; CoE, Committee of Ministers (1974), Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, September 20, 1974.
13 CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS No. 108, 1981.
14 but not of the European Union, since RT-RX is established in Novi Sad, Serbia, which is not an EU MS.
16 CoE, Amendments to the Convention for the protection of individuals with regard to automatic processing of Personal Data (ETS No. 108) allowing the European Communities to accede, adopted by the Committee of Ministers, in Strasbourg, on 15 June 1999; Article 23 (2) of the Convention 108 in its amended form.
Convention 108 also regulates the trans-border flow of personal data. In 2001, an Additional Protocol to Convention 108 was adopted introducing provisions on trans-border flows of personal data to a recipient, which is not subject to the jurisdiction of a Party to the Convention and on the mandatory establishment of national data protection supervisory authorities.\textsuperscript{18}

Another important instrument specifying the right to data protection at European level (which is not an EU instruments) is the OECD Guidelines of 1980 governing the protection of privacy and trans-border flows of personal data (OECD Guidelines).\textsuperscript{19}

\textit{The European Union}

\textbf{Primary EU law}

In the EU law, the fundamental rights to private and family life and to data protection are enshrined respectively in Article 7 and in Article 8 of the Charter of Fundamental Rights of the European Union (hereafter, CFREU).\textsuperscript{20} Data protection is also enshrined in the Treaty of the functioning of the European Union, Article 16.\textsuperscript{21} After the coming into force of the Lisbon Treaty in 2009, the CFREU has acquired the status of primary law.\textsuperscript{22} EU law is composed of “primary EU law”, namely the treaties (the Treaty on European Union, TEU and the Treaty on the Functioning of the European Union, TFEU)\textsuperscript{23} and the CFREU that have been ratified by all EU Member States and “secondary EU law”, such as regulations, directives and decisions adopted by the EU institutions which have been given authority under the treaties.

According to the CFREU, “everyone has the right to respect for his or her private and family life, home and communications”\textsuperscript{24}; moreover, everybody has the right to the protection of personal data concerning them.\textsuperscript{25} Data must be processed fairly for specific purposes (purpose limitation principle) and on the basis of consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data, which has been collected concerning them, and the right to have it rectified.\textsuperscript{26} Compliance with the rules mentioned above shall be subject to control by an independent authority.\textsuperscript{27} EU institutions must observe and guarantee these rights; they also apply to Member States when implementing Union law.\textsuperscript{28}

It is worth noting that the CFREU makes a clear distinction between the right to privacy and data protection. This distinguishes the CFREU from other important human rights instruments that mostly treat the protection of personal data as an extension of the right to privacy. The latter is often interpreted as a combination of two different dimensions: the \textit{informational privacy}, which involve the protection from unwanted access to private information, and the \textit{physical privacy}, namely the protection from unwanted access to the physical and personal

\begin{itemize}
\item \textsuperscript{18} CoE, Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data, regarding supervisory authorities and transborder data flows, CETS No. 181, 2001.
\item \textsuperscript{19} OECD, Recommendation concerning Guidelines governing the protection of privacy and transborder flows of personal data, September 23, 1980.
\item \textsuperscript{21} EU, Treaty on the Functioning of the European Union 2012/C 126/01.
\item \textsuperscript{22} See Article 6 (1) of the Consolidated Version of the Treaty on European Union [2010], OJ C83/13.
\item \textsuperscript{23} EU, Consolidated Version of the Treaty on European Union [2010], OJ C83/13; and Consolidated Version of the Treaty on the Functioning of the European Union [2010], OJ C83/47.
\item \textsuperscript{24} Article 7 CFREU.
\item \textsuperscript{25} Article 8 (1) CFREU.
\item \textsuperscript{26} Article 8 (2) CFREU.
\item \textsuperscript{27} Article 8 (3) CFREU.
\item \textsuperscript{28} Article 51 CFREU; European Union Agency for Fundamental Rights, Handbook on European Data Protection Law, 2014.
\end{itemize}
space of the individual. In doctrine, it has been suggested that data protection offers individuals more rights over more types of information than the right to privacy, in the context of personal data processing. It seems also that the new General Data Protection Regulation (GDPR) absorbs this interpretation stressing the independence of this right and considering data protection as a proactive right to manage one’s own personal data, offering individuals enhanced control over their personal information; this protection goes beyond protecting privacy. The GDPR refers primarily to the right to data protection, removing most references to the right to privacy. However, there is still a lack of clarity on this matter. The European Court of Justice, for instance, although recognizing that the two rights are separate, also refers to them as a merged species. Due to the obvious similarities and numerous situations in which these rights may overlap, they will be examined in tandem when analysing their application within the framework of the STARR project.

Article 52 (1) of the CFREU recognizes that limitations may be imposed on the exercise of rights such as those set forth in Articles 7 and 8 of the Charter, similarly to the limitations provided for in Article 8 (2) ECHR. Any limitations must be provided for by law, respect the essence of those rights and freedoms and, subject to the principle of proportionality, 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. The right to privacy and data protection, thus, are not absolute rights, but must be considered in relation to their function in society.

Secondary EU law

The main EU legal instrument on data protection is Directive 95/46/EC of the European Parliament and 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, (hereinafter, Directive 95/46/EC). It had to be transposed by each EU Member State into national law as a result of which all Member States have enacted their own data protection legislation.

Directive 95/46/EC, in fact, was adopted to harmonise national provisions on protection of individuals in processing and free movement of personal data. Directive 95/46/EC has two main purposes: to allow for the free flow of data within Europe and to achieve a minimum level of data protection throughout all Member States. Directive 95/46/EC is designed to give substance to the principles of the right to privacy already contained in Convention 108, and to develop them. It needs to be noted that “a number of provisions of the Directive 95/46/EC contain a substantial degree of flexibility, so as to strike the appropriate balance between protection of the data subject’s rights on the one side, and on the other side the legitimate interests of data controllers, third parties and the public interest which may be present”.

---

31 See e.g., Lindsey O., The Foundation of EU Data Protection Law, Oxford University Press, 2015, p. 131.
32 Ibid.
33 Article 52 (1) CFREU; see e.g. Case 131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González [2014], OJ C212/4, (n 50), para 74.
34 Ibid., para. 50.
35 See, e.g., CJEU, Joined cases C-92/09 and C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, November 9, 2010, para. 48.
In 2012, the European Commission proposed a new General Data Protection Regulation (hereinafter, GDPR), which entered into force on April 27, 2016.\(^{40}\) It shall apply from the 25\(^{th}\) of May 2018,\(^{41}\) after a two-year transition period, and it will replace the Directive 95/46/EC and provide a new comprehensive data protection law for the EU. Unlike directives, EU regulations do not require any transposing legislation to be passed by Member States. A new General Data Protection Directive will provide for data protection in the areas of police and judicial cooperation in criminal matters;\(^{42}\) since this new directive does not seem relevant for the STARR project at this point, it will not be further discussed.

More detailed data protection provisions are often needed in order to achieve the necessary clarity in balancing other legitimate interests. Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector (hereinafter, e-Privacy Directive)\(^{43}\), for example, deals with data protection in the electronic communications sector, which includes telecommunications, faxes, e-mail, the internet and other similar services, applications, such as smartphone apps.\(^{44}\) It is understood that the STARR solution would rely on such services, e.g. the smartphone and/or tablet app. Thus, it seems that the e-Privacy Directive will be applicable to the STARR solution.

**Scope of application of Directive 95/46/EC and GDPR and their application to STARR**

Pursuant to Article 3 of Directive 95/46/EC on the material scope of the Directive, it applies to data processing which is wholly or partially automated, also to non-automated processing of data which (intends to) form(s) part of a filing system. The scope excludes the processing of data covered by the Common Foreign and Security Policy (CFSP), in the law-enforcement and national security sectors or processing “in the course of a purely personal or household activity.” The GDPR does not change this structure/configuration. It only specifies that the GDPR also does not apply to data processing by Union institutions and bodies, as this is subject to Regulation 45/2001. It does not apply to the processing in the context of an activity, which falls outside the scope of Union law.\(^{45}\) With regards to the e-Privacy Directive, it harmonizes the data protection and privacy provisions in the Member States in the electronic communications sector. It thus particularizes and complements Directive 95/46/EC in this sector. The scope excludes the processing of data covered by the Common Foreign and Security Policy (CFSP) and in the law-enforcement and national security sectors, similarly to Directive 95/46/EC.

For STARR this means that Directive 95/46/EC and the GDPR are fully applicable (1) to the research phase of the project, e.g. when the STARR partners interview patients and medical specialists and collect their personal data or later on when pilots are performed with stroke survivors to test the developed STARR solution, and (2) to the possible exploitation of the STARR solution in a real-life environment, e.g. when patients interact with the solution to communicate through it with their carers or doctors. Therefore, the one(s) who will be designated as controller(s) will need to comply with the requirements of the Directive (and the GDPR). The requirements should be ideally complied with already at the stage when the STARR solution is designed, as well as when

---


\(^{41}\) Article 99 GDPR.


\(^{44}\) The Directive 2002/58/EC has been amended by Directive 2009/136, which introduces several changes, especially concerning cookies.

\(^{45}\) Article 2 GDPR.
operating the solution in practice. When a stroke survivor uses the solution to communicate with his/her relatives one could argue that this processing might fall under the definition of a “purely personal or household activity.” However, this exemption rather implies that the data protection framework does not create responsibilities for the relatives of the stroke survivor who participate in the communication loop. In any case, the communication between the stroke survivor and medical staff would be covered by the EU data protection framework. **Undoubtedly the personal data processing within the framework of the STARR project itself will fall under the material scope of the two laws as no exemption applies to it.**

As to the **territorial scope** of Directive 95/46/EC, pursuant to Article 4 (1) (a) thereof, EU Member States shall apply their national implementing laws to data controllers when “the processing is carried out in the context of activities of an establishment of the controller on the territory of the Member State.”

The Court of Justice of the European Union (CJEU) has clarified and interpreted this provision broadly in the *Google vs Spain* case, where it ruled that the mere setting up of a branch or subsidiary (*in casu* Google) in Spain whose purpose is promoting and selling advertising space offered by a search engine and oriented towards the inhabitants of a certain Member State falls within the scope of Article 4 (1) (a) of the Directive.

Recently the CJEU interpreted the provision more restrictively, implying that the mere existence of an establishment on the territory of a certain Member State in itself does not suffice for triggering the application of the national law of that Member State. However, the context was different, as there was no doubt about the applicability of EU law as such but the question was rather, which of all EU national laws was applicable. Once the applicability of EU law is established and it turns out that a controller has an establishment in more than one EU Member State, then he should designate a controller in each EU Member State who has to comply with the data protection law of the respective EU Member State. To remedy this situation where an establishment needs to comply with the data protection requirements of more than one Member State, the GDPR, which replaces the Directive, is conceived as a regulation and not as a Directive. This means that the Regulation, unlike the Directive, does not need to be implemented into national law. Thus, one single law is applicable in all EU Member States instead of 28 different laws.

**The implications for STARR are that in the project phase the one(s) who will be designated as controller(s) for a certain activity have to comply the provisions of their national data protection laws until the time the GDPR becomes applicable (i.e. May 2018). After this date the GDPR, will be one uniform law for all the EU Member States.**

Even if a controller is not established in the EU (and Article 4 (1) (a) of the Directive does not apply) but for the purposes of personal data processing makes use of equipment which is situated on EU territory, then the data protection law of the EU Member State where this equipment is situated is applicable, unless this equipment is used only for transit purposes. In that case, however, the controller should appoint a representative established in the Member State in which the equipment used for the personal data processing is situated. This is without prejudice to the responsibilities of the controller and the legal actions that can be taken against him/her. The role of this representative and his liability, however, is not clearly defined by the Directive and

---

46 Article 4 (1) (a) Directive 95/46/EC.
47 CJEU, C-131/12 Google vs Spain, 13 May, 2014.
49 Article 4 (1) (a) Directive 95/46/EC.
50 Article 4 (1) (c) Directive 95/46/EC.
51 Article 4 (2) Directive 95/46/EC.
The GDPR has modified the territorial scope of the EU data protection law. It applies to personal data processing “in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.”

Thus, it applies also to establishments of the processor and not only of the controller. In addition, it is not necessary that the processing takes place in the EU, as long as the processing is in the context of the activities of an establishment of a controller or processor in the Union. It is understood that if such a processing, under Article 3 (1) GDPR takes place in a Third Country (TC), the data will be transferred to this TC by the controller or processor established in the EU. Further, even if the controller and/or processor are not established on EU territory but still offer goods or services to data subjects in the EU, no matter whether against payment or for free, the GDPR is applicable. This is also the case when the controller and/or processor monitor the behavior of data subjects if the behavior takes place in the Union.

Similarly to the Directive, Article 27 of the GDPR requires the controller or processor, who is not established in the EU but to whom EU data protection law applies, to appoint a representative in the EU. This representative should be established in one of the Member States where the data subjects whose behavior is monitored or to whom services are offered are. The representative shall be mandated to be addressed by supervisory authorities and data subjects (in addition to or instead of the controller/processor). Again, the role of the representative should be without prejudice to the liability of the controller or processor who appointed them. Therefore, there is still some degree of uncertainty as to under what regime the data, which are processed in a Third Country by a controller or processor not established in the EU, should be processed in a Third Country. Unlike Directive 95/46/EC, the GDPR applies directly also to processors (and this not exclusively to controllers) not established in the EU. Bearing in mind the fact that the GDPR has provisions on data transfers in Chapter V GDPR, it would be logical to assume that the direct applicability of the GDPR to such data processing entities does not prevent the application of the provisions on data transfers but this has to be assessed on a case-by-case basis.

**Application to STARR**

For STARR this means that since all partners are established in the Union, except for RT-RK (established in Novi Sad, Serbia, which is not an EU Member State), use equipment in the EU and their (research) activities would be oriented towards data subjects in the EU (whether exclusively or not), the personal data processing activities in the framework/lifetime of the STARR project would fall within the territorial scope of Directive 95/46/EC and subsequently of the GDPR.

As concerns RT-RK, to determine the legal framework within which it may process personal data within the STARR project, one will need to determine exactly in which personal data processing operations it plans to

---

53 Ibid, p. 25.
54 Article 3 (1) GDPR.
55 Article 3 (2) (a) and (b) GDPR.
56 See Article 27 (2) GDPR. The requirement to appoint a representative does not apply to public authorities/bodies and to processing which is occasional, does not include on a large scale processing of special categories of data (e.g. health data) and does not pose risks to the rights and freedoms of natural persons.
57 Article 27 (3) GDPR.
58 Article 27 (4) GDPR.
participate, if any. If RT-RK processes personal data in STARR one needs to determine its role in this personal data processing, i.e. whether as a controller or as a processor, what equipment will be used and who owns it, as well as the data flows surrounding these data processing activities (including the different countries in which data processing will take place and possibly also transfers between RT-RK and the other STARR partners). This will also answer questions such as whether RT-RK will directly collect the data itself, whether it will use its own equipment, where exactly the data will be processed, etc. It is important to know that RT-RK has offices not only in Serbia, but also in Osijek, Croatia,\(^59\) which is an EU Member State. Thus, RT-RK has an establishment in the EU. However, it is not clear whether the personal data to be processed by RT-RK are to be processed in the context of this establishment in Croatia and thus whether the Croatian office can be considered as RT-RK’s representation in the EU. Another aspect to consider is whether the data processing to be carried out by RT-RK could take place in Croatia instead of in Serbia. Thus, there are two possibilities:

I. RT-RK processes the personal data in its offices in Croatia and not in Novi Sad. Then the data does not leave the EU and Croatian law needs to be observed, especially if RT-RK would act as a controller.

II. RT-RK processes the personal data in its Serbian offices. It could be the case that even if Directive 95/46/EC and subsequently the GDPR directly apply to RT-RK (e.g. because of use of equipment on EU territory or monitoring behavior of data subjects in the EU), to process the data in Serbia, a transfer still needs to take place. Data transfer(s) to RT-RK Novi Sad would also take place if the other STARR partners collect the data in the EU and transfer it to RT-RK, i.e. RT-RK is a processor for them. Such a data transfer from the EU to a Third Country falls within the scope of Articles 25 and 26 Directive 95/46/EC and/or subsequently within Articles 44-49 GDPR. The EU legal framework on data transfers is discussed in detail in Chapter 6 of the present deliverable. However, such a transfer could be problematic and present administrative burdens, e.g. submission of a notification to a data protection authority in the EU accompanied by detailed documentation related to the transfer, negotiating data security measures with the recipient, etc. Should it take place anyway, the administrative work should be taken care of well in advance.

CHAPTER 2: Relevant Definitions

PERSONAL DATA

Under EU law, “personal data” are defined as “information relating to an identified or identifiable natural person”\(^60\), a natural person can be considered as “identified” when his/her identity is manifestly clear and, within a group of people, he or she is distinguished from all other members of the group and recognisable as an individual.\(^61\) An “identifiable natural person” is an individual who can be identified, directly or indirectly, by obtaining and combining additional information, “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”.\(^62\) It is worth pointing

---

60 Article 2 (a) Directive 95/46/EC; Article 2 (a) Convention 108; Article 4 (1) GDPR.
62 Article 4 (1) GDPR. Emphasis added.
out that if data about a natural person are being processed, this person is called the “data subject”; in the context of STARR the data subject is the patient, precisely the stroke survivor.

The extent to which certain identifiers are sufficient to achieve identification depends on the context of the particular situation. A person’s name is the most common identifier. As many names are not unique, establishing the identity of a person may need additional identifiers (such as date and place of birth, sex, names of the parents, name of carers, address or a photograph) to ensure that a person is not confused with someone else. IP addresses can also be considered as data relating to an identifiable person. Recital 26 of the GDPR (following Recital 26 of Directive 95/46/EC), concerning the term “identifiable”, says that “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.” This means that a mere hypothetical possibility to single out the individual is not enough to consider the person “identifiable” but different and dynamic criterion should be taken into account.

It is important to stress that data concerns an individual when “it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated”. Thus, in order to consider that the data relate to an individual, first a content element is needed: information relates to an individual when it is “about” that individual, taking into account all the circumstances surrounding the case (for example, the results of medical analysis clearly relate to the patient/stroke survivors). Additionally, a purpose element and a result element should be present: the first one exists when the data are used or are likely to be used for the purpose of evaluating, treating in a certain way or influencing the status or behaviour of an individual; the latter exists when the use of data is likely to have an impact on a certain person’s rights and interests.

The legal definition of personal data reflects the intention of the European lawmakers for a wide notion of personal data, in order to cover all information, which may be linked to an individual. It is not necessary that the information is true or proven to be considered “personal data”. Data protection rules, in fact, take into consideration the possibility that information may be incorrect and, consequently, provide for a right of the data subject to access and to challenge that information through appropriate remedies.

From what concerns the nature and the content of the information, the concept of personal data covers “objective” information (such as the presence of a certain substance in patient’s blood or heart rate) and “subjective” information, opinions or assessments about a person (especially in sectors such as banking, insurance or employment); it includes data providing any sort of information such as personal information considered to be “sensitive data” (this category of data will be examined in depth in the following paragraph)

---

65 Recital 26 GDPR. Emphasis added.
71 Article 8 Directive 95/46/EC; Article 9 GDPR.
and also more general kinds of information regarding the individual’s private and family life *stricto sensu* or whatever types of activity is undertaken by the individual (working relations or the economic or social behaviour).\(^{72}\) For example, *medical data about stroke survivors and the received treatment, medication or recovery, which is expected to be processed in STARR, can be considered personal data. Names, date and place of birth, sex, names of the parents, name of carers, address, photographs, and all the other information that may be collected during the interviews with stroke survivors and with doctors, can also be considered personal data. Also information about the emotional state of a stroke survivor (about the stroke, the therapy or everyday life) and about his/her behaviour, such as the reaction to therapy and adherence to recommended treatments, can be treated as personal data. Again, drug prescription information (e.g. drug identification number, drug name, strength or manufacturer, reasons for use, prescriber’s first and last name or phone number, etc.) can be considered as personal data about the physician who prescribes the drug, even if the patient is anonymous.*\(^{73}\)

In conclusion, the concept of personal data includes information available in *whatever form*, be it, for example, numerical, alphabetical, graphical, acoustic or photographic. It contains information kept on paper or stored in computer memory. Many types of data stored on or generated by a smart device are personal data such as contacts, unique device and customer identifiers, identity of the data subject and of the phone, credit card and payment data, phone call logs, SMS, browsing history, email, pictures and videos, location.\(^{74}\) These considerations should be taken into account by all STARR partners when developing the mobile app for stroke survivors.

**BIOMETRIC DATA**

Special mention should be made to biometric data such as fingerprints, vein patterns, voices, facial structure, behavioural characteristics such as way to talk or to walk, etc. Article 4 of the GDPR defines “biometric data” as «personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data».\(^{75}\) They are “biological properties, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability.”\(^{76}\)

The reason why we mention here this particular category of data is because it is understood that some of the partners in STARR are interested in developing technologies that may process it. ULUX, for instance, is considering developing a vision-based system (through the use of Kinect 2) in order to monitor motor activities and emotional state of stroke survivors. Regarding the monitoring of emotions of stroke survivors, ULUX intends to use a facial recognition system still to be defined. Since the details of this technology are not defined yet, further analysis of this technology can be undertaken at a later stage only. It is enough to mention for now that *making emotions analysis falls within the scope of the applicable EU data protection law and such a processing would have to comply with its requirements*. As mentioned before, data about facial structure of an individual is considered biometric data. Partners are also interested in gait measurements, but, again, the details

---


\(^{73}\) Ibid., p. 7.

\(^{74}\) Article 29 Data Protection Working Party, WP 202, Opinion 02/2013 on apps on smart devices, February 27, 2013, p. 8.

\(^{75}\) Article 4 (14) GDPR.

of the relevant technology are not defined yet. It is also not clear yet if other biometric technologies are going to be used in the STARR project in order to collect behavioural data of stroke survivors and data about cognitive activities of patients (language or memory).

Differently from Directive 95/46/EC, the GDPR now specifically lists biometric data (and genetic data\(^77\)) as **sensitive personal data**, which, by their nature, have enhanced protection under EU law.\(^78\) Biometric data are becoming increasingly important for identifying persons in the technological age and their potential impact on the privacy and the right to data protection of individuals is extremely high.\(^79\) A particularity of biometric data is that they can be considered both as content of the information about a specific person as well as an element to establish a link between one piece of information and the person. Thus, they can work as “identifiers.” As a consequence, because of their unique link to a specific person, biometric data may be used to identify the individual (DNA data, for example, allows unambiguous identification of a person).\(^80\)

**SPECIAL CATEGORIES OF PERSONAL DATA**

As mentioned before, under EU law there are special categories of personal data which, by their nature, when processed, may pose a higher risk to the data subjects; their misuse may be irreversible and could have more severe and long-term consequences on the individual’s fundamental rights, such as the right to privacy and non-discrimination.\(^81\) For this reason they need enhanced protection. On the definition of sensitive data, both the Convention 108 (Article 6), the Directive 95/46/EC (Article 8) and the GDPR (Article 9) name the following categories: personal data revealing racial or ethnic origin; personal data revealing political opinions, religious or philosophical beliefs or trade union membership; and personal data concerning health or sexual life or sexual orientation. The GDPR now specifically adds the processing of genetic data and biometric data for the purpose of uniquely identifying a natural person as processing of special categories of personal data.

The processing of these special categories of data, otherwise known as sensitive data, **may generally not be allowed**, except under very specific circumstances which are analysed in detail in the next Chapter. Since it is supposed that the majority of data that are going to be collected in the STARR project are health data of stroke survivors, this category of data is of extreme importance and, for this reason, it will be examined in depth below.

**HEALTH DATA**

Following the path of Directive 95/46/EC, the GDPR continues to qualify health data as a special category of data to which a higher level of data protection applies. Under the Regulation, “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.”\(^82\) “Health data” is a much broader term than “medical data”. Information such as the fact that a person has broken a leg or that is wearing glasses or contact lenses, data about a person’s intellectual and emotional capacity or about smoking and drinking habits, data

\(^77\) According to the Article 4 (13) GDPR, “genetic data” are defined as “personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question”.

\(^78\) Article 9 (1) GDPR.


\(^80\) Ibid, p. 30.

\(^81\) Article 29 Working Party, Advice paper on special categories of data (“sensitive data”), April 20, 2011, p. 4.

\(^82\) Article 4 (15) GDPR.
about the membership of an individual in a patient support group or support group with health-related objective, are all data concerning the health of an individual.\textsuperscript{83}

The European Group on Ethics in Science and New Technologies (EGE), in the \textit{Opinion No 13 Ethical Issues of Health Care in Information Society} defines “health data” as including “a wide range of information about an individual, which all touch upon an individual’s private life. A health biography could include not only basic medical data (a history of all medical diagnoses, diseases and medical interventions, medications prescribed, test results, including imaging, etc.) but could also include more sensitive data (on mental health, relevant to family history, behavioural patterns, sexual life, social and economic factors, etc.) and health care administrative data (admissions and discharge, data routine, operational data, insurance and financial transactional data, etc).”\textsuperscript{84}

The broad scope of the term “health data” is reflected in what the GDPR points out in recital 35:

«Personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental status of the data subject. This includes information about the natural person collected in the course of the registration for, or the provision of, health care services as referred to in Directive 2011/24/EU of the European Parliament and of the Council\textsuperscript{85} to that natural person; a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on, for example, a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other professional, a hospital, a medical device or an in vitro diagnostic test».\textsuperscript{86}

The term “disease risk”, mentioned above in Recital 35, refers to data concerning the potential future health status of a patient, e.g. risks of having a (secondary) stroke. Therefore, health data could also include information about a person’s obesity, alcohol or tobacco consumption, drug use, physical inactivity, diet, compliance with medication and/or therapy, high or low blood pressure, cholesterol, arterial fibrillation, hereditary or genetic predisposition and predictions of the health status of an individual, or any other information where there is a “scientifically proven or commonly perceived risk of disease in the future”.\textsuperscript{87} This may also include cases where a data controller uses any personal data (health data or not) with the purpose of identifying disease risks (such as, for example, investigating exercise habits or diet so as to test new correlations between certain lifestyle factors and diseases) and of preventing disease which \textit{de facto} is the primary objective of the STARR project. In STARR, for instance, devices analysing a stroke survivor’s blood, weight or physical activity, and apps measuring blood pressure or heart rate (regardless whether the testing is performed by medical professionals or by devices and apps freely available on the commercial market and irrespective whether these devices are marketed as medical devices or not), can be included in this category of data; the same situation occurs, for instance, if a patient is using a glucose metering app, connected object or a

\textsuperscript{83} Article 29 Working Party, ANNEX - health data in apps and devices, February 5, 2015, p. 2.


\textsuperscript{86} Recital 35 GDPR. Emphasis added.

\textsuperscript{87} Ibid. Emphasis added.
wearable that warns if his/her glucose level is too high and advises the stroke survivor to take action, which may be performed in STARR.\textsuperscript{88}

In summary, all the STARR partners should be aware that personal data are health data when:

i) data are clearly \textit{medical data} (such as data on consumption of medicinal products or any other data contained in the medical documentation concerning the treatment of a patient, including administrative data);

ii) data are \textit{raw sensor data} that can be used in itself or in combination with other data to draw a conclusion about the actual health status or health risk of a person;

iii) conclusions are drawn about a person's health status or health risk.\textsuperscript{89}

Both the sharing and the linkage of such category of data may pose a high risk to the protection of the privacy of the individual whose data are involved. When data are shared they may be lost or stolen during the transfer or the data recipient may not provide sufficient protection to keep the data confidential. When data are linked, the combined dataset provides more information about the patient; thus, the resulting linked data could cause more harm to data subjects if it were lost, stolen or otherwise misused. A misuse of personal health information can have severe consequences for the patient such as financial and psychosocial harms; \textit{financial harms} can result from discrimination in health insurance or employment; \textit{psychosocial harms} could include embarrassment and loss of reputation, resulting in isolation and stress. Disclosures of personal data can also increase individual’s risk of experiencing identity theft, and, also, the risk of a loss of confidence in the health care system.\textsuperscript{90} Due to the wide range of personal data that may fall into the category of health-related data, this category represents one of the most complex areas of sensitive data.

LOCATION AND TRAFFIC DATA

According to Article 2 of Directive 2009/136/EC, which amends the e-Privacy Directive, “location data” is defined as “any data processed in an electronic communications network or by an electronic communications service, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service.”\textsuperscript{91} It is not known yet whether STARR partners are interested in processing stroke survivors’ location. However, since apps are going to be used in the project, this opens the possibility of collecting this data and thus the partners should be aware that if they process such data, they should comply with the law. Apps, in fact, are able to collect large quantities of data from a device (e.g. personal data stored on the device by the user and data from different sensors, including location).\textsuperscript{92} All kinds of information can be connected to a geographic location, such as health data or behavioural data.\textsuperscript{93}


\textsuperscript{89} “Irrespective of whether these conclusions are accurate or inaccurate, legitimate or illegitimate, or otherwise adequate or inadequate”, Article 29 Working Party, \textit{ANNEX - health data in apps and devices}, February 5, p. 5; Article 29 Working Party, \textit{Working Document on the processing of personal data relating to health in electronic health records (EHR)}, WP 131, February 15, 2007.

\textsuperscript{90} \textit{OECD} Health Policy Studies, \textit{Health Data Governance: Privacy, monitoring and research}, 2015, p. 22-23.

\textsuperscript{91} Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, J L 337, December 18, 2009, p. 11–36; “Location data may refer to the latitude, longitude and altitude of the user’s terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded”, Recital 14 Directive 2009/136/EC.

\textsuperscript{92} Article 29 Data Protection Working Party, WP 202, Opinion 02/2013 on apps on smart devices, February 27, 2013, p. 2.

\textsuperscript{93} Article 29 Data Protection Working Party, WP 185, Opinion 13/2011 on Geolocation services on smart mobile devices, May 16, 2011, p. 3.
“Traffic data” is “any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof.” 94 Traffic data may consist, for instance, of data referring to the routing, duration, time or volume of a communication, to the protocol used, to the location of the terminal equipment of the sender or recipient, to the network on which the communication originates or terminates, to the beginning, end or duration of a connection. They may also consist of the format in which the communication is conveyed by the network. 95 The same considerations made above regarding location data are valid here. It is not known yet if the STARR partners are interested or will be interested in processing traffic data through, for instance, an app installed on the mobile phone of a stroke survivor. Thus, when more information on this issue will be available, it will be possible to properly guide the partners in complying with the European data protection standards.

ANONYMISED AND PSEUDONYMISED DATA

European data protection law recognizes the concepts of anonymous and pseudonymous data. Anonymous data means information, which does not relate to an identified or identifiable natural person. Anonymising, in fact, means altering a set of personal data in order to eliminate all the identifying elements in such a manner that the data subject is not or no longer identifiable. Where data have been successfully anonymised, they are no longer personal data and the principles of data protection should therefore not apply to the processing of anonymous information, including for statistical or research purposes. 96 The assessment of whether the data allow identification of an individual, and whether the information can be considered as anonymous or not depends on the circumstances, and a case-by-case analysis should be carried out (an example could be in the case of statistical information, where despite the fact that the information may be presented as aggregated data, the original sample is not sufficiently large and other pieces of information may enable the identification of the person). 97 It is not known yet if in STARR partners will work with anonymous data but it is recommended in order to highly diminish the risks of stroke survivors’ identification.

Pseudonymous data are subject to data protection law, since they could be tied to an individual and, for this reason, should be considered to be information on an identifiable natural person. 98 “Pseudonymisation” means, in fact, replacing the name and other identifiable characteristics by a symbol in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information. That additional information is kept separately and is subject to technical and organisational measures in order to make identification of a person impossible or extremely difficult. 99 The aim of pseudonymisation is to be able to collect additional data relating to the same individual without having to know his/her identity (this is particular relevant in the context of research and statistics, like in STARR). 100 Pseudonymisation is achieved, for instance, by encryption of the identifiers; for everyone who is not in possession of the decryption key, pseudonymised data can be identifiable with difficulty. However, the link to an identity still exists in the form of the pseudonym and of the decryption key and, for those who are entitled to use the decryption key, re-identification is easily possible. The use of encryption keys by unauthorised persons must be particularly guarded against, that is why methods of pseudonymisation are so important since they affect the effectiveness of data

94 Article 2 Directive 2009/136/EC.
95 Recital 15 Directive 2009/136/EC.
96 Recital 26 GDPR.
98 Recital 26 GDPR.
protection; \(^{101}\) in fact, they can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations.\(^{102}\)

«Personal data with encrypted identifiers are used in many contexts as a means to keep secret the identity of persons. This is particularly useful where data controllers need to ensure that they are dealing with the same data subjects but do not require, or ought not to have, the data subjects’ real identities. This is the case, for example, where a researcher studies the course of a disease with patients, whose identity is known only to the hospital where they are treated and from which the researcher obtains the pseudonymised case histories. Pseudonymisation is therefore a strong link in the armoury of privacy-enhancing technology. It can function as an important element when implementing privacy by design.\(^{103}\)

Thus, where anonymisation is not possible, it is recommended the application of effective pseudonymisation methods to personal data to the STARR partners as a means to reduce the risks for the STARR data subjects.

DATA PROCESSING

Data protection law applies only when personal data are processed. Article 4 GDPR, following Article 2 of the Directive 95/46/EC, defines “processing” as “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”.\(^{104}\) It can be noticed that the definition of processing is extremely broad as to include virtually any operation that can be performed on personal data.\(^{105}\) In STARR the following activities are an example of processing: the collection of data, its mere storage, sharing with partners and others, dissemination, analysis, etc.

CONTROLLERS AND PROCESSORS

Under EU law, two are the main actors who process personal data: “data controllers” and “data processors”. Both have a legal responsibility for complying with the respective obligations under data protection law. Therefore, only those who can be held responsible under the applicable law can assume these positions.\(^{106}\) The distinction between “controller” and “processor” mostly serves to distinguish between those involved that are responsible as controller(s) and those that are only acting on their behalf, i.e. processors.\(^{107}\)

---


\(^{102}\) Recital 28 GDPR.


\(^{104}\) Article 4 (2) GDPR; similarly, see also Article 2 (b) Directive 95/46/EC, and Article 2 (c) Convention 108.

\(^{105}\) Placing information about individuals on an internet site, for instance, constitutes processing of personal data. In fact, the CJEU, in the *Bodil Lindqvist* case, held that: “the act of referring, on an internet page, to various persons and identifying them by name or by other means, for instance by giving their telephone number or information regarding their working conditions or hobbies, constitutes the ‘processing of personal data wholly or partly by automatic means’ within the meaning of Article 3 (1) of Directive 95/46.”, CJEU, C-101/01, *Bodil Lindqvist*, November 6, 2003, para. 27.


A data controller is defined as a “natural or legal person, public authority, agency or other body which, alone or jointly with others determines the purposes and means of the processing of personal data”. The role of the concept of controller is to allocate responsibility, determining who shall be responsible for compliance with data protection rules, and how data subjects can exercise their rights in practice. The one liable for a data protection breach is always the controller, i.e. the legal person or the natural person as formally identified according to the criteria of the Directive 95/46/EC and the GDPR. The concept is also an essential element in determining which national law is applicable to a processing operation or set of processing operations. In the private sector, a controller is usually a natural or legal person; in the public sector, it is usually an authority. Other entities, such as bodies or institutions without legal personality, can be controllers or processors only where special legal provisions so provide.  

It is possible to have multiple controllers (called “joint controllers”) for the same data set; they jointly determine the purposes and means of processing. Joint controllers shall, in a transparent manner, determine their respective responsibilities for compliance with the obligations under the law. In such complex data processing environments, in which different controllers play a role in processing personal data, compliance with data protection rules and responsibilities for possible breach of these rules should be clearly allocated, in order to avoid that the protection of personal data is reduced. In these cases, more than ever, it is paramount that a clear information notice is given to the data subjects, explaining the various stages and actors of the processing. In this context, the participation of the parties to the joint determination may take different forms and does not need to be equally shared. Rules on how to exercise joint responsibilities should be determined in principle by controllers. However, factual circumstances should be considered also in this case, with a view to assessing whether the arrangements reflect the reality of the underlying data processing.  

Therefore, the role of the controller is crucial and particularly relevant when it comes to determining liability and imposing sanctions. Even if liability and sanctions will vary depending on the Member States, since they are imposed according to national laws, the need to clearly identify the natural or legal person responsible for breaches of data protection law is beyond doubt an essential pre-condition for the effective application of the EU law. In STARR, the “controller(s)” is/are not yet defined. Concerning the mobile app that is planned to be created in STARR, for instance, this process of identification of the controller(s) is of particular importance due to the high degree of fragmentation between the many players in the app development landscape; thus, a definition of different roles should be prospected with extreme clarity and in time. Whenever a partner involved in the development, distribution and operation of the app is deemed to be a controller, such partner is responsible, alone or jointly with others, for ensuring compliance with all the requirements set forth under EU law.

---

108 Article 4 (7) GDPR; Article 2 (d), Directive 95/46/EC. Emphasis added.
110 Data processing in a business environment is often performed by corporate entities with complex structures, many of which may have access to or control, wholly or in part, over personal data. In such cases, it can be extremely difficult to establish whether or not a particular entity “determines the purposes and means of the processing of personal data” as written in Article 4 GDPR. If a natural person working within a company or public body uses data for his or her own purposes, outside the activities of the company, this person shall be considered as a de facto controller and will be liable as such; See KUNER C., European Data Protection Law, Oxford University Press, 2007, p. 69-73; Article 29 Working Party (2010), Opinion 1/2010 on the concepts of ‘controller’ and ‘processor’, WP 169, Brussels, February 16, 2010, p. 17.
112 Article 4 (7) GDPR.
113 Article 26 GDPR.
115 Ibid.
In STARR every data processing operation has to have a designated controller, which is to be decided amongst partners on a case-by-case basis. It is assumed that for the interviews with stroke survivors and doctors each partner is a controller, however, for the platform and the tests with it partner(s) which will be the controller(s) still need to be defined in the coming months.

A data processor is defined as a “natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.” Processors are organisations that act as service providers and process data only because another organisation (a controller) has engaged them to do so. Thus, the existence of a processor depends on a decision taken by the controller, who can decide either to process data within his organization, for example through staff authorized to process data under his direct authority, or to delegate all or part of the processing activities to an external organization. Therefore, the processor is a separate legal entity with respect to the controller and it processes personal data on behalf of the latter. The processor may have a reduced role, with activities limited to very specific task or context or quite general; processors, in fact, are supposed only to process personal data as directed by the controller. The latter decides why and how data shall be processed. As mentioned in the Convention 108, a controller decides also which categories of personal data should be stored.

Most data protection obligations must be met by the controller and, in most cases, data controllers (rather than data processors) are liable for data protection violations. However, the concept of “processor” plays an important role in the context of confidentiality and security of processing, as it serves to identify the responsibilities of those who are more closely involved in the processing of personal data, either under direct authority of the controller or elsewhere on his behalf. In STARR, the identification of which partners could be “the processors” for a certain data processing operation is not yet defined, as for the controllers. The same considerations made above are valid here; however, having processors is not obligatory. It will have to be determined whether STARR partners will undertake this role for particular data processing operations.

THIRD PARTIES AND RECIPIENTS

A “third party” is a “natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data”. A ‘third party’ is legally different from the controller; thus, disclosing data to a third party will always need a specific legal basis.

“Recipient” is a broader term than “third party”. It means a “natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not”.

The difference between these two categories of persons/entities lies mainly in their relationship to the controller and, consequently, in their authorisation to access personal data held by the controller. A recipient

---

118 Article 2 (e) Directive 95/46/EC.
120 Article 2 (d) Convention 108.
121 Article 23 Directive 95/46/EC; Article 24 GDPR.
123 Article 4 (10) GDPR.
124 Article 4 (9) GDPR.
may either be a person outside the controller or processor (this would then be a third party) or someone inside the controller or processor, such as an employee or another division within the same company or authority.\(^{125}\)

The distinction between recipients and third parties is important only because of the conditions for lawful disclosure of data.

In STARR, the identification of third parties and recipients is not yet defined and it is not certain there will be any third parties/recipients in the first place. Again, this process of identification is of particular importance especially in relation to the development of the mobile app for stroke survivors, due to the high degree of fragmentation between the many players in the app development landscape. We do not know yet whether this is relevant for STARR, but we inform the partners just in case they engage such third parties in their processing operations.

**CONSENT**

“Consent” of the data subject means “any freely given, specific, informed and unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her”.\(^{126}\) **Consent is one of the legal grounds for data processing and it looks likely to be relied on in STARR.** EU law sets out four criteria for consent to be legally valid, which aim to guarantee that data subjects truly meant to agree to the use of their data.

First, consent must be an **unambiguous indication** (such as by a written statement, including by electronic means, or an oral statement)\(^ {127}\) of the data subject’s wishes and there should be no reasonable doubt that the data subject wanted to communicate his or her agreement to allow processing of his or her data. Deducing consent from mere inactivity, or from silence or pre-ticked boxes, is not capable of delivering unambiguous consent. **Where data to be processed are sensitive (as it may happen often in STARR) explicit consent is mandatory and must be unambiguous.**\(^ {128}\)

Secondly, consent must be **freely given**, this means that the data subject must have been under no pressure when consenting. The existence of free consent is valid only “if the data subject is able to exercise a real choice and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent”.\(^ {129}\)

Thirdly, consent must be **informed**. Thus, the data subject must have sufficient information about the object and consequences of consenting before taking his or her decision. Whether or not the information given is sufficient can be decided only on a case-by case basis. **Usually, informed consent includes a precise and easily understandable description of the subject matter requiring consent and, additionally, it outlines the consequences of consenting or not consenting.** In STARR, for example, this is particularly important since the


\(^{126}\) Article 4 (11) GDPR.

\(^{127}\) This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject’s acceptance of the proposed processing of his or her personal data”, Recital 32 GDPR.


\(^{129}\) See Article 29 Working Party, *Opinion 15/2011 on the notion of consent, WP 187*, Brussels, July 13, 2011, p. 12; according to Recital 43 GDPR, “Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance”.
combination of sensors in wearables, everyday objects and environment, planned in STARR, gradually blending into the everyday life of the patients, may result in an invisible and unclear collection of personal data perceived by the stroke survivors. Thus, a clear and precise description of the consequences of consenting and of the activities planned by the partners should be presented. Moreover, the language used for information should be adapted to the foreseeable addressees of the information.130 This is particularly relevant for the STARR project, in which the necessity of obtaining the consent of stroke survivors for the collection of their data may clash with the delicacy of their conditions. In the preliminary research stage, interviews of stroke survivors are performed; on a later stage, they are requested to test and interact with the developed STARR solution. Some of the stroke survivors may have some permanent cognitive and language impairments (i.e. difficulties in learning, reading, or memory problems). The patients interviewed in France by CEA and HOPALE, for example, had mainly severe strokes, as they reported. Additionally, most of the stroke survivors are elderly persons; therefore the risk of misunderstanding is likely to be high and all the STARR partners should be extremely careful about meeting the requirements of patients and adapting their requests and their consent forms to the specific case. This means that controllers in STARR have to carefully consider the wording in consent forms and the means by which consent is achieved.131

Information must also be easily available to the patients. Accessibility and visibility of the information are important elements. In an online environment, layered information notices may be a good solution, as, in addition to a concise version of information, a more extensive version can also be accessed by the data subject.132

Finally, consent must be specific, its scope reasonably concrete. This is highly connected with the quality of information given about the object of consent. According to the recital 32 GDPR, “consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them.”133 Consent must be asked again if processing operations are to be added or changed in a way which could not reasonably have been foreseen when the initial consent was given by the data subject.134 In STARR, for instance, when partners ask participants for consent, they may not ask for a general consent for research activities but they should specify what the research purposes are as much as possible and stick to these specific purposes.

The GDPR recognises that, in a research context as in STARR, data subjects should be allowed to give their consent to certain areas of scientific research when in keeping with recognised ethical standards for scientific research.135 Stroke survivors should, therefore, have the opportunity to give their consent only to certain areas of research or parts of the research project to the extent allowed by the intended purpose.136

Only if all of these requirements are fulfilled will consent be valid in the sense of the data protection law. Additional requirements under civil law for valid consent, such as legal capacity, naturally apply also in the context of data protection, as such requirements are fundamental legal prerequisites. Invalid consent of persons who do not have legal capacity will result in the absence of a legal basis for processing data about such persons, unless another legal ground is found. It is important to be aware that consent does not legitimise excessive or

131 Hogan Lovells, Chronicle of data protection, The Final GDPR Text and What It Will Mean for Health Data, January 20, 2016.
132 Ibid.
133 Recital 32 GDPR. Emphasis added.
135 Hogan Lovells, Chronicle of data protection, The Final GDPR Text and What It Will Mean for Health Data, January 20, 2016; Article 7 GDPR.
136 Recital 33 GDPR.
disproportionate data processing, which means that even when consent is given, all the other legal principles have to complied with.

The requirement under the GDPR for obtaining valid consent is similar to the requirement under the Directive 95/46/EC, except for the fact that now the GDPR places the **onus on the controller** to demonstrate that consent to the processing operation was given. “In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given”. The controller should provide a pre-formulated declaration of consent “in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms”. Since the consent must be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing; for the consent to be freely given, the data subject has to have genuine or free choice or he/she has to be able to refuse or withdraw consent without detriment. Therefore, during all the different phases of the STARR project, according to the Article 7 GDPR, partners involved in the collection of data must obtain the consent (of patients, medical specialists and carers) “in a manner distinguishable from other matters, in an easily accessible form and using clear and plain language”, and participants must be able to withdraw their consent easily. If the consent is to be given by the data subject following a request by electronic means, the request must be “clear, concise and not unnecessarily disruptive to the use of the service for which it is provided”.

Therefore, for STARR this means that before data are collected, the controller should give an info notice to the data subjects, explaining the data operations to be performed on the personal data, should give the chance to the person not to give consent, (i.e. our subjects should not be forced to give consent), and when patients give consent for one set of operations, this does not mean that STARR partners can process the data for other purposes (unless they find another legal basis).

### CHAPTER 3: Legal grounds for processing

**PROCESSING OF PERSONAL DATA**

According to Article 7 Directive 95/46/EC and Article 6 of the new GDPR, processing of personal data is lawful only when at least one of the following criteria applies: a) when the data subject has given consent to the processing of his or her personal data for one or more specific purposes; b) when processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; c) when processing is necessary for compliance with a legal obligation to which the controller is subject; d) when processing is necessary in order to protect the vital interests of the data subject or of another natural person; e) when processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; f) and finally when processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subjects.

---

137 Recital 42 GDPR. Emphasis added.
138 Ibid.
139 Ibid.
140 Article 7 GDPR.
141 Recital 32 GDPR.
subject which require protection of personal data, in particular where the data subject is a child.\textsuperscript{142} The most likely legal basis for STARR is consent. However, if consent is not possible, one or more of the other legal bases have to be considered.

Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent, the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia: a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing; b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller; c) the nature of the personal data; d) the possible consequences of the intended further processing for data subjects; e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.\textsuperscript{143} Therefore, GDPR enables re-use of data, which is a breach of the purpose limitation principle. \textbf{Thus, we would like to recommend partners to respect the original purpose of data processing for which they first collected the data.}

**PROCESSING OF SENSITIVE DATA**

Processing of sensitive data, among which health data and biometric data, shall be prohibited except under certain clearly-defined circumstances such as for example: when the data subject has given his/her explicit consent for one or more specified purposes; when processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law; when processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; when processing relates to personal data which are manifestly made public by the data subject; when processing is necessary for reasons of substantial public interest; when processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services; when processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices; when processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.\textsuperscript{144}

In STARR, if the data controller collects data, for example, through an app or a device, and it concerns apps with a medical purpose (e.g. apps through which stroke survivors can share data on symptoms and compare which treatments work best for them; apps that contain reminders to take medication; personal data tracking, science, and collaboration apps to help both medical research and individuals to make healthier choices), or where health data can be reasonably inferred from the data tracked by the application (e.g. apps to track food and exercise; body fat monitor and scale used for the same objective; apps that allow stroke survivors to find correlations between their individual data streams, like how their diet correlates with their sleep and mood), the data controller needs to be able to rely on a derogation from the general prohibition in Article 8 of the Data Protection Directive and Article 9 GDPR.\textsuperscript{145} Thus, partners collecting and using health data

\textsuperscript{142} Article 7 Directive 95/46/EC; Article 6 (1) GDPR.
\textsuperscript{143} Article 6 (4) GDPR.
\textsuperscript{144} Article 9 (2) GDPR.
\textsuperscript{145} Article 29 Working Party, \textit{ANNEX - health data in apps and devices}, February 5, 2015, p. 5.
will need to be able to rely on a lawful ground – both for collecting personal data and sensitive personal data. The lawful grounds available in the GDPR broadly reflect the grounds under the Directive 95/46/EC.

Again, the most likely legal basis for STARR is consent, especially with regard to apps and devices that allow for the collection of health data. However, if consent is not possible, one or more of the other legal bases have to be considered. It is important to underline that “explicit consent” means opt-in consent (i.e. some affirmative act by the data subject which clearly indicates his assent to the processing); opt-out consent will not be sufficient. For STARR this means that when sensitive data is collected, the data subjects should, e.g. sign a paper, or click on button to agree. Consent is not required if the processing is necessary in the public interest for public health reasons (the “public health” ground), or if the controller(s) can argue that the processing is necessary for scientific research (in accordance with Article 89 (1), further discussed in the next paragraph), but only if based on Union or Member State law (“which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy”, in the first case, and, additionally, “which shall be proportionate to the aim pursued and respect the essence of the right to data protection” in the second case). Member States may also “maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health”.

Special measures are needed to protect health data, the processing of which is associated with serious privacy infringements, against abuse (e.g. the commercial use of patient data). A particular problem relates to the processing of health data for insurance purposes. On March 2001, the French DPA (CNIL) published a recommendation dedicated to healthcare matters. The recommendation sets out the following principles: healthcare data related to an identified or identifiable person may not be bought or sold, even if the individuals to whom these data refer have given their consent; navigational data gathered by health-related websites when an individual visits become sensitive data if they can be linked to other information on health-related issues collected directly from the individual (for example, because the individual filled out a health-related questionnaire). This information should therefore be given the same treatment as health-related information. Such information cannot be given to insurance companies, banks or employers. Thus, we would like to recommend the partners not to use sensitive data for further purposes, e.g. insurance or marketing (this goes both for the data used for research and later when they really offer the app in real life). In fact, these purposes go beyond the project’s goals.

PROCESSING OF PERSONAL DATA FOR RESEARCH PURPOSES

147 In the definition of “public health” provided by the GDPR in recital 54, are included “all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality”. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.
148 Article 9 (g) GDPR.
149 Article 9 (j) GDPR.
150 Article 9 (g) GDPR.
151 Article 9 (j) GDPR.
152 Article 9 (g) GDPR.
153 Article 4 (6) GDPR.
154 Article 29 Working Party, Advice paper on special categories of data (“sensitive data”), April 2011, p. 8-10.
155 Délibération n. 01-011 du 08 mars 2001, Délibération portant adoption d’une recommandation sur les sites de santé destinés au public.
In their judgments, both the ECtHR and the CJEU have stated that a balancing exercise with other rights is necessary when applying and interpreting Article 8 of ECHR and Article 7 and 8 of the CFREU. In relation to science, for example, European data protection law is aware of the special value of science to society. Therefore, the general restrictions for the use of personal data are diminished. The GDPR provides a qualified compliance framework regarding the processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, under Article 89. The appropriate safeguards for the rights and freedoms of the data subject include technical and organisational measures in order to ensure, in particular, the principle of data minimization (i.e. processing the minimal amount of personal data). Pseudonymisation is given as an example of the measures that could be used.

In STARR, partners may aim at processing personal and sensitive data for scientific research; if so, they must implement safeguards provided by Article 89 GDPR. It is strongly recommended a clear identification of the purpose(s) of the processing(s) for scientific research, although it is known that it is often not possible to fully identify the purpose of such processing at the time of data collection.

**PROCESSING OF LOCATION AND TRAFFIC DATA**

Location and traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, may only be processed when they are made anonymous, or with the consent of the users/subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users/subscribers, before obtaining their consent, of the type of location data or traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party. Users/subscribers shall be given the possibility to withdraw their consent at any time. Traffic data “must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication”.

While many provisions of the Directive 2002/58/EC apply only to providers of publicly available electronic communication services and providers of public communication networks, Article 5(3) of Directive 2009/136/EC applies to every entity (such as the mobile app planned to be created in STARR) that places on or reads information from smart devices, without regard to its nature. The above-mentioned article prescribes that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber/user is only allowed on condition that the subscriber/user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter
alita about the purposes of the processing, and having been offered the **right to refuse** such processing by the data controller.\textsuperscript{161}

### OBLIGATIONS OF THE CONTROLLER

In STARR, the identified controller(s) shall, **both at the time of the determination of the means for processing and at the time of the processing itself**, implement “appropriate technical and organisational measures” (such as pseudonymisation) to ensure and to be able to demonstrate that processing of data is performed in accordance with the law, taking into account the nature, scope, context and purposes of processing as well as the risks for patients.\textsuperscript{162} Those measures shall be reviewed and updated where necessary and shall include, where proportionate, the “implementation of appropriate data protection policies by the controller”.\textsuperscript{163} Moreover, the controller shall implement those measures “in an effective manner and integrate the necessary safeguards into the processing”,\textsuperscript{164} in order to protect the rights of stroke survivors.

Appropriate measures will ensure that, by default, “only personal data which are necessary for each specific purpose of the processing are processed.”\textsuperscript{165} This applies “to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility”.\textsuperscript{166} Such measures should especially ensure that by default personal data are not made accessible without the individual’s intervention to an indefinite number of persons. An approved certification mechanism may also be used.\textsuperscript{167} Therefore, in STARR, the controller for each data processing operation should adopt internal policies and implement measures, which meet in particular the **principles of data protection by design and data protection by default**, as explained above.\textsuperscript{168}

The new GDPR aims to create incentives to apply pseudonymisation when processing personal data. As stated in recital 29 of the regulation, “measures of pseudonymisation, whilst allowing general analysis, should be possible **within the same controller** when that controller has taken technical and organisational measures” and that “additional information for attributing the personal data to a specific data subject is kept separately”.\textsuperscript{169} Moreover, “the controller processing the personal data should indicate the authorised persons within the same controller”.\textsuperscript{170}

If the power to determine the means of processing is delegated to a processor, the controller must nonetheless be able to interfere with the decisions of the processor regarding the means of processing. Overall responsibility still lies with the controller, who must supervise the processors to ensure that their decisions comply with data protection law.\textsuperscript{171} Under Article 28 GDPR, **where processing is to be carried out on behalf of a controller**, the

---

\textsuperscript{161}Article 5 (3) Directive 2009/136/EC.
\textsuperscript{162}Article 24 (1) GDPR.
\textsuperscript{163}Article 24 (1) (2) GDPR.
\textsuperscript{164}Article 25 (1) GDPR. Emphasis added.
\textsuperscript{165}Article 25 (2) GDPR.
\textsuperscript{166}Ibid.
\textsuperscript{167}Ibid.
\textsuperscript{168}Ibid.
\textsuperscript{169}Recital 29 GDPR.
\textsuperscript{170}Ibid.
controller shall use only processors that provides sufficient guarantees to implement appropriate technical and organisational measures. The processor cannot involve another processor without a prior specific or general written authorisation of the controller. Furthermore, “processing by a processor shall be governed by a contract or other legal act under Union or Member State law that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.” Thus, if a controller delegates the processing to a processor, usually a written agreement should be signed between them, in which the processor commits, for instance, to act only under the instructions of the controller and to maintain proper security and confidentiality measures.

The processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller. Each controller and, where applicable, the controller’s representative, shall maintain a record of processing activities under its responsibility. The same is provided for the processor and, where applicable, for the processor’s representative. The records shall be in writing, including in electronic form. Furthermore, the controller or the processor shall make the record available to the supervisory authority on request and cooperate.

CHAPTER 4: Key principles of personal data processing

The processing of personal data must comply with the general data protection principles established by legislation, such as Article 5 Convention 108, Article 6 Directive 95/46/EC and Article 5 GDPR. The data protection principles are revised with the new GDPR but are broadly similar to the principles set out in Directive 95/46/EC: fairness, lawfulness and transparency; purpose limitation; data minimisation; data accuracy; storage limitation; security, integrity and confidentiality. The novelty that the GDPR introduces is the accountability principle. In the following paragraphs an analysis of these principles is provided in the context of STARR.

Fair, lawful and transparent processing

The first principles are lawfulness, fairness and transparency: “personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.” In STARR, it means that partners must have legitimate grounds for collecting and using personal data; they should not use them in ways that have unjustified negative effects on individuals concerned and they have to be transparent about how they intend to use the data. Partners also have to guarantee that they will not misuse the data.

The principles of transparency and fairness are inseparably connected to the legal ground of consent. As it has been already observed in Chapter 2, in STARR, the data controller must clearly inform stroke survivors whether the data, for instance, are protected by any medical secrecy rules, or not, or whether the data will be combined with other data stored on a device or collected from other sources. Moreover, clear examples of the consequences of such combination of data, what the purposes are of further processing and to what third

172 Article 28 (1) GDPR.
173 Article 28 (2) GDPR.
174 Article 28 (3) GDPR.
175 Article 28 (3) (a) (b) GDPR.
176 Article 29 GDPR.
177 Article 30 (1) GDPR.
178 Article 30 (2) (3), GDPR.
179 Article 30 (4) GDPR; Article 31 GDPR.
180 Article 5 (1) (a) GDPR.
parties the data may be transferred must be provided. Such information must be made available in a clear and easily accessible manner before stroke survivors decide on installing apps or buying devices (also before downloading the app). Therefore, assessing whether information is being processed fairly and in a transparent manner depends partly on how it is obtained. In particular, if anyone is deceived or misled when the data is obtained, then this is unlikely to be fair.

**Purpose limitation**

The second principle is purpose limitation: “personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.” Purpose limitation is a key provision that deserves careful consideration and it is a prerequisite for other data quality requirements.

The concept has two main building blocks, the purpose specification (“personal data shall be collected for specified, explicit and legitimate purposes”) and the compatible use (“and not further processed in a manner that is incompatible with those purposes”). They aim to protect the data subject by setting limits on how controllers are able to use their data and so they contribute to transparency, predictability and legal certainty and reinforce the fairness of the processing.

For STARR this means that partners involved in processing should prevent the use of individuals’ personal data in a way that they might find inappropriate. The controller(s) must therefore carefully consider what purpose(s) the personal data will be used for, and must not collect personal data, which are not necessary, adequate or relevant for the purpose(s) which are intended to be served. The purpose of processing data must be visibly defined before processing is started. Under EU law, this must be done either by notification to the appropriate supervisory authority or, at least, by internal documentation which must be made available by the controller for inspection by the supervisory authority and access by the data subject.

The purpose specification will determine the relevant data to be collected, retention period and all other key aspects of the processing. The purpose must be specified, sufficiently defined to enable the implementation of any necessary data protection safeguards, and to delimit the scope of processing operation. A purpose that is too vague or general, without details, or not presented in a user-friendly manner, usually does not meet the criteria of being “specific”. Then, purpose must be explicit, that is, sufficiently unambiguous and clearly expressed; it should leave no doubt or difficulty in understanding. Finally, purpose must be legitimate, the processing based on at least one of the legal grounds provided for in Article 7 Directive 95/46/EC and Article 6 GDPR. Legitimacy also extends to other areas of law and must be interpreted within the context of the processing.

Personal data may be collected for more than one purpose. In some cases, these purposes, while distinct, are nevertheless related to some degree. In this situation, the concept of an overall purpose, under whose umbrella a number of separate processing operations take place, may be useful. However, controller(s) should avoid

---

182 Article 5 (1) (b) GDPR.
183 Article 29 Working Party, WP 203, Opinion 03/2013 on purpose limitation, April 2, 2013, p. 11.
186 Ibid.
identifying only one broad purpose for further processing activities that are in fact only barely related to the actual initial purpose. When the purpose is unrelated, in fact, each separate purpose should be specified in enough detail to be able to assess whether collection of personal data for this purpose comply with the law. If personal data are processed for several purposes, all requirements of Article 6 Directive 95/46/EC and Article 5 GDPR apply to each purpose separately. Of course, a case-by-case analysis is required.\(^{187}\)

The notion of compatible use offers some degree of flexibility for data controller(s). It may happen, in fact, that when initially specifying the purpose, neither the controller nor the data subject thought additional purposes would be necessary, although it subsequently transpired that the data could indeed be very useful for other things.\(^{188}\) Further processing is authorised as long as it is not incompatible with the initial purpose(s); compatibility needs to be assessed on a case-by-case basis. Any processing following collection, whether for the purposes initially specified or for any additional purposes, must be considered “further processing” and must thus meet the requirement of compatibility. In order to perform a substantive compatibility assessment, account should be taken of: a) the relationship between the purposes for which the data have been collected and the purposes of further processing, namely the greater the distance between the purpose of collection and the purposes of further processing, the more problematic this would be for the compatibility assessment; b) the context in which the data have been collected and the reasonable expectations of the data subjects as to their further use; c) the nature of the data and the impact of the further processing on the data subjects; d) the safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects.\(^{189}\)

In general, the more sensitive the information involved, as it may often happen in STARR with the collection of health data or biometric data, the narrower the scope for compatible use would be. When the processing involves health data, for instance, further processing for different purposes (outside the professional health care domain) is strictly limited. The data controller must define clear compatible and legitimate purposes of the data processing. This is an essential guarantee against the risks of misuse of the data.\(^{190}\) Additionally, transfer of data to third parties is a new purpose needing an additional legal basis.\(^{191}\) There are some types of processing, where it is not obvious at first sight whether or not the processing of these data should qualify as the processing of health data. This is especially the case where the data are processed for additional purposes and/or combined with other data or transferred to third parties. These types of data processing may create risks, including the risk of unfair treatment based on data about a person’s assumed or actual health status. If data are health data, but mistakenly treated as “ordinary” personal data, there is a risk that the high level of protection deemed necessary by the European legislator is undermined. This risk specifically applies to further processing of such data for profiling and marketing purposes, given that the key business model of most apps is based on advertising.\(^{192}\) In STARR, it is strongly recommended to avoid processing stroke survivors’ data for incompatible purposes, i.e. those not related to research such as profiling and marketing purposes.

\(^{187}\) Ibid., p. 16.
\(^{188}\) Ibid., p. 21.
\(^{189}\) Ibid., p. 21-27.
\(^{191}\) Ibid.
\(^{192}\) Article 29 Working Party, ANNEX - health data in apps and devices, February 5, 2015, p. 3.
The specification made regarding the “further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes”\textsuperscript{193} may be seen as a specification of the general rule.\textsuperscript{194}

Data minimisation

The third principle is \textit{data minimisation}: “personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.”\textsuperscript{195} This means that \textbf{in STARR a data controller should limit the collection of personal information to what is directly relevant and necessary to accomplish a specified purpose}. Controller(s) should also retain the data only for as long as is necessary to 
\textbf{fulfil that purpose}. In other words, \textit{data controllers should collect only the personal data they really need, and should keep it only for as long as they need it}.

In STARR, for example, \textbf{no data on the medical and emotional state of the future app users, which would not be necessary for the treatment, should be collected}. Thus, the STARR partners will have to clearly document the categories of data they need for the purposes of the project. The data minimization principle is necessary for carrying out the research and also designing the application in a way it will ensure that the minimum data is collected, stored and communicated on stroke survivors. Controller(s) are encouraged to apply proper anonymization techniques\textsuperscript{196} and other security measures, including privacy by design.\textsuperscript{197}

Data accuracy

The fourth principle is \textit{data accuracy}: “personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay”.\textsuperscript{198} The obligation to ensure accuracy must be seen in the context of the purpose of data processing. In \textbf{STARR, regular checking of the accuracy of data, including updating, is an absolute necessity because of the potential damage which might be caused to the stroke survivor’s heath if data were to remain inaccurate}.

Storage limitation

The fifth principle is \textit{storage limitation}: “personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed”.\textsuperscript{199} As mentioned in the previous paragraph about data minimisation, \textbf{in STARR, duration of storage should not exceed the period for which the data is necessary for carrying out a specific purpose}. Personal data may be stored for longer periods when the processing of data for scientific research purposes is involved (in accordance with

\begin{itemize}
\item \textsuperscript{193} Article 5 (1) (b) GDPR.
\item \textsuperscript{194} Recital 50 GDPR; Article 29 Working Party, WP 203, Opinion 03/2013 on purpose limitation, April 2, 2013, p. 40.
\item \textsuperscript{195} Article 5 (1) (c) GDPR.
\item \textsuperscript{196} See: Article 29 Working Party, WP 216, Opinion 05/2014 on Anonymisation Techniques, April 10, 2014, p. 11-37.
\item \textsuperscript{197} See: Article 29 Working Party, WP 202, Opinion 02/2013 on apps on smart devices, February 27, 2013, p. 11; Article 29 Working Party, ANNEX - health data in apps and devices, February 5, 2015, p. 6.
\item \textsuperscript{198} Article 5 (1) (d) GDPR.
\item \textsuperscript{199} Article 5 (1) (e) GDPR.
\end{itemize}
Article 89(1) GDPR but it is recommended to the partners the implementation of the appropriate technical and organisational measures required by the law in order to safeguard the rights of individuals. 200

Data security, integrity and confidentiality

The sixth principles are data security, integrity and confidentiality: “personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures”. 201 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights of individuals, in STARR the controller(s) and the processor(s) shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia: the pseudonymisation and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing. 202 In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. 203 Adherence to an approved code of conduct 204 or an approved certification mechanism 205 may be used as an element by which to demonstrate compliance with the requirements set out by law. 206 Additionally, the controller(s) and processor(s) shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller. 207

If in STARR a case of a personal data breach occurs, the controller(s) shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of stroke survivors. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. 208 The processor shall notify the controller without undue delay after becoming aware of a personal data breach. 209 The notification of a personal data breach to the supervisory authority shall at least: describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; describe the likely consequences of the personal data breach; describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. 210 Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases.

---

200 Article 8 (1) GDPR.
201 Article 5 (1) (e) GDPR.
202 Article 5 (1) (f) GDPR.
203 Article 32 (1) GDPR.
204 Article 32 (2) GDPR.
205 Article 40 GDPR.
206 Article 42 GDPR.
207 Article 42 (1) GDPR.
208 Article 32 (3) GDPR.
209 Article 32 (4) GDPR.
210 Article 33 (1) GDPR.
211 Article 33 (2) GDPR.
212 Article 33 (3) GDPR.
without undue further delay.\textsuperscript{211} The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.\textsuperscript{212}

**When the personal data breach is likely to result in a high risk to the rights of a person, the controller shall communicate the personal data breach to the data subject without undue delay, describing in clear and plain language the nature of the personal data breach.**\textsuperscript{213} The communication of a personal data breach to the data subject shall not be required if, for instance, the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach (in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption); the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise; it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.\textsuperscript{214} If the controller has not already communicated the personal data breach to the data subject, the supervisory authority may require it to do so.\textsuperscript{215}

*Accountability of the controller*

Finally, the last general data protection principle is accountability of the controller: the controller shall be responsible for, and be able to demonstrate compliance with, principles stated in Article 5 GDPR.\textsuperscript{216}

**CHAPTER 5: Data subjects rights**

The EU data protection framework confers on data subjects several rights. In the context of STARR the data subjects could be (1) the patients and health professionals whose data is (would be) collected during the interviews and/or whose data would be processed in the course of the validation of the STARR technical solution and (2) the future users of the STARR solution when it becomes potentially operational.

(a) Directive 95/46/EC

The rights that currently exist under the Directive are the right of information, of access to one’s personal data, of rectification, erasure and blocking, the right to object and the right not to be subject to automated decisions which significantly affect an individual. These will be discussed in turn with reference to their application in the STARR project. In addition, *Article 8 CFREU* explicitly mentions the right of access and rectification.

*The right of information*

Pursuant to Article 10 Directive 95/46/EC, the controller or his representative should provide the data subjects information about the identity of the controller (and his representative if applicable), the purposes

\textsuperscript{211} Article 33 (4) GDPR.
\textsuperscript{212} Article 33 (5) GDPR.
\textsuperscript{213} Article 34 (1) (2) GDPR.
\textsuperscript{214} Article 34 (3) GDPR.
\textsuperscript{215} Article 34 (4) GDPR.
\textsuperscript{216} Article 5 (2) GDPR.
of the processing, the recipients of the data, whether it is optional or obligatory for data subjects to provide their data and the consequences (if any) of not providing their data, the data subject’s right to access his data and/or have it rectified. As this is the minimum data to be provided, the controllers are free to provide further information with regards to the processing of data subjects’ data. If the data are not obtained from the data subject, then the controller or his representative should inform the data subject also of the categories of data concerned, in addition to the information given above. The aim is to guarantee fair processing and allow individuals to exercise control over the processing of their data. It also enhances transparency. In principle, the information is to be provided at the time the data are collected. If the data are not obtained from the data subject and the controller plans to disclose this data to third parties, then the information has to be provided at latest at the time of this first disclosure. The controller is not obliged to provide this information where the data are not collected directly from the data subject and they are to be processed for scientific and historical research purposes on condition that the provision of the information to the data subjects is impossible or involves disproportionate efforts or data recording and disclosure is laid down by law and there are adequate safeguards.

Application to STARR

When collecting data from the volunteers who will participate in the STARR interviews, in testing the final STARR solution or other STARR research activities, the designated controller for the particular activity will have to provide the above-mentioned information to the volunteers. As it is a research project with volunteers who will meet personally the STARR researchers, the latter can easily hand them out the required information printed out on leaflets, for example. This should be done before the volunteers provide their consent. This information should be written in such a way that individuals can easily understand it. For this purpose the information should be translated in a language understood by the volunteer. It should be explicitly mentioned that since this is research project, participation is voluntary and no negative consequences will ensue for those who do not wish to participate and provide their data.

A situation might occur where STARR researches obtain personal data already collected outside the STARR project. If the disclosure to the STARR project is laid down by law with appropriate safeguards in the Member State where the controller is established (e.g. HOPALE wishes to process medical records of HOPALE’s patients for research purposes in STARR and this is expressly provided for in French law), then HOPALE would not be obliged to inform each patient. However, for transparency purposes this is still recommendable if it is possible and would not require disproportionate effort.

Providing the required information would be more challenging in a real-life situation where stroke survivors would download the STARR application directly. In the first place, the controller for the data processing through this app would need to be defined. In case there are multiple controllers (e.g. a hospital director and the app developer and/or provider), these controllers will have to agree on the content of the information to be provided to data subjects and the method of providing it to the stroke survivors before

---

217 Article 10 Directive 95/46/EC.
218 Article 11 (1) Directive 95/46/EC.
219 Article 11 (2) Directive 95/46/EC.
they download the app and it starts collecting their data. An option could be providing the information on the screen of the stroke survivor’s device, followed by two buttons – ‘I consent’ and ‘I do not consent.’

The right of access

Pursuant to Article 12 (a) Directive 95/46/EC, data subjects have the right to obtain from the controller information whether the controller is processing data concerning the data subject, as well as information on the purposes of the processing, the categories of data processed and recipients to whom the data are disclosed. The data subject has the right to have the data processed on him (and their source) to be communicated to him. This right can be exercised without constraint, at reasonable intervals, and without excessive delay or expense. Pursuant to the CJEU, however, this does not mean that data subjects automatically have the right to obtain a copy of a document containing their data as a summary thereof would be sufficient. Especially in the case when automated decisions are taken about individuals, the data subject should know the logic involved in this processing.

Application to STARR

During the research and testing/validation phase of the project, the volunteers should have the right any time to turn to the designated controller(s) for the particular data processing operation (e.g. the interviews and/or the validation at the end of the project) and to inquire whether STARR processes data on them and see which data is processed on them, for what purposes and the recipients of the data. This access to their personal data will enable the concerned volunteers to exercise their other rights, e.g. request the rectification of their data if, e.g. it is inaccurately or unlawfully collected.

In real-life cases when the app would be operational, the stroke survivors should be able any time to request access to the information that the app processes both on their terminal device and on the back-end of the system, e.g. on the computers and other storage devices in the respective hospitals or by the app/communication providers. They should be able to do this in a language they speak and understand well. Similarly to the right of information, the right of access allows the data subjects to exercise control over the processing of their own data and enhances transparency.

The right of rectification, erasure and blocking.

Data subjects have the right to request their data to be rectified (i.e. corrected), erased (i.e. deleted) or blocked (e.g. frozen) if their data is processed in breach of Directive 95/46/EC, e.g. because it is incomplete or inaccurate. This helps ensure that, e.g. no wrong decisions are taken with regards to a certain data subject, that the data are not used for incompatible purposes or that no excessive data is processed about them.

Application to STARR

In the research and testing/validation phase of the project STARR wishes to obtain accurate results about the needs of the stroke survivors for a successful therapy, rehabilitation and preventing another stroke, as

221 Article 12 (b) Directive 95/46/EC.
well as on the performance of the STARR technology when it is ready. Thus, it is essential that the personal
data on the patients is accurate and the data subjects should have the right to request that inaccurate data
is rectified or it is blocked until rectified or even erased if, e.g. a data subjects withdraws his consent and
requests that the data previously collected on them is deleted. The same argument goes also for the
subsequent app usage in an operational environment. As the processing the data through the app concerns
the health of stroke survivors and the medical diagnosis given to them, as well as the treatment provided to
them, the accurate collection, analysis and communication of their data, e.g. on health, is essential for the
success of the therapy. Thus, stroke survivors should be allowed at any time to request inaccurate data to
be rectified and block its processing until the inaccuracy is solved. Data erasure is more difficult as the data
are processed in the medical context and doctors are obliged to store certain data on their patients (this
might differ from country to country or medical institution to medical institution). Therefore, it is up to
every controller of the application to determine the data erasure policies in accordance with the applicable
rules.

The right to object

Article 14 (a) Directive 95/46/EC confers on data subjects the right to object to the processing of their
personal data on compelling legitimate grounds relating to his particular situation. If the objection is
justified, the controller should terminate the processing this particular data.

Similarly, Article 14 (b) Directive 95/46/EC provides for the right to object to the processing of data for
purposes of direct marketing.

Application to STARR

This right implies that in the first place no one should be obliged to participate in the STARR research
activities and subsequently use the STARR solution and thus have their data processed by the STARR
project and the STARR solution. If volunteers who participate in the STARR research and validation activities
decide that they do not wish their data to be processed any longer, they should have the right to request
the controller to terminate the processing of their data.

The same applies also to the operational phase when a stroke survivor might wish to stop using the app,
she should be free to stop using it. Depending on what data has been collected on him by the app, he
might object to the processing only of some of his data. Depending on the situation, the right to object
might also involve the request directed at the respective hospital/clinic to stop using the data collected via
the app, unless they are required for keeping the medical records.

Most importantly, the stroke survivors have to be informed of and be allowed to object to the further
processing of their data for purposes of direct marketing, e.g. targeting stroke survivors with
advertisements about medication and medical products. Since marketing of products is a purpose
incompatible with the purpose of diagnosis and treatment, objecting to direct marketing will not affect the
health of the stroke survivors and thus there should be no reasons to deny data subjects this right.
Automated decisions

Pursuant to Article 15 of Directive 95/46/EC, individuals have the right not to be subject to a decision which significantly affects him or produces legal effects concerning him and which is taken only on the basis of automated processing of data (not necessarily only his personal data) which intends to evaluate his performances. In the context of STARR, this could be interpreted to mean that the stroke survivors’ data should not be processed via the app by (health) insurance companies, for instance, to automatically determine whether someone qualifies for health insurance and if yes – which health insurance plan they should be allowed to participate in. This evaluation should not depend on conclusions taken on the basis of the app data only when this would produce negative impact on the stroke survivors and deprive them of opportunities that they would normally enjoy.

(b) GDPR

Chapter III of the GDPR, which will replace Directive 95/46/EC, enshrines the provisions on the rights of data subjects. Oftentimes these rights are quite similar in content to the ones that Directive 95/46/EC currently provides for. Still, there are new rights, e.g. on data portability, and clarification on the mechanism for exercising data subjects’ rights. Therefore, the following paragraphs will highlight the novelties that the GDPR introduces in respect of data subjects’ rights and will not repeat the provisions that were taken from the Directive. In addition, the following discussion will not repeat the recommendations as to how the data subjects’ rights should be exercised in the framework of STARR, unless there are differences as compared to the Directive.

Transparency and mechanisms for exercising data protection rights

Article 12 GDPR explicitly provides for transparency towards data subjects. Thus, the controller shall communicate to them information related to the processing of their data “in a concise, transparent, intelligible and easily accessible form, using clear and plain language.” This would make it possible for data subjects to comprehend and assess the risks of the processing of their data and exercise more control over this processing.

It is the responsibility of the controller to facilitate the exercise of data subjects’ rights. If a data subject has made a request, e.g. for access to his/her data and their rectification, the controller should inform the said data subject of the actions taken in respect of the request. The given deadline is one month, with a possibility of extension by two months if the circumstances necessitate this. In this case the controller should inform the data subject within one month and put forward the reasons for the delay. The same deadline applies in the case the controller does not act upon the request of the data subject, in which case the controller has to inform the data subject of the possibility to lodge a complaint with a supervisory authority and seek a judicial remedy. The information is to be provided free of charge, unless the request

---

222 Article 12 (1) GDPR.
223 Article 12 (2) GDPR.
224 Article 12 (3) GDPR.
225 Article 12 (4) GDPR.
is “manifestly unfounded or excessive.” In these cases the controller can either charge a reasonable fee or refuse to react to the request, in which case he should demonstrate that the request is manifestly unfounded or excessive.\textsuperscript{226} In case the controller has reasonable doubts about the identity of the data subject, he may request additional information to confirm his identity before acting upon the request.\textsuperscript{227}

**Application to STARR**

The implications for STARR are that in the research and validation activities of the project, which involve personal data processing of interviewees and volunteers, STARR should put in place mechanisms to comply with the above-mentioned requirements and enable the data subjects in STARR to exercise their rights. This could be achieved, for example, with proper STARR internal policies. When the controller for each data processing operation in STARR is designated, he should abide by this policy. The same applies to the controller of the future STARR solution, e.g. the particular hospital, who should put in place such mechanisms for the STARR app users to exercise their data protection rights.

**The right to information**

When the data are collected directly from the data subject, Article 13 GDPR requires the controller to provide more information to the data subject as compared to the requirements under Article 10 Directive 95/46/EC. Thus, in addition to the required information under the Directive, the controller would have to inform the data subject also of the following: the contact details of the controller, if applicable – the contact details of the data protection officer, the legal basis for the processing, if the processing is based on the legitimate interest(s) of the controller or a third party – which this interest is, and last but not least - if a transfer is to a TC or international organization is intended, the existence or absence of an adequacy decision by the Commission or in case another basis is used for the transfer – the existence of safeguards and how the data subject can have access to these safeguards.\textsuperscript{228}

To ensure fair and transparent processing, the controller should further inform the data subject of (1) the storage period, (2) the existence of the rights to access, rectification, erasure or restriction of processing, data portability or right to object to the processing, (3) the right to withdraw one’s consent if the legal basis is consent, (4) the right to lodge a complaint with a supervisory authority, (5) whether the provision of the data is a statutory or contractual requirement, whether it is compulsory and what the consequences of failure to provide the data are and (6) whether the data will be used for automated decision-making such as profiling and meaning information on the logic involved for the automated decisions and possible consequences for the data subjects.\textsuperscript{229}

If the controller intends to process the data for purposes different from the original one for which the data were collected, then he should notify the data subject thereof before this further processing.\textsuperscript{230} It is not explicitly stated that the data subject may object to such further processing. It is assumed that the right to object could be applicable in this case. Furthermore, this provision does not explicitly state that the further

\textsuperscript{226} Article 12 (5) GDPR.
\textsuperscript{227} Article 12 (6) GDPR.
\textsuperscript{228} Article 13 (1) GDPR.
\textsuperscript{229} Article 13 (2) GDPR.
\textsuperscript{230} Article 13 (3) GDPR.
processing should be only for purposes compatible with the original one(s), as Article 5 (1) (b) GDPR requires. As Austria has pointed out, the GDPR weakens the purpose limitation principle by allowing more (re)-uses of the data to be considered as compatible.\textsuperscript{231} It is encouraging that the data subject should be informed; however, the existence of actual possibilities for the data subject to prevent such further processing is doubted.

When the data are \textit{not} collected directly from the data subject, Article 14 GDPR requires that the controller shall provide in principle the same information as under Article 13 GDPR and in addition inform the data subject of the categories of personal data to be processed and the source from which the data have been obtained.\textsuperscript{232} The information shall be provided to the data subject at latest within one month after the collection. If the data are used for communication with the data subject, then the controller should provide the information at latest at the time of the first communication with the data subject. If the data are to be disclosed to another recipient, then the controller should inform the data subject at latest when the data are disclosed to third parties.\textsuperscript{233}

Similar to Directive 95/46/EC, there are exceptions to the obligation to provide this information. The one that could possibly apply to STARR is the exception for research purposes, whereby if the provision of information proves to be disproportionately difficult or impossible and would seriously impair the objectives of the research, for example. Nevertheless, the safeguards provided for in Article 89 (1) GDPR have to be respected and the controller should take the appropriate measures to protect the data subject’s rights and legitimate interests.\textsuperscript{234}

\textbf{In conclusion, in the STARR project and later when the solution is operational, the designated controller(s) should provide the information as required by Articles 13 or 14 GDPR and restrict this right only in so far as provided in these Articles.}

\textbf{The right of access}

The main differences between the right of access under Directive 95/46/EC and under Article 15 GDPR is the obligation under Article 15 GDPR to provide information also on the envisaged storage period or criteria for determining it, the envisaged consequences of automated processing if any, the right to object to the processing, to lodge a complaint with a supervisory authority.\textsuperscript{235} In addition, if data are transferred to a Third Country (TC) or international organization, then the data subject should be informed of the safeguards surrounding this transfer.\textsuperscript{236} The latter is especially important for STARR as one of the partners who is expected to participate in the data processing is RT-RK (Serbia). As soon as their role in the data processing is defined, the information to the data subjects should include a description on how the data was transferred to RT-RK Serbia and what safeguards were made, if such a transfer should take place.

\textsuperscript{232} Article 14 (1) (d) and 14 (2) (f) GDPR.
\textsuperscript{233} Article 14 (3) GDPR.
\textsuperscript{234} Article 14 (5) (b) GDPR.
\textsuperscript{235} Article 15 (1) GDPR.
\textsuperscript{236} Article 15 (2) GDPR.
in the first place. Last but not least, without prejudice to the rights and freedoms of the others, the controller shall provide a copy to the data subject of his/her personal data which are being processed. This should be free of charge, unless the data subject requests further copies.²³⁷

Thus, if a volunteer who participates in the STARR interviews and/or validation demonstrations and wishes to have access to his data, should be provided with a copy thereof, containing the information as provided in Article 15 GDPR.

*The right to rectification*

Article 16 GDPR on the right to rectification does not differ essentially from the right to rectification provided for in Article 12 (b) Directive 95/46/EC. In Article 16 GDPR it is explicitly mentioned that the controller should rectify the data “without undue delay.” Thus, if requests for rectification are received in the course of STARR, e.g. a stroke survivor provided his medical data during one of the interviews and later wishes to correct the provided data or make it complete, the designated controller should fulfill this request without undue delay.

*Right to erasure or ‘right to be forgotten’*

Article 17 GDPR clarifies in more detail the conditions under which a data subject could exercise his right to erasure, i.e. at least one of the following conditions needs to be satisfied: (1) the data are not needed any more in relation to the purpose for which they are processed, (2) the data subject withdraws his consent and there is no other applicable legal basis for the processing, (3) the data subject objects to the processing pursuant to his right to object and there are no overriding legitimate grounds to continue the processing, (4) the personal data have been unlawfully processed, (5) the personal data have to be erased pursuant to a legal obligation to which the controller is subject, (6) the personal data have been collected by under-age children in relation to the provision of information society services. When one of these conditions is satisfied, the controller shall erase the data “without undue delay.”²³⁸ For STARR this means that, e.g. a volunteer wishes to withdraw his participation in the interviews or subsequently in the validation demonstrations, he may request the deletion of his data. Or alternatively if during the interviews the STARR partners collected more medical data from patients and subsequently it is established that not all of this data would be necessary, then the unnecessary data should be erased. Another example would be if the STARR partners illegally collect personal data, then they would be asked to erase it. In any case, at the end of the project, if the data are not needed for further research purposes, they should be deleted.

If the controller has made the personal data available and the data subjects’ request for erasure is justified, the controller shall take reasonable steps to inform the other controllers who process the data of the request for erasure.²³⁹

²³⁷ Article 15 (3) and (4) GDPR.
²³⁸ Article 17 (1) GDPR.
²³⁹ Article 17 (2) GDPR.
However, there are exceptions to the right to erasure in several cases. The one most likely to possibly apply to STARR is the one concerning research. However, the restriction applies only in so far as the data erasure would seriously impair or render impossible the research purposes. When a controller relies on such a restriction, he should still observe the requirements in Article 89 (1) GDPR.\textsuperscript{240}

**Right to restriction of processing**

The right to restriction in Article 18 GDPR resembles the right to blocking under Directive 95/46/EC, i.e. freezing the further processing of the data. In Article 18 GDPR this right has been developed and the conditions for exercising it are specified. Thus, one of the following conditions should be fulfilled: (1) the accuracy of the data is contested by the data subject until the data controller has verified the accuracy, e.g. a patient or a STARR volunteer contests that the wearable connected to the app which measures the blood pressure has measured it correctly and believes there are mistakes (2) the processing is unlawful and the data subject does not wish to have the data deleted, but requests the restriction of their usage, e.g. the STARR app would collect further data than the stroke survivor has consented to but he does not want the data to be deleted as he might want to use it later as evidence for the unlawful processing, (3) the controller does not need the data any more but the data subject requires them to establish, exercise or defend their legal claims, e.g. the research purpose has been fulfilled and the data should be deleted, but the data subject requests the data to be kept, e.g. if the data are needed for the STARR volunteer to prove that they were present at a certain time at the place where a STARR test/validation took place, (4) the data subject has objected to the processing of the data and the controller needs to examine whether the legitimate interests of the controller override those of the data subject, e.g. a STARR volunteer wishes to have the data deleted, i.e. objects to the further processing of the data, but STARR wishes to examine whether the research interests of the STARR controller override the objection of the data subject.\textsuperscript{241}

Once the processing the data is restricted, the data will remain stored but will not be available for any other data processing operations. However, they can be further processed upon one of the conditions: (1) the data subject consents to the further processing, (2) the data is needed for the establishment, exercise or defense of legal claims or (3) for the protection of the rights of another natural or legal persons or (4) for reasons of important public interest of the Union or of a Member State.\textsuperscript{242}

If the restriction of the processing is lifted, then the controller should notify the data subject before the restriction is lifted.\textsuperscript{243}

In cases where the data subjects exercises his right to rectification, erasure or restriction of processing, the controller should notify the recipients of the data subject’s data, unless this proves disproportionately difficult or impossible. The data subject should be informed of these recipients if he/she requests so.\textsuperscript{244} For example, if a STARR volunteer wishes to withdraw his consent for participating in the interviews or the

\textsuperscript{240} Article 17 (3) (d) GDPR.
\textsuperscript{241} Article 18 (1) GDPR.
\textsuperscript{242} Article 18 (2) GDPR.
\textsuperscript{243} Article 18 (3) GDPR.
\textsuperscript{244} Article 19 GDPR.
validation demonstrations, the controller, e.g. HOPALE, should communicate this to the other STARR partners who received the data of that volunteer.

**Right to data portability**

One of the novelties of the GDPR is the introduction of the right to data portability. In essence, it means that data subjects have the right to receive from the controller to whom they have provided their personal data this data in a structured and machine-readable format so that they can transmit this data to another controller without any hindrances from the first controller. The two conditions are that the processing should be based on consent (and not on the basis of performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) and the processing is carried out by automated means.\(^{245}\) Where technically feasible, the data should be transmitted from one controller to the other one.\(^{246}\) This right is without prejudice to the right to erasure.\(^{247}\)

This implies that in the case the STARR app solution would become operational and there would be other providers of similar technologies, the stroke survivor should have the right to switch to another application provider and his medical history, as processed by the STARR solution, should be provided in a machine-readable format to the data subject and possibly directly to the controller of the other application.

**Right to object**

In essence the right to object under Article 21 GDPR mirrors the right to object as under Article 14 Directive 95/46/EC. One difference is that Article 21 GDPR explicitly mentions the right to object in the context of research on grounds relating to the data subject’s particular situation unless the processing is necessary for the performance of a task carried out for reasons of public interest.\(^{248}\) Thus, unless STARR identifies such compelling tasks to be carried out in the public interest, a STARR volunteer’s objection to the processing of his data should be respected.

**Automated individual decision-making, including profiling**

In substance this right as enshrined in Article 22 GDPR is similar to the one in Article 15 Directive 95/46/EC. The only difference is that the GDPR allows automated individual decision-making if the data subject has given his explicit consent. Article 22 GDPR introduces an additional guarantee, namely that automated decisions may not be taken on the basis of sensitive data such as health/medical data, unless the data subject has given their explicit consent or the data are needed for substantive public interest and adequate safeguards are applied.\(^{249}\)

---

\(^{245}\) Article 20 (1) GDPR; Article 20 (3) GDPR.
\(^{246}\) Article 20 (2) GDPR.
\(^{247}\) Article 20 (3) GDPR.
\(^{248}\) Article 21 (6) GDPR.
\(^{249}\) Article 22 (4) GDPR.
CHAPTER 6: Transfers to Third Countries

In the context of the STARR project the personal data might need to be transferred to Third Countries (TC) because (1) one of the STARR partners, i.e. RT-RK, is not established in the EU but in Serbia, and a cloud solution is planned to be used for the STARR architecture through which RT-RK would have access to the data (see STARR D6.1) and (2) if the STARR solution becomes operational and again this solution would rely on cloud storage or data would be transferred to a TC in another way, e.g. one of the app providers would be located in a TC.

During the Bilbao meeting, 27-29 September 2016, the possibility that RT-RK will not be involved in the personal data processing was discussed. It is understood that RT-RK does not need personal data to develop the software. If they need data for the calibration of this software, it is possible for them to work with simulated or completely anonymized data. The possibility that the host of the platform, where the personal data will be stored and further processed, i.e. TID, controls the access to the platform with the data and restricts it to partners in the EU only, was also discussed. These options of access control and data anonymization/simulation are privacy-friendly solutions and their implementation in the project is strongly encouraged. In case RT-RK would work only with simulated data and/or would receive completely anonymized data from the other STARR partners without being able to access the personal data, then this would mean that RT-RK is not going to process personal data and thus no transfer to a TC would take place.

As to cloud solutions, at the Bilbao meeting, 27-29 September 2016, it was discussed that there are other possibilities for the computation and storage of personal data, such as hosting the data on physical servers in Spain and/or France, which would be preferred to cloud solutions from a privacy point of view. This will be further discussed with the concerned partners in the coming months.

Even though the relevance of data transfers for STARR is still debated and a final decision will be taken at a later stage, the following paragraphs will nevertheless explore the EU framework on data transfers to TCs so that the STARR partners are familiar with it. As it is not certain at which moment in the lifetime of the project this transfer might take place, if such a transfer takes place at all, it is not clear whether the transfer will be subject to Directive 95/46/EC or to the GDPR. Thus, the provisions of both instruments will be examined.

Directive 95/46/EC

Under Article 25 of Directive 95/46/EC, for data to be transferred to a Third Country (TC), e.g. Serbia, this TC should provide an “adequate level of protection” (Article 25 (1)). In the Schrems case the CJEU established that “adequate” should mean “essentially equivalent” to the level of protection afforded in the EU.256 Pursuant to Article 25 (2), there are several factors that play a role in assessing the adequacy of the concerned TC, namely:

- All the circumstances surrounding the transfer, in particular the nature of the data, the purpose and duration of the proposed processing,

---

256 CJEU, C-362/14, Schrems, 6 October, 2015 par. 73.
The country of origin and of final destination,
- The rules of law, both general and sectoral, in force in the TC in question, and
- The professional rules and security measures which are complied with in that country.

The Commission may find that a particular TC ensures such an adequate level of protection in view of its domestic law and or of its international commitments it has entered into.\textsuperscript{251} Such adequacy decisions would be possible also under Article 45 of the new GDPR. As of now the European Commission has not found Serbia to provide such an adequate level of protection, i.e. there is no adequacy decision for Serbia.\textsuperscript{252}

Even if Serbia is not considered to be “adequate” in data protection terms, transfers to entities in Serbia could still be effected by way of one of the derogations provided for in Article 26 (1). These are derogations from the general prohibition on transferring data to third countries and should be thus the last resort only. Of these derogations, the one which looks most suitable for the STARR project is the “unambiguous consent” of the data subject.\textsuperscript{253} This is possible within a research environment such as STARR. However, the data subjects would have to be clearly informed of the intended transfer to Serbia and explicitly give his consent, e.g. by signing a specific consent form.

A Member State may authorize a transfer to a country which does not provide an adequate level of protection if the concerned controller in the said TC “adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of corresponding rights.”\textsuperscript{254} These safeguards could be adduced via standard contractual clauses, for example.\textsuperscript{255} The Member State authorizing such a transfer should inform the Commission and the other Member States. These may object on justified grounds and the Member State which intended to authorize the transfer should comply with the Commission’s objection, expressed through a decision.\textsuperscript{256} The Commission has already issued two sets of clauses for transfers to controllers established outside the EU/EEA and one set of clauses for transfers to processors outside the EU/EEA.\textsuperscript{257} It is understood that controllers may rely on them without having to inform the Commission and the other Member States of such transfers. In case the challenge to the quality of such clauses is successful, then other clauses would need to be drafted.

The GDPR

As to the applicable provisions of the GDPR, it states that the level of protection of the privacy and data protection rights of the individuals should not be undermined by such international transfers.\textsuperscript{258} In the absence of an adequacy decision (as is the case with Serbia), the personal data may be transferred if the importing controller or processor ensures adequate safeguards and enforceable data subject rights and effective legal remedies are available.\textsuperscript{259} Depending on the instrument through which the safeguards are provided for, the national data protection supervisory authorities might or might not need to authorize

\textsuperscript{251} Article 25 (6) Directive 95/46/EC.
\textsuperscript{253} Article 26 (1) (a) Directive 95/46/EC.
\textsuperscript{254} Ibid.
\textsuperscript{255} Article 26 (2) Directive 95/46/EC.
\textsuperscript{256} Ibid.
\textsuperscript{257} Article 26 (3) Directive 95/46/EC.
\textsuperscript{259} Article 44 GDPR.
\textsuperscript{259} Article 46 (1) GDPR.
the transfer. Those cases are outlined in Article 46 (2) and 46 (3) GDPR. Standard Contractual Clauses adopted or approved by the Commission are one option. If a controller relies on them for the transfer of data to a Third Country, then no further authorizations from a supervisory authority is needed.\textsuperscript{260}

In addition, transfers can take place on the basis of Binding Corporate Rules (BCRs) as outlined in Article 47 GDPR. These BCRs are mostly applicable for big undertakings and corporations. BCRs could be used in cases where one undertaking has representations/establishments in different countries, e.g. in one EU Member State (e.g. Croatia) and several more, e.g. in Serbia and/or Japan, etc. These BCRs should be legally binding, apply to and be enforced by every member of the undertaking. They should “expressly confirm enforceable rights” to the concerned data subjects. In addition, their content should comply with a number of requirements, i.e. the BCRs should contain certain provisions.\textsuperscript{261} These are enumerated in Article 47 (2) GDPR, e.g. structure and contact details of undertakings, description of data to be transferred, the application of the data protection principles, the rights of data subjects, liability, complaint procedure, compliance verification procedure, etc.\textsuperscript{262} Last but not least, BCRs should be approved by the competent supervisor authority.\textsuperscript{263} As described in Chapter 1 above, it is not clear whether RT-RK’s offices in Croatia could be considered as a valid establishment for the purposes of the GDPR and whether such BCRs exist within RT-RK. Thus, it is not clear whether they can be relied on in STARR.

Similarly to Article 26 Directive 95/46/EC, Article 49 of the GDPR also allows for derogations for specific situations only, i.e. these should not be the primary choice of the controller but their usage should be rather exceptional. If in STARR one needs to resort to these derogations in a final instance, again the most suitable basis would be the consent of the data subject. The wording is different from the wording of the Directive. Pursuant to Article 49 (1) (a), the consent should be explicit and the data subject should be first informed of the possible risks of the transfer due to the absence of an adequacy decisions and of appropriate safeguards. Consent cannot be relied on by public authorities in the exercise of their public powers.\textsuperscript{264}

In a very last resort, if a transfer could not be based on any of the above-mentioned provisions, it could still take place if all of the following conditions are met. Thus, the transfer should (1) not be repetitive, (2) concern only a limited number of data subjects, (3) be necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject and (4) the controller has assessed all circumstances surrounding the data transfer and pursuant to this assessment has provided suitable safeguards for personal data protection. This assessment should be documented and the supervisory authority should be informed. The concerned data subjects should be specifically informed of the transfer and of the legitimate reasons for it.\textsuperscript{265} However, it is very unlikely that in the framework of a research project these conditions would be satisfied. Thus, in STARR the other possible options should be preferred.

\textsuperscript{260}Article 46 (2) GDPR.
\textsuperscript{261}Article 47 (1) GDPR.
\textsuperscript{262}Article 47 (2) GDPR.
\textsuperscript{263}Article 47 (1) GDPR.
\textsuperscript{264}Article 49 (3) GDPR.
\textsuperscript{265}Article 49 (1) second subparagraph j Article 49 (6) GDPR.
Requests by judicial and/or administrative authorities for transfers and/or disclosure of data may take place only on the basis of an international agreement between the specific TC and the Union or one of its Member States. Thus, e.g. if once the patient data from the demos are made available to RT-RK in Serbia (via the cloud), and subsequently a Serbian court requests access to this data, this may follow only if an international agreement exists.\(^{266}\)

CHAPTER 7: Data Protection Impact Assessment

7.1. General DPIA requirements

One of the novelties of the GDPR is the introduction of a requirement for a carrying out a Data Protection Impact Assessment (DPIA). A DPIA needs to be carried out by the controller in cases where a data processing operation is likely to be high-risk with regards to the rights and freedoms of individuals. The objective is to assess the impact of the planned processing on the protection of personal data.\(^{267}\) This can be achieved by first identifying the risks for the data subjects, in the case of STARR the stroke survivors who would use the technology in the future, and by proposing mitigation measures to address these risks and evaluating these mitigation measures.\(^{268}\) It should be an ongoing exercise and should be gradually completed and updated.

Pursuant to the GDPR, there are several cases where a DPIA is considered to be especially necessary. This list, however, is not exhaustive. One of the mentioned cases is when special categories of data, e.g. health data such as medical data on stroke survivors, are being processed on a large scale.\(^{269}\) The assessment should contain at least a systematic description of the data processing and the purposes of the processing and where applicable – the legitimate interests of the controller. When the purpose is specified, the necessity and proportionality of the data processing should be assessed on the basis of this purpose. Further, the risks to the stroke survivors should be assessed and measures and safeguards should be proposed to address these risks and to ensure personal data protection. It should also document how compliance with the Regulation is ensured.\(^{270}\)

However, it seems that a DPIA is not mandatory if the personal data processing concerns personal data from patients by an individual physician or a health care professional.\(^{271}\) This could imply that in a situation where the stroke survivor uses the STARR app to communicate only with his/her doctor and/or carer, then such a PIA might not be necessary before the app is put in operation. However, bearing in mind that in an operational environment the personal data processing which takes place through the app will involve not only the health professionals but also possibly the app providers, relatives and friends (e.g. if he data is used as a social network platform as in Use Case 3), data might be processed in the cloud whereby unauthorized entities might gain access to it, then it is advisable to carry out such a DPIA, identify and address the risks created through this complex processing of personal data, which involves several parties.

\(^{266}\) Article 48 GDPR.
\(^{267}\) Article 35 (1) GDPR.
\(^{269}\) Article 35 (2) (b) j Article 9 (1) GDPR.
\(^{270}\) Article 35 (7) GDPR.
\(^{271}\) Recital 91 GDPR.
When carrying out a DPIA, the controller should include the views of stakeholders, e.g. the future users of the STARR application, especially the stroke survivors.\(^{272}\)

7.2. DPIA considerations for STARR

The following paragraphs will provide a first iteration of the DPIA for the STARR solution.\(^{273}\) Since the technical developments are still at their initial phase, a full DPIA cannot be carried out at this moment. Thus, the DPIA should be a living document and can be further elaborated on. As the Article 29 Working Party has maintained, the DPIA should consist, amongst others, of a description of the envisaged data processing, the risks for the rights and freedoms of the data subjects, the mitigation and security measures, safeguards.\(^{274}\)

(1) Description of the envisaged processing

At this time no description of the STARR technology is available. First prototypes can be found in STARR Deliverable 6.1. When the technical partners have agreed on the technical model of the STARR technology, a description will be provided.

As to the list of personal data to be processed, they will be fully defined once the technology purposes and architecture are defined. However, for now, based on current discussions in STARR, it appears that the following categories of data could be processed: dietary information, blood pressure, exercise/movements of limbs (graphical representation), emotions, compliance with exercise and performance assessment. However, this list is subject to change. STARR partners are encouraged to inform of FIZ of any technical details that bear relevance for the accurate description of the envisaged STARR platform. The main purposes of the STARR solution are to assist stroke survivors with the rehabilitation after a stroke (in a home environment), prevent another stroke, help stroke survivors become more independent in their daily activities and give them feedback on that, monitor their daily progress and health condition, provide a social platform for the different stroke survivors, provide a channel of communication between the stroke survivor on one hand and (1) doctors and/or (2) carers and/or (3) relatives taking care of the survivor and/or (4) other stroke survivors in the network of one stroke survivor.

(2) Main risks and mitigation measures

Main risk to the right to privacy and data protection is the loss of or illegal access to health data, which reveal sensitive information to stroke survivors. On one hand this could compromise them (through mere exposure of health condition and daily performance). On the other hand the data can be held against them, e.g. pharmaceutical or (health) insurance companies targeting the specific survivors to sell them medicines and other medical products. Loss of data could lead to inconveniences in the further therapy of patients.

---

\(^{272}\) Article 35 (9) GDPR.

\(^{273}\) This refers to the STARR solution, not to the processing related to the interviews/technology tests in the lifetime of STARR.

The table below sets the framework for carrying out the DPIA and it should be elaborated on, especially the last column, in the course of the project when more information is available. The table has been inspired by the Article 29 Working Party.\(^{275}\)

<table>
<thead>
<tr>
<th>Nr</th>
<th>Risk</th>
<th>Risk Description</th>
<th>Severity (Low, Medium, High)</th>
<th>Impact on stroke survivor</th>
<th>Proposed mitigation measure – To be completed by technical partners</th>
<th>Implemented (Y/N)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data security breach</td>
<td>E.g. data loss, hacking, interception, etc.</td>
<td>TBD</td>
<td>Cannot control one’s own data, possible abuse depending on who gains access to it</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Illegal access</td>
<td>E.g. through cloud computing access from all over the world, cannot be controlled, e.g. by security agencies</td>
<td></td>
<td>Cannot control one’s own data, possible abuse depending on who gains access to it</td>
<td>E.g. local storage of data/no cloud computing, encryption, strict authentication mechanism</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Inaccurate processing</td>
<td>Wrong blood pressure measurement and communication to the doctor</td>
<td></td>
<td>Wrong diagnosis and treatment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Permanent tracking in/and or outside</td>
<td>Application collects someone’s location all the time</td>
<td></td>
<td>STARR obtains further information on someone’s lifestyle and location, can be part of big data and conclusions can be made against this person, e.g. profiling for purposes of direct marketing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Excessive data collected</td>
<td>e.g. data not necessary for the therapy or diagnosis</td>
<td></td>
<td>Obtain more information on stroke survivor, carry out datamining and profiling</td>
<td>Determine data collection and data deletion policies in STARR</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Re-purposing</td>
<td>Use for marketing purposes and health insurance determination, loss of control over use of data</td>
<td></td>
<td>Manipulation of choice</td>
<td>Stick to purpose limitation principle</td>
<td></td>
</tr>
</tbody>
</table>

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 689947.
<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Storage</td>
<td>Data stored for longer than necessary, allows re-purposing of data usage and illegal access</td>
<td>See above</td>
<td>Stick to STARR recommendations on data storage</td>
</tr>
<tr>
<td>8</td>
<td>Lack of legal basis</td>
<td>Data processed without legal basis, e.g. no consent provided when no other legal basis exists</td>
<td>Illegal processing – this can also occur if the consent is not valid, i.e. a data subject does not have a real and informed choice</td>
<td>Ask for consent which is specific, informed and explicit</td>
</tr>
<tr>
<td>9</td>
<td>Lack of transparency</td>
<td>Data subjects not given the necessary information before and during the data processing or given false information</td>
<td>Data subjects cannot take informed decisions and exercise their rights or exercise control over their data</td>
<td>Provide proper information notice</td>
</tr>
<tr>
<td>10</td>
<td>Lack of accountability</td>
<td>No proper data processing documentation and documentation on DP compliance maintained</td>
<td>Controller cannot monitor the data processing operations and their compliance with the DP framework, no policies in place for DP subjects to exercise their rights</td>
<td>Proper documentation policies to be put in place</td>
</tr>
<tr>
<td>11</td>
<td>Breach of data subjects’ rights</td>
<td>No policies to allow data subjects to exercise their rights or not complying with them</td>
<td>Data subjects cannot request information on the data processed on them, cannot have it rectified, erased or blocked or cannot object to the processing</td>
<td>Comply with the recommendations on how to allow data subjects to exercise their rights</td>
</tr>
</tbody>
</table>

Figure 1: Preliminary list of risks and proposed mitigation measures for the STARR technology
7.1. Data protection risks in STARR, recommendations to overcome them. Principles of privacy-by-design and default

The GDPR officially enshrines in law two concepts which have been widely discussed and analyzed even before the GDPR was adopted, namely privacy by design and privacy by default.276

Pursuant to the concepts of privacy by design, the controller, both at the time of determining the means of processing and during the actual processing, implement “appropriate technical and organizational measures” in order to implement data protection principles “in an effective manner” and to integrate the necessary safeguards into the processing so that the requirements of the Regulation are satisfied and the data subjects’ rights are respected.277 Such appropriate measures could range from pseudonymisation to automated data deletion. To determine what the appropriate measure(s) for each data processing operation are, the controller should consider on one hand the state of the art, the cost of implementation and the nature, context, scope and purposes of the personal data processing and on the other hand the risks of the processing for the data subjects.278

The risks for data subjects are analyzed in the table above, where also measures to overcome these risks by means of compliance with the GDPR principles and provisions, is proposed. This table is to be further elaborated on in the course of the project as the appropriate measures are not to be determined only before the beginning of the processing but also in the course of it, i.e. adjustments and improvements should be adopted too.

In addition, the technical and organizational measures adopted by the controller should by default, aka privacy by default.279 Through these measures it should be ensured that only the personal data which is necessary for a specific purpose should be processed, i.e. the principle of data minimization should be complied with. The principle applies to the amounts of data, to the extent of their processing, to the storage period and their accessibility, e.g. the default features should ensure that the personal data are not made accessible without the data subject’s cooperation to an indefinite number of individuals. For STARR this means that the measures indicated in the table above should be default settings in the STARR solution.

If any approved certification mechanism is available and can be used in STARR to implement the principles of privacy by design and by default, it can be used as one of the elements to demonstrate compliance with these principles.280

---

276 Article 25 GDPR.
277 Article 25 (1) GDPR.
278 Article 25 (1) GDPR.
279 Article 25 (2) GDPR.
280 Article 25 (3) GDPR.

This project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 689947.


3. Conclusion

The present deliverable provided a first analysis of the EU privacy and data protection requirements and principles as they apply to the STARR project at the present stage of its development. The following recommendations have been made to the STARR partners. In designing the STARR technology, partners should:

- integrate in the STARR solution(s) the principles of data protection (i.e. fairness, lawfulness and transparency; purpose limitation; data minimisation; data accuracy; storage limitation; security, integrity and confidentiality) (see chapter 4);
- carrying out a DPIA, with FIZ help, identifying the privacy and data protection risks for the stroke survivors who would use the technology in the future. They should also propose mitigation measures to address these risks (see chapter 7).

Regarding the research or testing activities in STARR, it is important that all the partners:

- clearly define what type of personal data they are going to process, how, and for what purpose(s) (to be done before processing starts) (see chapters 2-3-4);
- clearly define who the controller(s) will be - and, eventually, which partners could be processor(s) (see chapters 2-3).

In addition to the previous bullet points, the following recommendations can be made:

- before the data is processed, the controller should inform the stroke survivor, explaining the data operations to be performed on the personal data, should give the chance to the person not to give consent, and when patients give consent for one set of operations, this does not mean that STARR partners may process the data for other purposes (unless they find another legal basis). During all the different phases of the STARR project, according to Article 7 GDPR, partners involved in the collection of data must obtain the consent (of patients, medical specialists and carers) “in a manner distinguishable from other matters, in an easily accessible form and using clear and plain language”, and participants must be able to withdraw their consent easily. All the STARR partners should be extremely careful about meeting the requirements of patients and adapting their requests and their consent forms to the specific case (see chapters 2-3-4);
- protecting data subjects’ rights (i.e. right of information, of access and rectification, erasure and blocking, the right to object and the right not to be subject to automated decisions, the right to data portability, etc.) should be one of the goals of the project (see chapter 5);
- finally, with regard to the possible transfer of data to a Third Country (i.e. Serbia) in STARR, the EU procedures on data transfers should be complied with. In addition, the implementation of privacy-friendly solutions is strongly encouraged (i.e. the options of access control and data anonymization/simulation) (see chapters 6-7);
- we encourage the partners to fill in the table presented in the present deliverable (see chapter 7, p. 56-57).

281 Article 7 GDPR.
4. Bibliography

Legislation

Consolidated Version of the Treaty on European Union, O.J. C83/13


European Convention on Human Rights, Council of Europe, 4.11.1950

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS No. 108, 1981


CoE, Committee of Ministers (1973), Resolution (73) 22 on the protection of the privacy of individuals vis-à-vis electronic data banks in the private sector, 26 September 1973

CoE, Committee of Ministers (1974), Resolution (74) 29 on the protection of the privacy of individuals vis-à-vis electronic data banks in the public sector, 20 September 1974

CoE, Amendments to the Convention for the protection of individuals with regard to automatic processing of Personal Data (ETS No. 108) allowing the European Communities to accede, adopted by the Committee of Ministers, in Strasbourg, on 15 June 1999; Art. 23 (2) of the Convention 108 in its amended form

CoE, Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data, regarding supervisory authorities and transborder data flows, CETS No. 181, 2001

**Case-law**

**Court of Justice of the European Union (CJEU)**

C-101/01, Bodil Lindqvist, November 6, 2003

C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU, 29 January 2008

Joined cases C-92/09 and C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, 9 November 2010

C-543/09, Deutsche Telekom AG v. Germany, May 5, 2011

Joined cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, 24 November 2011

C-372/12 and 141/12, M.S. and Y.S., 21.09.2012

C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos and Mario Costeja González, 8 April 2014

C-230/14, Weltimmo, 1.10.2015

C-362/14, Schrems, 6.10.2015


**European Court of Human Rights (ECtHR)**

*M.S. v. Sweden*, 27 August 1977
Klass and Others v. Germany, No. 5029/71, 6 September 1978

Malone v. the United Kingdom, No. 8691/79, 2 August 1984

Leander v. Sweden, No. 9248/81, 26 March 1987

Costello-Roberts v. the United Kingdom, No. 13134/87, 25 March, 1993

Copland v. the United Kingdom, No. 62617/00, 3 April 2007

S. and Marper v. the United Kingdom, Nos. 30562/04 and 30566/04, 4 December 2008

Uzun v. Germany, No. 35623/05, 2 September 2010

Gillan and Quinton v. The United Kingdom, No. 4158/05, 12 January, 2012

Von Hannover v. Germany (No. 2) [GC], Nos. 40660/08 and 60641/08, 7 February 2012

Books

KUNER C., European Data Protection Law, Oxford University Press, 2007


Opinions, reports, handbooks, etc

Article 29 Working Party, Working document on data protection issues related to RFID technology, WP 105, January 19, 2005


Article 29 Working Party, Opinion 8/2010 on applicable law, 16 December 2010

Article 29 Working Party, Advice paper on special categories of data (“sensitive data”), April 20, 2011


Article 29 Data Protection Working Party, WP 202, Opinion 02/2013 on apps on smart devices, February 27, 2013

Article 29 Working Party, WP 203, Opinion 03/2013 on purpose limitation, April 2, 2013


Article 29 Working Party, WP 216, Opinion 05/2014 on Anonymisation Techniques, April 10, 2014

Article 29 Working Party, ANNEX - health data in apps and devices, February 5, 2015


COM (90) 314 final, September 13, 1990, (commentary on Article 2)


Délibération n. 01-011 du 08 mars 2001, Délibération portant adoption d’une recommandation sur les sites de santé destinés au public


European Data Protection Supervisor, Opinion 1/2015, Mobile Health – Reconciling technological innovation with data protection, May 21, 2015


Hogan Lovells, Chronicle of data protection, *The Final GDPR Text and What It Will Mean for Health Data*, January 20, 2016


OECD, *Recommendation concerning Guidelines governing the protection of privacy and transborder flows of personal data*, 23 September, 1980
