A Demonstration of 4D Digital Avatar Infrastructure for Access of Complete Patient Information

Project acronym: MyHealthAvatar

Deliverable No. 11.2
Survey on strengths and weaknesses of the European data protection framework in supporting the patient in scenarios like MyHealthAvatar

Grant agreement no: 600929

Dissemination Level		
PU	Public	**X**
PP	Restricted to other programme participants (including the Commission Services)	
RE	Restricted to a group specified by the consortium (including the Commission Services)	
CO	Confidential, only for members of the consortium (including the Commission Services)	

COVER AND CONTROL PAGE OF DOCUMENT	
Project Acronym:	MyHealthAvatar
Project Full Name:	A Demonstration of 4D Digital Avatar Infrastructure for Access of Complete Patient Information
Deliverable No.:	D11.2
Document name:	Survey on strengths and weaknesses of the European data protection framework in supporting the patient in scenarios like MyHealthAvatar
Nature (R, P, D, O)[1]	R
Dissemination Level (PU, PP, RE, CO)[2]	PU
Version:	1
Actual Submission Date:	28/02/2015
Editor: Institution: E-Mail:	Prof. Dr. Nikolaus Forgó LUH forgo@iri.uni-hannover.de

ABSTRACT:
This Deliverable presents an analysis of position papers by different stakeholders such as patient organisations, regulatory authorities and researchers on the strengths and weaknesses of the planned General Data Protection Regulation in regards to the development of patient-centred health information in electronic format.
Moreover, the Deliverable shows the results of a conducted survey on the necessary steps to foster the development of digital avatars in the best interest of the individual patient.

[1] **R**=Report, **P**=Prototype, **D**=Demonstrator, **O**=Other

[2] **PU**=Public, **PP**=Restricted to other programme participants (including the Commission Services), **RE**=Restricted to a group specified by the consortium (including the Commission Services), **CO**=Confidential, only for members of the consortium (including the Commission Services)

KEYWORD LIST:
Survey, stakeholders, General Data Protection Regulation, strengthens, weaknesses

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 600929.

The author is solely responsible for its content, it does not represent the opinion of the European Community and the Community is not responsible for any use that might be made of data appearing therein.

MODIFICATION CONTROL			
Version	**Date**	**Status**	**Author**
0.1	01.09.2014	Draft	Prof. Dr. Nikolaus Forgó, Dr. Marc Stauch, Dipl.-Jur. Sarah Jensen
0.2	01.02.2015	Draft	Dr. Marc Stauch, Dipl.-Jur. Sarah Jensen, Ass.-iur. Alan Dahi
0.3	10.02.2015	Draft review	Prof. Dr. Norbert Graf (USAAR), Prof. Dr. Feng Dong (BED)
0.4	15.02.2015	Pre-final draft	Prof. Dr. Nikolaus Forgó, Dr. Marc Stauch, Dipl.-Jur. Sarah Jensen, Ass.-iur. Alan Dahi
1.0	28.02.2015	Final	Prof. Dr. Nikolaus Forgó, Dr. Marc Stauch, Dipl.-Jur. Sarah Jensen, Ass.-iur. Alan Dahi

List of LUH contributors

- Prof. Dr. Nikolaus Forgó
- Dipl.-Jur. Sarah Jensen
- Ass. iur. Alan Dahi
- Dr. Marc Stauch

Contents

1 Executive Summary

This Deliverable provides an overview of the opinions of relevant European stakeholders on the draft General Data Protection Regulation with a particular focus on how it might affect the development of patient-centred health information in electronic format, i.e. digital avatars. Amongst the stakeholders are patient organisations, regulatory authorities, and researchers, but also consumer and industry associations.

The Deliverable reveals that the stakeholders in general welcome an overhaul of the current data protection framework and the potential for harmonisation a regulation would bring. However, they also warn that some issues need to be considered, e.g. the issue of broad consent and (administrative) obligations for data controllers that could be seen as detrimental to research and not necessary for data protection purposes.

In addition to evaluating published position papers, we contacted stakeholders who were thematically particularly involved with the subject matter of digital avatars and data protection.

2 Introduction

This Deliverable seeks to give an overview of how stakeholders perceive the strengths and weaknesses of the European data protection framework with an assessment of its impact on the development of patient-centred health information in electronic format (so-called digital avatars).

The methodology chosen for this survey was to analyse the position papers of various stakeholders on the planned EU Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data[3] ("General Data Protection Regulation" - GDPR).

The stakeholders include, inter alia, patient organisations, regulatory authorities and research groups. The GDPR is currently in the ordinary legislative process and is awaiting its second reading in the Council. This Deliverable will not focus on the current Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("Data Protection Directive" – the Directive), because D11.1 already describes the legal and ethical framework of MyHealthAvatar, and therefore also the Directive.

As a first step in this Deliverable, we will present the opinions of stakeholders on the planned GDPR for a selection of issues. We will not only take into account those position papers that discuss the current version by the European Parliament (which accepted the version by the LIBE committee vote from October 2013), but also those that focus on the original draft by the European Commission from January 2012.

The overview should help us understand the legal issues that might affect digital avatars and whether they would foster or harm MyHealthAvatar.

As a second step, we present the opinion of stakeholders we contacted on which aspects of the GDPR need to be addressed to foster the development of digital avatars that are in the best interests of patients. The survey and its responses are presented in Appendices 2 and 3, respectively. It should be noted that, given the complexity of the issues, only stakeholders with a particularly close connection with the issues were contacted. Additionally, because of ongoing delays in the EU legislative process and uncertainty surrounding the text's ultimate version, the survey was delayed. As a result, it is to a certain degree premature to anticipate the precise effects the GDPR will have on digital avatar infrastructures. Consequently, the survey and its responses were formulated in a more general manner. Many stakeholders nevertheless felt that they would rather wait for the GDPR's final form to emerge before answering the questions. Future replies will be considered and reported during the course of the project.

[3] See http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf for the version following the LIBE Committee vote.

3 Stakeholders

The aim of this Deliverable is to produce an overview of the necessary steps in order to promote, from a legal perspective, the development of digital avatars in the best interest of the user.

The successful development of digital avatars as a medical tool that users will willingly turn to will depend not only on having a technologically functioning framework, but also on whether users feel comfortable with the system, and whether the European economy sees sufficient chances in digital avatars to invest resources in their development. All of these aspects are influenced by the law. What the law permits, prohibits, encourages or discourages will have a pronounced effect on how individual stakeholders approach the issue of digital avatars.

Because of the multitude of stakeholders who would play a substantial role in the development, use and promotion of digital avatars, we evaluated the position papers of stakeholders from different backgrounds. The backgrounds represented by stakeholders include information technology and digital rights, medical research and practice, social insurance and private insurance, governmental health organisations, government data protection authorities, and consumers.

For example, commercial enterprises might feel that the legal risks outweigh the possible financial rewards that can be reaped by pursuing digital avatars. In such a case, digital avatars will not find –at least in the private sector– any backing. It would then be up to the state to push their development, even if against the difficulties of a possibly hostile legal situation.

Medical researchers are important stakeholders, too, because one of the benefits of digital avatars would be that the information collected could eventually be provided to benefit research, subject to the user's consent.

Physicians are another very important group of stakeholders. Data could not only be provided by the user, but, if the user is willing, data could also be provided by the physician, e.g. data collected after an examination could be uploaded to the digital avatar for future reference.

Finally, the acceptance by consumers will greatly depend on the legal framework behind digital avatars. For example, will the consumer feel that their data is safe – both from a legal and technical point of view. As illustrated in Deliverable 11.1, this will to a great extent depend on whether data can only be stored and accessed (certain exceptions, e.g. for emergencies, notwithstanding) if the patient gives permission to do so.

The following are the stakeholders whose position papers on the upcoming GDPR were evaluated. They represent a cross-section of the above-mentioned stakeholder categories.

BFB (Bundesverband der Freien Berufe) is the German association of liberal professions.[4] We evaluated the BFB's position paper because, for example, physicians belong to the liberal professions. Physicians will play a key role in the use of digital avatars, and can provide valuable input on issues that might affect them.

BPC (Belgian Privacy Commission) is Belgium's data protection authority[5] provide a regulatory organisation's opinion on issues surrounding the GDPR.

BITKOM represents Germany's IT, telecommunications and new media industries,[6] which would be some of the main private industries active in the development of digital avatars.

CDT (Center for Democracy and Technology) is an NGO working to preserve the user-controlled nature of the internet and support freedom of expression,[7] and thus analyse the GDPR from a civil-rights perspective.

CEDPO (Confederation of European Data Protection Organisations) represents a number of data protection organisations and aims to promote the role of the Data Protection Officer as well as providing advice on data protection and working towards harmonising data protection in Europe.[8] CEDPO offers insight into the practical data protection aspects that would need to be considered.

COCIR is the European trade association of the medical imaging, health ICT and electro-medical industries,[9] and thus represents an important industry with regards to digital health avatars.

DIGITALEUROPE represents Europe's digital technology industry,[10] another industry with a clear interest in the potential uptake on PHR platforms, and their associated tools and apps, and that can provide valuable input regarding the development of digital avatars.

---

[4]See http://www.freie-berufe.de/. The position paper can be found here: http://www.freie-berufe.de/fileadmin/bfb/3_Presse/3_Stellungnahmen-und-Positionspapiere/Stellungnahmen/2013/BFB_Stellungnahme_vom_22._Februar_zur_Datenschutzgrundverordnung__englische_Version.pdf.

[5] See http://www.privacycommission.be/. The position paper can be found here: http://2014.privacyforum.eu/programme/apf-position-papers-edition.pdf/download.

[6] See http://www.bitkom.org/en/about_bitkom/42611.aspx. The position paper can be found here: http://www.bitkom.org/files/documents/reddot.pdf.

[7] See https://cdt.org/about/. The position paper can be found here: https://cdt.org/insight/cdt-analysis-of-the-european-commissions-proposed-data-protection-regulation/.

[8] See http://www.cedpo.eu/pages/114336/About_CEDPO.html. The position paper can be found here: https://www.gdd.de/downloads/materialien/internationales/CEDPO_1.Paper_final.pdf/.

[9] See http://www.COCIR.org/index.php?id=4. The position paper can be found here: https://dataskydd.net/sites/default/files/wp-content/uploads/2013/01/COCIR-position-paper-on-the-General-Data-Protection-Regulation-_Final_25-October2012.pdf.

[10] See http://www.digitaleurope.org/Aboutus.aspx. The position paper can be found here: http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=549&PortalId=0&TabId=353.

Ecommerce Europe represents European companies selling products and services online[11] Digital avatars would also be provided online, and frequently by private industry, so that Ecommerce Europe's stance on the GDPR should be considered.

EDRi (European Digital Rights) is an association of digital civil rights organisations with the objective to promote civil rights in the field of information and communication technology[12] that sheds light on the civil rights issues the GDPR might raise.

ENCR (European Network of Cancer Registries) was established within the Europe Against Cancer Programme framework of the European Commission and promotes collaboration between cancer registries.[13] Digital avatars can provide valuable information to cancer registries, which is why ENCR's position paper on the GDPR was evaluated.

EPF (European Patients' Forum) represents European patients' groups in public health and health advocacy, for example for specific chronic diseases.[14] Patient groups are a further stakeholder that could benefit from the data collected by digital avatars, as the patient's involved in such organisations are frequently very willing to share data amongst each other and with researchers.

EPHA (European Public Health Alliance) is an association of public health NGOs, patient groups, health professionals, and disease groups,[15] i.e. all stakeholders who are at the core of digital avatars.

ESIP (European Social Insurance Platform) is a forum for national social security institutions in Europe.[16] It is quite possible that social security institutions will be interested in adopting digital avatars as a method to increase efficiency of health care.

ESMO (European Society for Medical Oncology) represents medical oncologists and advocates a multidisciplinary approach to cancer treatment. It also supports continuing

[11] See http://www.ecommerce-europe.eu/about. The position paper can be found here: http://www.ecommerce-europe.eu/stream/ecommerce-europe-position-paper-data-protection.

[12] See https://EDRi.org/about/. The position paper can be found here: https://edri.org/files/1012EDRi_full_position.pdf.

[13] See http://www.encr.eu/index.php/who-we-are/about-us. The position paper can be found here: http://ieaweb.org/wp-content/uploads/2012/12/2012-10-5-ENCR-EUROCOURSE-Position-paper-on-the-proposed-EU-Data-Protection-Regulation.pdf.

[14] See http://www.eu-patient.eu/About-EPF/whoweare/. The position paper can be found here: http://www.eu-patient.eu/Documents/Policy/Data-protection/Data-protection_Position-statement_10-12-2012.pdf.

[15] See http://www.epha.org/IMG/pdf/epha_Leaflet_2011.pdf. The position paper can be found here: http://www.epha.org/IMG/pdf/EPHA_position_data_protection_Oct2012_final.pdf.

[16] See http://esip.eu/?q=aboutus. The position paper is available here: http://esip.eu/files/AIM-ESIP%20Position%20Paper%20on%20Data%20Protection.pdf.

medical oncology education and training.[17] ESMO was selected because of the benefits for research and treatment in the field of cancer that digital avatars could provide.

ESNG (European Social Networks Group) represents European social networks and advocates for clear rules and regulations and a strengthened self-regulatory system.[18] Digital avatars can be seen as a type of health-centred social network, either standalone or by linking with existing social networks, which is why ESNG's position paper was evaluated.

EUROCHAMBRES is an association of national and transnational chambers of commerce and industry in Europe.[19] Digital avatars will not only be a health tool, they will also be used by private industry as part of the market economy. Chambers of commerce and industry can provide relevant insight.

EUROCOURSE (Europe against Cancer: Optimisation of the Use of Registries for Scientific Excellence) and the ENCR Working Group is an FP7 project aiming at improving the use of cancer registries in Europe,[20] and as such can also provide an interesting point of view with regards to the GDPR and its effect on the important research resource of cancer registries.

ICO (Information Commissioner's Office) is the UK's independent data protection authority.[21] ICO provides the UK's regulatory body's assessment of the GDPR.

IMS Health is a company that collects data from European hospitals, general practices and pharmacies in order to better understand patient care in Member States. Its databases are used by industry, governments, regulatory bodies, academia and patient organisation.[22] It is a good representative of how private industry could use the data collected by digital avatars.

---

[17] See http://www.esmo.org/content/download/8906/178633/file/ESMO-Member-Benefits-Brochure-2015.pdf, p. 5. The position paper can be found here: http://www.esmo.org/Policy/Political-Initiatives/EU-General-Data-Protection-Regulation/ESMO-Position-Paper (Annals of Oncology 25, 2014, pp. 1458-161).

[18] See http://esng.eu/about-esng/. The position paper can be found here: http://esng.eu/wp-content/uploads/2012/08/120416_EUROPEAN-SOCIAL-NETWORKS-POSITION-PAPER.pdf.

[19] See http://www.EUROCHAMBRES.be/Content/default.asp?pagename=WhoWeAre. The position paper can be found here: http://www.EUROCHAMBRES.be/objects/1/Files/PositionPaperDataProtectionRegulation.pdf.

[20] See http://www.eurocourse.org/. The position paper can be found here: http://ieaweb.org/wp-content/uploads/2012/12/2012-10-5-ENCR-EUROCOURSE-Position-paper-on-the-proposed-EU-Data-Protection-Regulation.pdf.

[21] See https://ico.org.uk/about-the-ico/who-we-are/. The position paper can be found here: https://www.yumpu.com/en/document/view/35557670/tnrbd/1.

[22] See http://ec.europa.eu/justice/policies/privacy/docs/lawreport/paper/imshealth_en.pdf, p. 1. The position paper can be found here: http://ec.europa.eu/justice/policies/privacy/docs/lawreport/paper/imshealth_en.pdf.

Insurance Europe is a federation of Member State insurance associations that represent insurance and reinsurance companies.[23] Insurances will be interested in the data collected by digital avatars.

NHS Confederation (National Health Service Confederation) is the UK's umbrella organisation of its publicly funded health care systems.[24] The NHS provides a governmental health care approach to the GDPR.

Science Europe is an association of European research funding and performing organisations with the goal of fostering research in the European Research Area.[25] Digital avatars are still very much at the forefront of cutting edge research, so that the opinion of research organisations on the GDPR will help assess any issues that might inhibit research.

TMF (Technology, Methods, and Infrastructure for Networked Medical Research) represents networked medical research in Germany and serves as a platform for interdisciplinary exchange for organisational, legal and ethical, and technological problems in medical research.[26] Its assessment of the GDPR is therefore more holistic in nature and indeed covers all the aspects that surround digital avatars.

[23] See http://www.insuranceeurope.eu/about-us. The position paper can be found here: http://www.insuranceeurope.eu/uploads/Modules/Publications/insurance_europe_key_messages_on_the_european_commission%27s_proposed_general_data_protection_regulation.pdf.

[24] See http://www.nhsconfed.org/. The position paper can be found here: http://www.nhsconfed.org/~/media/Confederation/Files/public%20access/Position_Paper_Genera_%20Data_%20Protection_Regulation_20121116EZ.pdf.

[25] See http://www.scienceeurope.org/about-us/about-us-full/. The position paper can be found here: http://www.scienceeurope.org/uploads/PublicDocumentsAndSpeeches/SE_DPR_Position_FIN.pdf.

[26] See http://www.tmf-ev.de/EnglishSite/AboutUs.aspx. The position paper can be found here: http://www.tmf-ev.de/Desktopmodules/Bring2Mind/DMX/Download.aspx?EntryId=25118&PortalId=0.

4 The current situation and the planned General Data Protection Regulation

4.1 General Overview

The European data protection regime is currently being revised. While the applicable Data Protection Directive[27] constitutes the main data protection instrument in the EU (see D11.1 for further details in terms of the regulations), lawyers feel that the central components of European Data Protection need to be revised for several reasons.

One major issue is that the Directive is now almost 20 years old – it dates from 1995 – and that it cannot provide a legal framework adapted to new technical developments and their challenges on data protection law.

Another problem is that a directive leaves scope for its implementation, which leads to the fact that currently each of the 28 Member States has its own law (based on the Data Protection Directive) and that the data protection levels across the EU diverge from each other.

In contrast, a regulation is self-executing and in theory does not require any implementing measures, which means that a regulation could lead to a harmonized level of data protection among all 28 Member States – if it does not provide Member States with the option of enacting their own laws on certain issues.

On 25 January 2012, the EU Commission presented the first draft of the GDPR[28]. It sparked a debate and many stakeholders published position papers in which they criticised various parts of it and suggested improvements.

The EU Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE)[29] took these position papers into consideration and presented a report with many proposed amendments in January 2013. Parts of this report were adopted in an unofficial consolidated version passed by the LIBE on 21 October 2013. This version was accepted by the plenary of the European Parliament on 12 March 2014 and is as of now the basis for further negotiations.

The general objective of the GDPR is not only to harmonise data protection throughout the EU, but also to establish data protection regulations fitting for a Digital Single Market. It also

[27] Directive 95/46/EC, see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML.

[28] See http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf.

[29] The Committee on Civil Liberties, Justice and Home Affairs protects within the Union citizens' rights, human rights and fundamental rights which are laid down in the Treaties and in the Charter of Fundamental Rights of the European Union. Moreover, it deals with issues of protection of personal data.
See http://www.europarl.europa.eu/committees/en/libe/all-announcements.html for further information.

seeks to establish a European Data Protection Board to ensure the harmonised application of data protection law and to prevent a “race to the bottom”.

The concept of privacy by design/by default focuses on the idea that beyond a pure legal protection of privacy, also data processors and producers of IT systems must incorporate privacy into their products and services. Other approaches that also have to do with the technical aspects of privacy protection are the principle of data minimisation and the right to erasure (also called the right to be forgotten).

The right to erasure refers to the fact that it is hard for individuals to understand which information about them is available on the internet, and that individuals often do not feel properly equipped to communicate their request for the deletion of their personal data to big companies such as Google, Facebook, etc. The planned right to erasure is criticised by some lawyers out of the worry that its implementation could unilaterallyy restrict the freedom of the press, of expression and of information.

Furthermore, 19 definitions are put forward in Article 4. What is new is that Article 4 Nr. 2a defines pseudonymous data and Recital 23 anonymous data. By this it is hoped to create incentives to use pseudonymous or even anonymous data instead of directly identifiable data.

Moreover, the data subject’s control over the data processing shall be increased by the notion of the rights to information and transparency; additionally, the notion of explicit consent is planned.

Furthermore, a one-stop-shop shall be established meaning that citizens shall be able to turn to a single Data Protection Authority where problems or questions arise.

Chapter V is characterised by the principle that the transfer of personal data to third countries shall only be legally possible if there is a legal basis in the GDPR. Consequently, if a foreign company targets European consumers, European data protection law should apply, even if the actual data processing occurs outside of the EU. An example would be a US firm using Amazon’s cloud with US-based servers, but targeting consumers in the EU.

Since the Treaty of Lisbon entered into force in 2009, the European Union does not legally comprise the three pillars[30] anymore. Therefore, it was legally possible to adopt sanctions in case of illegal data processing in the draft of the GDPR.

[30] The “European Community pillar” on economic, social and environmental policies; the “common foreign and security policy pillar"; and the third pillar on “police and judicial co-operation in criminal matters”.

4.2 *Key legal points for analysis of the planned GDPR*

This Deliverable does **not** seek to analyze and summarize **all** the planned changes of the GDPR, but will rather focus on the major points that could influence digital health projects such as MyHealthAvatar.

Therefore, we will analyse various position papers on the following key legal aspects: harmonisation, the definition of anonymous and pseudonymous data, the notion of consent, and the interaction between Articles 9, 81 and 83 dealing with the processing of data concerning health and the processing for scientific research purposes, but also the right to erasure, the general prohibition on profiling, and finally the transfer of personal data beyond EU borders.

Harmonisation is an important issue because any digital avatar will likely be used not only by a single Member State, but European-wide through the internet. This means that potentially a number of jurisdictions will need to be evaluated. Harmonisation would greatly facilitate legal compliance.

The definitions of anonymous and pseudonymous data play a crucial role for digital avatars because any data that might be shared with third parties, for example with medical researchers or government organisations for statistical reasons, might frequently be in the form of either pseudonymous or anonymous data.

The notion of consent is the ethical and legal keystone of the European data protection framework. Processing of a data subject's data is first and foremost always conditional on consent, even if there are exceptions.

The interaction between the Articles 9, 81 and 83 is essential to the functioning of digital avatars because the personal data collected will most typically be of a health nature and hence sensitive data. Articles 9, 81 and 83 deal with the processing of such data and its use for scientific research purposes.

Following the recent decision on the so-called "right to be forgotten", the general public is now very much aware of its right to erasure. Also, considering the sensitive nature of the data collected by digital avatars, but also its potential importance for medical research, the right is important.

Similarly, because of the sensitive nature data and the risks that emanate from the availability of such data, for example with regards to decisions taken against the individual based on the data, the general prohibition on profiling is another key aspect that needs to be considered.

Finally, the internet-based nature of digital avatars will mean that data can easily be transferred beyond EU borders, so that this issue also merits evaluation.

5 Opinions of stakeholders

This section will provide an overview of the points discussed above (section 4.2).

5.1 Harmonisation of data protection in the EU

The currently applicable Data Protection Directive means each Member State has its own data protection laws, because directives need to be implemented into national law.

Directives also grant a certain amount of leeway in their implementation, which means that there are numerous different rules at the national level that are not laid down by the Data Protection Directive. For example, § 28a and § 28b of the German Federal Data Protection Act (BDSG)[31] cover the data transfer to credit agencies and scoring. A consequence of this leeway is that data protection levels across the EU differ.

Moreover, there is no single European institution tasked with protecting citizens' personal data – rather, there are autonomous and independent national data protection supervisory authorities.

In contrast, a regulation is self-executing and does not require any implementing measures. This means that a regulation would lead to a harmonized level of data protection among all 28 Member States, albeit only if the regulation does not provide Member States with the option of enacting their own laws on certain issues (which might actually be the case in the GDPR).

One worry with this is that Member States that currently have a higher level of data protection than the GDPR offers would suffer from a drop in the level of their data protection. Despite this, the stakeholders whose position papers we analyzed say that they welcome the adoption of harmonized data protection rules. Harmonization would in principle lead to easier compliance for intra-EU projects. No longer would a multitude of Member State data protection laws need to be considered.

5.1.1 Positions

Stakeholders who are more business oriented generally welcome harmonisation because of reduced transaction costs. For example, **ESNG** calls the harmonization efforts *"a milestone on the path to greater equality of competition and opportunity"* [32] and **DigitalEurope** remarks that a one-stop regime would lead to a more efficient and streamlined regulatory framework.[33] **EUROCHAMBRES**[34] and **Insurance Europe**[35] are also in favour of harmonising the EU data protection framework.

[31] See http://www.gesetze-im-internet.de/bdsg_1990/.

[32] ESNG, p.2.

[33] DigitalEurope, p. 8.

[34] EUROCHAMBRES, p. 1.

[35] Insurance Europe, p. 2.

Stakeholders who are more research oriented generally also welcome the harmonisation of European data protection law. **CEDPO** states that harmonisation is essential for a data protection framework that is both effective and economically reasonable.[36] **COCIR**[37], the **NHS**[38] and **TMF**[39], who each discuss the GDPR with a focus on health research, all welcome harmonisation. For example, **TMF** is of the opinion that harmonisation will make data protection easier and increase legal certainty, particularly for *"integrated projects at a European level."*[40]

There are still critical voices, however. For example, **EUROCOURSE and ENCR Working Party** jointly analysed the Parliament's First Draft from a health research point of view. They agree that a "*more harmonised regime could strengthen the possibilities of data sharing across the EU in the sense of assembling data in pan European epidemiological research projects*"[41], but also warn that a harmonisation of data protection could pose a threat to research in the field of public health and public health itself[42].

They note that there are "*crucial differences in approaches to research and in research cultures across the Member States*",[43] and argue that any harmonisation must "*protect the capacity for research done to protect public health, monitoring of health care and the safety of health interventions*".[44] Otherwise, harmonization could lead to less data being shared because of difficulties in collecting data at the national level. This would weaken European research.[45]

The main concern in this context is not harmonisation per se, but rather that the regulation removes exemptions to explicit consent in public health monitoring and research.[46] The topic of "explicit consent" is also highly debated in several other position papers and is therefore discussed in a separate chapter.

5.1.2 Effect on digital avatars

A regulation and thus the potential for a European-wide harmonised legal framework would foster the development of electronic patient-centred health information. Harmonization would mean that it would no longer be necessary to have costly and cumbersome analyses of multiple national legislation, nor would there be a multitude of differing legal requirements that would need to be adhered to from a digital avatar provider (however only if the regulation does not permit national exceptions).

[36] CEDPO, p. 3.

[37] COCIR, http://www.COCIR.org/site/index.php?id=113.

[38] NHS, p. 1.

[39] TMF, p. 6.

[40] Ibid.

[41] EUROCOURSE AND ENCR WORKING PARTY, p. 5.

[42] Ibid, p. 3.

[43] Ibid, p. 5.

[44] Ibid, p. 4.

[45] Ibid, p. 3.

[46] Ibid, p. 3.

On the other hand, there is also the fear that citizens living in Member States that had a higher level of data protection before the GDPR is enacted could be put off by the perceived lower level of protection of the GDPR. However, it is unlikely that the GDPR will actually offer a lower level of data protection than the Directive mandates. One of the tasks of Member States and the EU will be to show that the GDPR is a step forward and not a step back – the European public would hopefully feel comfortable using personal health records such as MyHealthAvatar from a data protection and privacy perspective.

Consequently, harmonisation will likely have a positive effect on the development of digital avatars.

5.2 Definition of anonymous and pseudonymous data

The basic principle of the Data Protection Directive is that it only applies when personal data is processed.

This principle is also stipulated by the GDPR. Article 2 states that the *"Regulation applies to the processing of personal data wholly or partly by automated means, irrespective of the method of processing, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."*

According to Article 4 (2) of the Parliament's version of the GDPR, personal data *means "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, unique identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social or gender identity of that person".*

Recital 23 explains how to determine whether a person is identifiable:

"The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify or single out the individual directly or indirectly. To ascertain whether means are reasonable likely to be used to identify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development."

Recital 23 continues that "*the principles of data protection should therefore not apply to anonymous data, which is information that does not relate to an identified or identifiable natural person. This Regulation does therefore not concern the processing of such anonymous data, including for statistical and research purposes."* In other words, anonymous data is not personal data. Consequently, it does not fall within the scope of the GDPR.

Considering that Article 4 GDPR has the heading "Definitions" and establishes 18 definitions, of which anonymous data is not one, one could criticise that the recital's (non-binding) definition of anonymous data is too opaque for non-lawyers. The fact that the definition is mentioned only in the penultimate sentence of recital 23 does not help either.

5.2.1 Positions

TMF qualifies the definition of anonymous data as "*imprecise*"[47] because *"Recital 23 merely states that the 'principles of data protection […] should not apply to data rendered anonymous in such a way that the data subject is no longer identifiable'. There is no clearer indication that the right to data protection does not apply to data as long as it is considered anonymous."*[48] Additionally, TMF notes that according to the GDPR the identifiability assessment should not only take the state-of-the art into consideration, but also the direction in which technology is likely to develop. TMF argues that the latter requirement should be dropped because making realistic future projections is virtually impossible.[49]

Also, while TMF welcomes the new definition of "pseudonymisation" because it *"is a widespread [research] tool with a good track record that promotes data efficiency*", they criticize that because anonymous data isn't clearly defined the two concepts cannot be clearly differentiated[50].

The TMF paper also discusses the concept of "relative personal data". It argues that if the concept is to include knowledge available to any entity, in other words "*all global knowledge*", as can be interpreted by the GDPR's statement in recital 23 that the means likely to be used include those "*by the controller processing or by any other person*", then the definition of personal data could be widened to an unacceptable extent. On the other hand, TMF notes that by recital 23's reference to the means likely to be used, the GDPR might actually intend to effect a personal restriction of the concept. Consequently, TMF calls for a clear definition of the concept of relative personal data for the sake of legal certainty for medical and other research.[51]

Similarly, **EDRi** is of the opinion that recital 23 is not concrete enough and calls for a clearer understanding of the term "identifiable": *"Data are often presumed non-identifiable, or anonymous while it in fact still traces back to an individual. Personal data should not be regarded anonymous if the data can still be de-anonymized. 'Masking out' or depersonalization of personal data are valuable security measures, but such measures should not be used to determine whether data are personal data or not. Recitals 23 and 24 should reflect this view point more clearly*".[52]

[47] TMF, p. 7 et seq.

[48] Ibid, p. 10.

[49] Ibid.

[50] Ibid.

[51] Ibid, pp. 10 et seqq.

[52] EDRi, p. 3.

Ecommerce Europe goes a step further and calls for the introduction of a new provision in article 4 that would explicitly state that anonymous data is not personal data.[53] Overall, though, Ecommerce Europe is generally appreciative of the new concepts and definitions, and believes they may adequately balance business and consumer interest, but joins in the criticism that their scope is not yet sufficiently defined to be of proper use.[54]

Science Europe[55] and **COCIR**[56] also both recommend excluding anonymised data explicitly from the scope of the Regulation.

Along the same lines as "anonymous data", the concept of "pseudonymous data" is highly debated.

Article 4 (2a) defines "pseudonymous data" as "*personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organizational measures to ensure non-attribution*".

Contrary to anonymous data, pseudonymous data is personal data (as defined in Article 4 (2)), thus the rules stipulated in the GDPR would apply.

BPC speaks out clearly against the introduction of the new notion of pseudonymous data into the regulation since it *"might add to the existing problem in distinguishing personal from non-personal data"*[57] and "*would weaken the protection granted to individuals, especially if exemptions for pseudonymous date [sic] are voted."*[58] The BPC argues that data pseudonymisation should rather only be seen as a technical measure to implement principles such as data security, data minimization, privacy by design and proportionality – all of which can be taken into account when weighing opposing interests.[59]

"For example, article 33.3 e) of the GDPR mentions the process of pseudonymisation as a manner to ensure security of the data: while pseudonymisation is not a method of anonymisation, since it merely reduces the linkability of a dataset with the original identity of a data subject, it can be a useful security measure for the same reasons. Pseudonymisation can also be a way to ensure that data affected by a breach are adequately protected against identification in the context of data breach provisions (articles 31 and 32 of the GDPR)."[60]

[53] Ecommerce Europe: Position Paper, p. 5 et seq.

[54] Ecommerce Europe, p. 5.

[55] Science Europe: Position Statement, p. 5.

[56] COCIR, p. 2.

[57] BPC, p. 6.

[58] Ibid.

[59] Ibid, pp. 4, 6.

[60] Ibid, p. 5.

ICO also believes that having two different types of personal data would be confusing and counterproductive to clarifying what personal and non-personal data actually is. Additionally, the organisation worries that distinguishing pseudonyms from other forms of personal identifiers will be particularly problematic in practice.[61] Another problem with pseudonyms is that some might in actuality not be personal data, for example because any additional information that relates to a single individual no longer exists, so that while individuals could still be distinguished amongst each other, they could still never actually be identified insofar that they could be treated differently.[62]

As a result, ICO argues that the GDPR should recognise only a single type of personal data, but treat different types of identifiers according to the risk they pose for data protection.[63]

BITKOM also criticises the notion of pseudonymous data on the basis that it ignores the proportionality principle as applied to personal data and will therefore not only "*block further development of the majority of new digital products and services*" [64], but also make it impossible to differentiate between merely formal requirements and truly important processes when dealing with one's own personal data: Pseudonymous data would always be treated as personal data, even if the identification process were to require an unreasonable amount of resources.[65]

NHS joins in the call for cutting pseudonymised data out of Article 4 because of the difficulty in creating a definition that can be applied across all sectors.[66]

CDT, too, sees a clear need for clarifying the language in recital 24 *"to ensure that data subjects possess a personal interest in data that is not readily linkable to real-name identity."*[67]

EPF remarks that "*the degree of anonymity of the data*" must be made clear to the patients when seeking consent.[68]

5.2.2 Effect on digital avatars

It is arguable whether the notion of pseudonymous data would really change the already existing system of needing to distinguish between anonymous data and personal data. Several Member States[69] have already implemented the category of "pseudonymous data"

[61] ICO, p. 2.

[62] Ibid.

[63] Ibid, p. 2 et seq.

[64] BITKOM, p. 2.

[65] Ibid.

[66] NHS, p. 1.

[67] CDT, p. 1.

[68] EPF, p. 6.

[69] E.g. the German Federal Data Protection Act ("BDSG") defines in section 3 paragraph (6a) pseudonymising as "*replacing a person's name and other identifying characteristics with a label, in order to preclude identification of the data subject or to render such identification substantially difficult*".

and the Article 29 Working Party[70] provides guidance in their opinion 4/2007[71] on how this category of data should be understood.

Under the current regime of the Data Protection Directive, pseudonymous data is personal data, so that in this respect the draft GDPR is not necessarily different to Member State implementations.

However, it could be problematic that the definition stipulated in the current version of the GDPR leads to uncertainties whether data is personal or not.

Looking at MyHealthAvatar, the use of anonymous and pseudonymous data will be relevant probably only within the development phase and the non-public validation phase. Often, for example, the initial building of tools can take place using anonymised or even synthetic data.

When opening the platform to the public for validation, it is questionable if it would make sense to continue to use pseudonymous data. Probably, the user would want to test the platform to its full extent, which can only happen by using actual personal health and lifestyle data.

5.3 Consent

A further key point that is highly debated in the position papers is the notion of "**explicit**, and **specific** consent". Article 4 (8) defines the data subject's consent as "*any freely given **specific**, informed and **explicit** indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed".*

In the recitals, recital 25 states that *"[c]onsent should be given explicitly by any appropriate method enabling a freely given specific and informed indication of the data subject's wishes, either **by a statement or by a clear affirmative action** that is the result of choice by the data subject, ensuring that individuals are aware that they give their consent to the processing of personal data".*

Originally the draft Regulation, in recital 41, stated the general principle that sensitive and vulnerable data must only be processed when the data subject has given explicit consent, but also that derogations from this principle should be provided for in respect of specific needs, *"in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms"*. This recital was deleted by the LIBE vote, but at the same time

[70] The party is made up under Article 29 of Directive 95/46/EC. According to Article 2 of Directive 95/46/EC it is composed of a representative of the supervisory authority or authorities designated by each Member State and of a representative of the authority or authorities established for the Community institutions and bodies, and of a representative of the Commission. The independent European advisory body aims at the protection of individuals with regard to the processing of personal data.

[71] Opinion 4/2007, p. 18.

Article 81 (2a) was changed to grant Member States the right to provide for exemptions to the consent requirement for research that serves a high public interest, subject to certain requirements, one of them being notifying the Commission of the provisions adopted (cf. Article 81 (3a)).

The position papers analysed very often focused on the topic of explicit and specific consent, in part because the exemptions to the consent requirement provided by the Data Protection Directive are heavily relied upon in research. It is neither always feasible nor practicable to obtain consent from every research subject. No longer having an exemption would likely severely impact the way research is conducted in the EU.

5.3.1 Positions

EPF welcomes the notion of explicit consent[72] and the right to withdraw consent, and is of the opinion that explicit consent should be required as a rule.[73] However, EPF believes "*that there should be legal clarity regarding what explicit consent entails (e.g. whether it should be written consent), and the situations where this type of consent is required or not.*"[74]

EPF is also aware that the concept of explicit consent could raise problems for healthcare activities, e.g. during an average medical consultation, as it would take too much time away from the care of the patient.[75] Therefore, EPF recommends referring to the right to informed consent in the provisions for the definition of data concerning health.[76]

Moreover, EPF advocates that patient organisations need to be involved in the drafting of consent forms at the national level.[77]

While rather a question of specific consent, Article 9 GDPR, EPF also notes the importance of secondary use of patients' health and genetic data and endorses clear consent forms in regard of potential future use of the patient's data.[78]

Article 83 (1) (a) states that personal data may be processed for scientific research purposes without explicit consent[79] only if the purpose "*cannot be otherwise fulfilled by processing data which does not permit or not any longer permit the identification of the data subject*".

The need for explicit consent is also a major point in the position paper published by **Eurocourse and the ENCR Working Party**, relating to the Parliament's first draft of the GDPR. They warn against the idea that public health research can usually also be done only with anonymized or pseudonymized data. They argue that public health research *"often*

[72] EPF, p. 8.
[73] Ibid.
[74] Ibid.
[75] Ibid.
[76] Ibid.
[77] Ibid.
[78] Ibid, p. 9.
[79] EUROCOURSE and ENCR Working Party, p. 8.

*involves the assessment of the risk of disease in which the impact of exposure to a substance (e.g. asbestos) on the risk of disease (e.g. mesothelioma) or consequences of modern technology (e.g. mobile phones) must be measured in very large populations of individual persons over several decades. Disease risks can often only be discovered by research of this type, and it is not possible to do it without access to and repeated linkage of data which must be considered indirectly identifiable according to present standards or simply identifiable*9."[80]

Moreover, Eurocourse and ENCR note that source data (such as from electronic health care records) are sometimes inaccurate and that a check can only be done if researchers can interact with the data sources about individual patients. This is not possible if one-way pseudonymisation is used.[81]

The two organisations also point out that Trusted Third Party constructions are very costly.[82]

With regards to the questionnaire submitted (see Appendix 2), EUROCOURSE felt the legislation to be too complicated to properly answer the questions.

Overall, however, **EUROCOURSE** sees no major problem with digital avatars and consent because the patient decides with whom the data is shared. At the same time, EUROCOURSE points out that for the uploaded health data to be useful for research and innovation it needs to be of a high quality and representative – something that could be an issue considering that is the patient who will be uploading the data and not hospitals, doctors, etc., unless the patient grants them consent to do so. If at the end of the day it is only the patient who uploads the data, digital avatars might not end up being more than a cloud-based diary.

They also point out that if the concept of informed consent is kept as proposed, serious cross-border collaboration will not be possible. As part of its response, EUROCOURSE referred to an article on the reform of the European data protection framework and its impact on public health research.[83] One of the major issues discussed therein is the problem of requiring explicit consent for secondary research and that this would effectively kill cancer registries and epidemiological studies. EUROCOURSE argues that Nordic countries have a long and successful tradition of balancing the interests of the individual against the interests of society in registry-based research, and that the GDPR should learn from this experience.

[80] Ibid, p. 8 et seq.

[81] Ibid, p. 9.

[82] Ibid.

[83] Mette Rye Andersen, Hans H. Storm, "Cancer registration, public health and the reform of the European data protection framework: Abandoning or improving European public health research?, in European Journal of Cancer (2013). DOI: http://dx.doi.org/10.1016/j.ejca.2013.09.005.

Alzheimer Europe, a patient organisation and a stakeholder contacted with regards to the survey, also chose to focus on the issue of consent[84] instead of completing the questionnaire in full. Because of the nature of dementia, the capacity to understand the information provided, i.e. the informed aspect of consent, is one of the topics most important for the organisation. While knowledge or belief that the patient has dementia should be considered as grounds for doubting the capacity consent, it should never be considered proof that the patient is unable to give valid consent. Rather, further testing must be conducted to properly assess the capacity to consent.

EDRi appreciates that the definition of consent would be strengthened by the draft GDPR[85] and that Article 7 (1) stipulates that the controller shall bear the burden of proof regarding having obtained consent.[86] However, some additional changes would enable better protection of users in the online environment, e.g. if the regulation were to clearly state the necessity for a "*clear affirmative action*" for giving consent.[87] Nevertheless, EDRi believes that the criteria of being freely given, specific, informed and explicit are well suited for a "*meaningful consent*".[88]

Ecommerce Europe focuses on the economic aspects of the notion of explicit consent, which could also be relevant for the exploitation phase of MHA. The group is of the opinion that the strict requirements for explicit consent represent an unneeded burden on businesses and consumers that disrupts the current Directive's balance between data protection and business interests. Rather, the requirements for consent should be context-based and take into account the sensitivity of the data being processed and the risks to privacy. Instead of explicit consent, Ecommerce Europe calls for unambiguous consent. In addition, Ecommerce Europe suggests permitting consent to be given through device settings, as this would take both the consumer's interest of user friendly solutions and business's interest in keeping costs down and standardizing the consent process.[89]

Regarding the categories of "pseudonymous data", "encrypted data", and "anonymous data", Ecommerce Europe would prefer to have them fall outside the scope of the draft GDPR and therefore not be subject to the requirement of consent to be processed.[90]

EUROCHAMBRES agrees that requiring explicit consent would not only be costly, but also cumbersome, and that the requirements behind explicit consent are generally excessive. Only with regards to sensitive data does the organisation feel that explicit consent is appropriate.[91]

---

[84] Inter alia http://www.alzheimer-europe.org/Ethics/Ethical-issues-in-practice/Ethics-of-dementia-research/Informed-consent-to-dementia-research/%28language%29/eng-GB?#fragment-2.

[85] EDRi, p. 4.

[86] Ibid, p. 19.

[87] Ibid, p. 4.

[88] Ibid, p. 15.

[89] Ecommerce Europe, p. 6.

[90] Ibid.

[91] EUROCHAMBRES, p. 3.

Additionally, EUROCHAMBRES submits that the burden of proof for given consent should be further specified. With regards to the provision of the draft GDPR that a significant imbalance between parties makes consent invalid, EUROCHAMBRES submits that it will only lead to legal uncertainty in the field and that it should be dropped.[92]

The **NHS European Office** generally agrees with the Commission's approach to consent with regards to healthcare and research, but with the caveat that where health data is processed according to article 81, explicit consent should not be required.[93]

Insurance Europe provides as an argument against the requirement of explicit consent that, for example, mentioning a patient's health problem on an insurance claim or the hospital admission form would mean that, being sensitive data, administrative employees would be unable to process the documents without the patient's explicit consent.[94]

Science Europe in principle agrees with the requirements of informed consent and calls consent the *"basis for trust" and a "key ethical requirement"*. Consequently, *"[i]nformed, specific, explicit consent should be the norm, sought wherever this is possible and where it does not lead to a disproportionate burden that may risk preventing important scientific research from being carried out."* [95] From a practical viewpoint, though, Science Europe also points out that it is not always possible to obtain consent from study participants, for example in the fields of emergency care research, where studies need a very large sample size, or where seeking consent would negatively impact research findings because of an introduced bias. In such cases, ethics committees should be able to decide whether the general consent requirement can be waived.[96]

EPHA believes that a "one-size-fits-all approach" to the issue of consent is inappropriate and that the requirements of consent should take into account the different levels of competency for granting consent and of digital literacy,[97] and is consequently against the general rule that consent should always be explicit.

ESIP believes that explicit consent for health purposes can put the patient in danger. They also argue that for social security organizations, explicit consent should only apply to new contracts and not to existing ones (the organization is apparently under the false impression that the Directive does not require explicit consent for sensitive health data.[98]

[92] Ibid.

[93] NHS, p. 3.

[94] Insurance Europe, p. 3.

[95] Science Europe, p. 5.

[96] Ibid.

[97] EPHA, p.2.

[98] ESIP, p. 5.

IMS Health remarks that the requirement of consent may actually be counterproductive and illustrates this with regards to the Directive. Explaining that the concept of 'processing' is given a very broad scope by the Directive, so that even the act of anonymization itself very likely falls under it, IMS Health posits that organizations are actually discouraged from using anonymization techniques to enhance privacy because, considering that both anonymization and other types of processing require consent, the organization can spare itself the anonymization effort and simply seek consent for other processing.[99]

Regarding the fact that Article 7 (1) places the burden of proof that consent was given on the data controller, **TMF** writes that it is arguable that no proof must be provided that the facts were explained to the data subject, nor of the method to do so, nor what was explained, as Article 7 (1) only talks of proof that consent was given. This in combination with articles 4 (8), 11, and 14 (4) would indicate that prior explanation of the facts is not a condition for effective consent. This can be done afterwards, too, as is the case today (exceptionally) for research on patients admitted as emergencies. However, as a general rule, it would be a departure from how informed consent is understood and practiced today – whether this is what the legislature actually intended is unclear.[100]

Moreover, because (by virtue of Article 7 (4) as revised by the Parliament) consent would only be valid for the period required to process data for the purpose given, effective research demands that giving broad consent must be possible.[101]

5.3.2 Exemptions from consent

Article 7 (4) of the original GDPR excluded consent as a legal basis for data processing in cases of a significant power imbalance between the data subject and the data controller. The **BFB** criticised the rule for invariably denying the patient or client of a liberal professional such as a doctor "*the possibility to give consent for data processing*",[102] even though the data is "*absolutely essential for providing liberal professional services*".[103]

Also **TMF** criticised that it was not sure if the imbalance would also apply to the relationship between patients and the treating doctors and warned that section 4 would "*put the legal certainty of many research projects linked to the treatment of patients at risk*"[104]. Therefore, TMF welcomes dropping it.[105]

For **EDRi**, consent is one of the most important topics. The organisation argues that the current rules on consent are ineffective because technology is now so sophisticated that data subjects are frequently unaware that their data are being collected and processed and

[99] IMS Health, p. 3.

[100] TMF, pp. 13 et seqq.

[101] Ibid, p. 16.

[102] BFB, p. 4.

[103] Ibid, p. 5.

[104] TMF, p. 14.

[105] Ibid.

also to what extent they might be affected thereby. Additionally, any information on the practices of data controllers is mostly given via complicated privacy notices that are moreover rarely read. Finally, controllers often claim consent by using pre-ticked boxes, etc., without data subjects having in actuality given free and informed consent.[106]

Moreover, EDRi feels that consent is given too weak a role amongst the criteria that permit processing and that other options, such as the "legitimate interest" of Article 6 (1) (f) are too permissive. Instead, any processing based in "legitimate interest" should be clearly marked as such and the reasons for doing so should be published.[107]

Regarding the "significant imbalance" exception to valid consent, EDRi advocates introducing a non-exhaustive list similar to the one in the Unfair Contract Terms Directive as a guideline for which situations represent a significant imbalance.[108]

The current LIBE version of Article 7 (4), it should be noted, has dropped this exception, albeit – as noted above – reinforced the requirement for data retention and use to be limited (in the absence of fresh 'reconsent') to the original purposes of collection.

5.3.3 Effect on digital avatars

Under the current regime under the Directive, explicit consent is only necessary for the processing of sensitive data. MyHealthAvatar is designed to store sensitive data, namely "data concerning health" as defined in Article 8 (2) Data Protection Directive. If we take into account the GDPR's planned definition of data concerning health, the broad approach would lead to the fact that probably also lifestyle data, which the user will be able to upload to and store in the platform, would be considered to be sensitive data. Consent would therefore need to be explicit, with or without the introduction of a general requirement for explicit consent.

Only in certain exceptional cases would such data not be sensitive, so the debate could potentially affect digital avatars. Anyhow, the typical user of MHA will register from home before storing personal data in the platform. So it would be necessary for practical reasons and to avoid litigation to obtain explicit consent beforehand.

5.4 Interaction between Articles 4 (12), 9, 81 and 83: The processing of sensitive patient data in the light of scientific research purposes

The interaction between Articles 4 (12), 9, 81 and 83 and thus the processing of sensitive patient data for scientific research purposes is highly debated and frequently at the core of the position papers we analysed. This has to do with the aims and purposes of the organisations that drafted the position papers.

[106] EDRi, p. 14.

[107] Ibid, p. 14 et seq.

[108] Ibid, p. 15.

5.4.1 Article 4 (12)

The GDPR defines data concerning health in Article 4 (12) as *"any personal data which relates to the physical or mental health of an individual, or to the provision of health services to the individual."*

EPF welcomes the inclusion of a comprehensive definition of data concerning health in the Regulation because of the legal clarity it brings. Moreover, because the definition encompasses all data shared by healthcare providers, it also ensures patients' trust.[109]

However, EPF would prefer a definition that encompasses all health services and would therefore endorse the definition *"any information which relates to the physical or mental health of an individual or to the provision of health services and care to the individual"*, aligning it with Recital 26.

Insurance Europe shares the view of many organisations that the definition is too broad because it includes certain administrative data that would need consent to be processed,[110] burdening both consumers and insurers.[111] By way of example, Insurance Europe explains that delays in the pay-out of covered medical expenses could arise.[112]

Therefore, Insurance Europe recommends implementing a clear definition that excludes administrative information and is restricted to clinical and medical information. Otherwise, so Insurance Europe, the current definition would mean that even the "*serial number of a medical device may be considered as 'data concerning health' although it is associated to a medical equipment and not to a data subject.*"

COCIR agrees that the definition is "*too broad*"[113] and recommends that it should be restricted to "*data that can lead to the identification of a data subject*".[114]

Regarding the exploitation stage of MyHealthAvatar, an improved definition of data concerning health could help in understanding when Articles, 9, 81 and 83 apply. This is important because the legal framework regarding data concerning health will differ from that for non-sensitive data.

When storing their data, users should be aware that some data could be of interest to certain third parties such as employers, insurance companies, etc. The consortium should keep in mind that the definition of data concerning health as it is defined in the GDPR is very broad since the wording "*or to the provision of health services to the individual*" widens the scope of the rules dealing with sensitive health data.

[109] EPF, p. 3.

[110] Insurance Europe, p. 3.

[111] Ibid.

[112] Ibid.

[113] COCIR, p. 2.

[114] Ibid.

Regarding the development and validation stages, when experimenting with real data, e.g. to show the benefit of MHA through different use cases, we need to adhere to the rules regarding the processing of data concerning health as stated in Articles 9, 81 and 83 GDPR.

5.4.2 Special categories of data (data concerning health) – Article 9

Article 9 states the basic rule that the processing of special categories of data, e.g. data concerning health, is forbidden unless the data subject has given consent or there is a legal exemption (as specified in Article 9).

According to recital 42, "*[d]erogating from the prohibition on processing sensitive categories of data should also be allowed if done by a law, and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where grounds of public interest so justify and in particular for health purposes, including public health and social protection and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, for historical, statistical and scientific research purposes, or for archive services.*"

So the processing of sensitive data not only requires a legal basis, but also suitable safeguards and a special public interest.

Article 9 more or less corresponds with Article 8 Data Protection Directive, apart from some amendments – for example, genetic and biometric data are not mentioned in Article 8 Data Protection Directive (even if they are nevertheless treated as data concerning health, as recital 26 Data Protection Directive shows).

One of the exemptions foreseen is Article 9 (2) (a), which states that processing is lawful if consent was given "*for one or more specified purposes*". The requirement of a specified purpose is a rejection of the concept of **broad consent**, which is consent given for general, in contrast to specifically, described purposes.

TMF explains that it prefers broad consent to specified consent because the former is the only way cutting-edge research projects involving biobanks, registers and cohorts can function and comply with the law – the goals of such projects are often not clear until the research has already progressed.[115] TMF argues that abandoning the already achieved consensus on broad consent would set back medical research by years.[116]

TMF calls for safeguarding data received through broad consent by involving accredited ethics commissions. The commission would weigh the right of individuals to their personal

[115] TMF, p. 6.

[116] Ibid.

data with the societal interest in research.[117] Introducing this process in the General Data Protection Regulation would help establish a standard across Europe.[118]

Moreover, it can be critical for research projects to "*weigh up freedom of research and the interests of data protection in certain cases*"[119]. The common practice in Germany has shown that "*no major breach of data-protection interests is to be feared*".[120]

TMF also calls for legal backing to the debated concept of "*relative personal reference*", according to which re-identifiable data need only not be re-identifiable to the body receiving it to be considered totally anonymous. This is in contrast to the absolute approach that argues that for data to be totally anonymous, it must generally not be re-identifiable to the party receiving it or to a third party.[121]

EDRi criticises that Member States are given the possibility to enact domestic legislation prohibiting certain processing of sensitive personal data, even if the data subject consented, noting that domestic rules would contradict the planned harmonisation and lead to the fact that some processing would be allowed in some Member States but prohibited in others.[122]

Moreover, EDRi remarks that also Article 9 (2) (g) creates the risk of a lack of harmonisation because "*suitable measures*" to safeguard the rights and interests of the data subject are not defined,[123] but are one of the preconditions for Member States being able to enact a national exemption to the default prohibition of processing of special categories of data.

5.4.3 Processing of personal data concerning health – Article 81

Article 81 applies to the processing of personal data concerning health and Article 83 sets rules for the processing for historical, statistical and scientific research purposes. The interaction of these provisions is critical because it concerns the processing of sensitive health data for scientific research purposes – the case in MyHealthAvatar.

The first paragraph of Article 81 refers to Article 9 (2h), which states that the processing of personal data concerning health is legal without consent of the data subject if the processing is necessary for health purposes and subject to the conditions and safeguards referred to in Article 81.

The mentioned health purposes in Article 81 (1) include:

> (a) the purposes of preventive or occupational medicine, medical diagnosis, the provision of care or treatment or the management of health-care services (...);

[117] Ibid.

[118] Ibid.

[119] Ibid, p. 7.

[120] Ibid.

[121] Ibid.

[122] EDRi, p. 11.

[123] Ibid.

(b) reasons of public interest in the area of public health (...);

(c) other reasons of public interest (...).

Nevertheless, personal data should not be used when the purposes can be achieved without its use, unless based on the consent of the data subject or Member State law.[124]

As far as the participation in scientific research activities in clinical trials is concerned, Article 81 (1c) states that the relevant provisions of Directive 2001/20/EC apply for the purpose of consent.

Where the data subject's consent is required for the processing of medical data exclusively for public health purposes of scientific research, the data subject can give consent for one or more specific and similar research projects, and may also withdraw their consent at any time.[125]

Similarly, where the processing of personal health data is necessary for historical, statistical or scientific research purposes, a requirement is the consent of the data subject but also the conditions and safeguards referred to in Article 83,[126] i.e. that using de-identified data is not possible and that the personal data is kept safe using the highest technical standards.

Article 81 (2a), however, also allows Member States to provide for exceptions to this requirement of consent for research that serves high public interests if that research cannot possibly be carried out otherwise. In such cases, the data must be anonymised - if the research purpose permits the use of anonymised data – and otherwise pseudonymised. Additionally, all necessary measures to prevent unwarranted re-identification of the data subjects must be taken. As always, the data subject has the right to object pursuant to Article 19.

It is intended that the Commission will be empowered to adopt delegated acts further specifying public interest in the area of public health, and also research areas of high public interest.[127]

EPF welcomes that health data benefit from a higher level of protection under the General Data Protection Regulation and remarks that the rules stipulated in Article 9 "*ensure that patient data can be processed for essential purposes, such as the provision of healthcare, public interest [...], for public health and research purposes*".[128]

[124] See Article 81 (1a) GDPR.

[125] See Article 81 (1b) GDPR.

[126] See Article 81 (2) GDPR.

[127] See Article 81 (3) GDPR.

[128] EPF, p. 4 et seq.

EPF believes that "*secondary use of health data is vital to advancing health research*"[129] and was thus very critical of the Commission's initial proposal for the GDPR, because it did not mention public health research in Articles 9, 81, 83. Consequently, because Article 81 of the consolidated version after the LIBE vote now establish rules concerning public health research, even if consent is generally needed, EPF likely welcomes the new rules.

TMF complains that it is not clear how Article 9 and 81 on the one hand and Article 83 on the other apply to each other, and that there is no logic behind the references:[130]

"*Furthermore, the system under articles 9, 81 and 83 is hard to understand even for readers who are practised at comprehending legal texts. While on the one hand art. 9, section 2, h, only allows processing of personal data concerning health in compliance with the provisions in art. 81 and merely for health-related purposes, art. 81, sections 1b, 1c and 2 also regulates the processing of medical data or health-related data for research purposes. However, for research purposes in section 2, i, the underlying art. 9 explicitly and exclusively refers to the provisions of art. 83. Therefore, these provisions would only be relevant if art. 83 referred to art. 81.*"[131]

These difficulties of comprehension not only lead to legal uncertainty, they create *"a huge amount of red tape"*. Therefore, "*unambiguous rules*" are needed in order to foster research.[132]

TMF also states that the "*research limitations are too narrow*", especially because Articles 81 and 83 do not properly balance the rights of individuals to self-determination and the freedom of research. A consequence is that research without consent is prohibited, even in the facility where the patient is being treated.[133]

TMF criticises further that the Member State exemption for research without consent is "*very restrictive*" and "*would undermine the principle of harmonisation of the legal framework which was intended and therefore the added value achievable for research due to international harmonization*".[134]

ESMO worries that the current wording of the draft GDPR may have unintended consequences that may jeopardize the survival of "*retrospective clinical research, biobanking, and population-based cancer registries in the EU.*"[135] The criticism especially concerns the Article 81 (1) (b) wording *"consent may be given for one or more specific and*

[129] Ibid, p. 5.
[130] TMF, p. 5.
[131] Ibid, p. 21.
[132] Ibid, p. 5.
[133] Ibid, p. 6.
[134] Ibid.
[135] ESMO, p. 1458.

similar researches", which could be understood to require a patient's specific consent each and every time new research is performed on already available data and tissue.[136]

Moreover, ESMO points out that the current wording would kill population-based disease registries, because the recording of data would require consent from each individual. Such registries live from collecting the data of each individual of a given population and obtaining consent from every individual would be impossible.[137]

ESMO represents the interests of medical oncology research, so it is not surprising that ESMO is interested in a legal framework that does not impede the data processing of sensitive health data. However, ESMO acknowledges that it is important to protect the privacy of patient data. Its main concern is that the proper balance between protecting the individual's privacy and facilitating research has not been found.[138]

ESMO believes that "*a safe balance between all rights concerned can be achieved*"[139] and emphasises that "*progress in health research [...] must continue in the EU countries*."[140] Therefore, ESMO endorses a 'broad', one-time consent because *"patients should have the right to give once forever their consent for their data and/or tissues to be processed for research purposes"*, while researchers should not be forced to continually seek re-consent whenever new research is planned using already given data and tissue samples.[141]

ESMO stresses that the rights of the patient would be sufficiently protected because they *"will be informed that their data/tissues will be used for future research, and they will be informed about the conditions under which their data and tissues will be stored, making the protection safeguards a part of their consent".*[142]

Consequently, a **broad consent** would give patients the right to "donate" their data for public health research purposes. In contrast, the notion of '**specific' consent** would lead to the fact that researchers then would need to obtain continuous patient re-consent every time new research is carried out and consent would be "*practically unfeasible, time-consuming, administratively burdensome, expensive, and also intrusive into patients' lives even many years after their disease experience*."[143]

EUROCOURSE and ENCR Working Party are worried that Articles 9, 81 and 83 *"may lead to additional legislation (on for example encryption, TTP's or pseudonymisation of data) hampering the possibilities to conduct register-based research in countries proved excellent*

[136] Ibid.

[137] Ibid, p. 1459 et seq.

[138] Ibid, p. 1458 et seq.

[139] Ibid, p. 1459.

[140] Ibid.

[141] Ibid.

[142] Ibid.

[143] Ibid.

in this or imposing bureaucracy in the pursuit of greater legislative coherence across the EU."[144]

According to Eurocourse and ENCR Working Party, it is an "*illusion*" that epidemiological research using record linkage can be done with solely anonymous or pseudonymous data using TTP constructions. For one thing, individuals in very large populations need to be monitored over decades and it is not possible to do so without accessing and linking indirectly or directly identifiable data. Furthermore, the necessary source data, frequently taken from EHRs, can be inaccurate and needs to be checked. The verification process requires researchers to interact with the data sources.[145]

Another point mentioned is the costs of using TTP constructions. The Working Party, while recognising that data security is of the utmost importance, points out that no data breaches have been reported from countries where disease registries have been kept without TTP constructions.[146]

5.4.4 Effect on digital avatars

As pointed out in D11.1, processing of personal data concerning health will take place each time a MHA user stores health data in the platform. Article 81 is thus of central importance – the question is what paragraphs apply and whether they foster or hinder the building and use of patient-centred electronic health information.

Although the system of MHA is designed to help the user take care of their health, Article 81 (1) would not affect MHA because it will be the user who will process the data and not a health professional subject to the obligation of professional secrecy or another person also subject to an equivalent obligation of confidentiality under Member State law or rules established by national competent bodies. No doctor will have access to the stored data unless the user authorises him or her and thus there will be no automatic retrieval or consultation in the meaning of Article 4 (3).

The new paragraph 1b will also not affect systems such as MHA because the user does not store medical data "*exclusively for public health purposes of scientific research*". For the same reason, paragraph 1c does not fit either.

Paragraph 2 is more likely to apply, but its application is still relatively farfetched because primarily the user will not process the data for reasons of public interest. Although it could very well be that the user also wishes physicians and researchers to use the stored information for research purposes in order to solve problems the public is much interested in, the primary focus will be the self-management of health-related questions.

[144] EUROCOURSE and ENCR Working Party, p. 15.

[145] Ibid, pp. 5, 8.

[146] Ibid, p.8.

As a consequence, consent given by the MHA user will be crucial to comply with legal requirements. Consent is not a hindrance to systems like MHA. To the contrary, an appropriate legal framework can help to foster acceptance by the critical mass of users helping the system to become a truly effective resource. The user will trust providers complying with legal (and ethical) requirements rather than those that have been criticized by data privacy activists in the past. Nonetheless, implications for the smooth operation of the platform, and its user friendliness, if specific consent is enacted in the Regulation as a requirement for each distinct act of processing, should be kept under review.

5.5 Right to erasure – Article 17

The draft GDPR foresees the right to erasure. It shall encompass the right of the data subject to demand from the data controller the erasure of personal data relating to themselves and to abstain from further disseminating any such data. This applies also to third parties in regards to links to or copies of and replication of the data. The right may be acted upon by the data subject if, inter alia, the data are no longer necessary for the purposes they were collected or processed for; or where the data subject withdraws consent or the storage period consented to has expired; or where the data subject objects pursuant to Article 19.

The right to erasure is not absolute. Exemptions in accordance with Articles 81 and 83 are foreseen in Article 19 (3).

5.5.1 Positions

BFB acknowledges the so-called rights to be forgotten and to erasure, but warns that too extensive data subject rights might hinder or even endanger professional activity, both legally and financially, and therefore calls for a restriction of the rights.[147]

TMF, in contrast, mentions that Article 17 in general complies with their current recommendations.[148] **EUROCOURSE and ENCR Working Party** only stress that the exemptions must be maintained for epidemiological research to have a future in the EU.[149]

Ecommerce Europe remarks that the “right to be forgotten” already exists in some sense in the current directive, which mandates that personal data may not be stored indefinitely and that individuals have the right to have their data deleted and also the right to withdraw their consent. The new “right to be forgotten” is therefore unnecessary and redundant in light of these rights and rules that would be carried over to the GDPR. As currently proposed, the right to erasure of Article 17 GDPR seems to be more fitting for social networks, but not for ecommerce, where it could create unintended consequences, such as companies needing to develop new data management systems. Additionally, businesses are under the obligation to keep personal data for a number of reasons, such as tax or warranty

[147] BFB, p. 5.

[148] TMF, p. 17.

[149] EUROCOURSE and ENCR Working Party, p. 9.

purposes, that do not harmonize with Article 17 GDPR[150] (even if Article 17 (3) (d)'s exemption "*for compliance with a legal obligation*" would seem to fit the bill.

As a consequence, Ecommerce Europe would rather strengthen existing rights than introduce new ones. In particular, Article 17 GDPR should be dropped in favor of extending the right to have personal data deleted, for example by incorporating the right of erasure of any links to the personal data and copies thereof to be deleted.*[151]*

EDRi draws in general the same conclusions as Ecommerce Europe, and points out that making online services liable for content over which they have no control would lead to the development of technical measures such as filtering and blocking techniques that would by their very nature negatively impact the privacy of individuals.[152] EDRi suggests extending the scope of Article 80 to "all media" to ensure adequate protection of the right to free speech.[153]

EUROCHAMBRES is also critical and calls for amending or deleting the right to erasure. EUROCHAMBRES writes that Article 17 GDPR would not only be costly, but also impractical to implement, particularly with regards to social networks. It would also threaten internet-based business models. As an example for its impracticability, EUROCHAMBRES points out that a data controller will often be unable to identify all the personal data of an individual, such as where the data was originally provided by a third party. Therefore, any right to be forgotten should only be directed to data under the control of the controller.[154]

Similarly, it would also be frequently impossible for a data controller to inform third party data processors that the data subject requested their data to be erased because, especially in the online environment, data controllers would be, for practical reasons, unable to keep track of all third parties that get hold of publicly available data or to whom the data is else how made available to them.[155]

EUROCHAMBRES calls for the right to be forgotten to be limited to data submitted by users and to exclude data generated by users who use a particular service – an example being error messages or statistics. EUROCHAMBRES also asks for the possibility to retain data for a limited time for purposes of reactivating a user account at the user's request.[156]

EUROCHAMBRES also notes that the effect of the right to be forgotten on the freedoms of expression and communication need to be more thoroughly analysed. The current draft does not properly balance these rights with the individual's right to privacy.[157]

[150] Ecommerce Europe, p.8.

[151] Ibid.

[152] EDRi, p. 16.

[153] Ibid, p. 17.

[154] EUROCHAMBRES, p. 3 et seq.

[155] Ibid.

[156] Ibid, p. 4.

[157] Ibid.

Regarding cases where the online service permits the sending and receiving of correspondence, EUROCHAMBRES notes that the other parties of a communication should be allowed to keep a copy of the correspondence, i.e. not be affected by one party's request to have their data deleted.[158]

EPHA generally takes the same approach as EUROCHAMBRES and also notes that documenting data processing should not become too much of a burden, especially in the health sector.[159]

5.5.2 Effect on digital avatars

The right to erasure means that platforms such as MyHealthAvatar must allow the user to delete their account. In fact this will already be enabled for ethical reasons, and as an important expression of the citizen/patient empowerment that lies at the platform's core. It follows that the provision will not have any substantial effect on the development of digital avatars.

5.6 Profiling – Article 20

Profiling is defined as "*any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person or to analyse or predict in particular that natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour*".[160] In effect, profiling is a "map" of a person that is made to evaluate past and current and predict future behaviour.[161]

Article 20 gives the data subject who is a natural person the right to object to profiling and mandates that the data subject be informed about their right "in a highly visible manner"[162].

5.6.1 Positions

EPF supports exemptions that are for public interest, research and healthcare purposes, as well as the case-by-case right to object to further retention.[163]

EDRi sees three main issues with profiling data subjects, namely that the profile might be wrong, particularly when the data subject displays uncommon characteristics (i.e. is a statistical outlier); that profiles can be difficult to verify, because the algorithms they rely on or frequently commercial subjects and moreover hard to understand; and that the outcomes of profiles are likely to perpetuate with the risk of discrimination and other forms of unfair treatment.[164]

[158] Ibid.

[159] EPHA, p. 2.

[160] Article 4 (3a) GDPR.

[161] EDRi, p. 11.

[162] Article 20 (1) GDPR.

[163] EPF, p. 11.

[164] EDRi, p. 12.

In order to mitigate these problems, EDRi proposes that it should be made explicitly clear that the right to object to profiling should be to both online and offline profiling. With regards to online profiles, the draft should recognise that online identifiers are personal data. Data subjects should also have the right to receive meaningful information about the logic behind the profiling, while the data controller should be accountable towards DPAs so that the legality of the profiling can be assessed. Also, the "suitable measures" referred to in Article 20(2)(b) should include specific protection against discrimination as a result of profiling. Finally, and of particular importance for digital health avatars, profiling in the private sector should never include sensitive data; in the public sector sensitive data may be used only where the data are essential as long as the sensitive data do not make up the bulk of the data used.[165]

5.6.2 Effect on digital avatars

The data collected by digital avatars could potentially be used to automatically evaluate certain aspects of the patient – indeed, this would be one of the main benefits of digital avatars. In this regard it is evident they would come within the definition of profiling under Article 20. For example, a scenario could be imagined where diabetics input their blood sugar readings. When the values are out of the normal range, the digital avatar system could alert the individual and suggest countermeasures to be taken. However, no stakeholders perceived this as problematic for digital avatars. Indeed, it is implicit for any ethically operated avatar that users will be informed in a transparent way about how their data will be processed; in this regard avatars can circumvent any issues relating to profiling by enabling their users to refuse consent and object to certain measures.

5.7 Transfer of personal data beyond EU borders – Chapter V

The rules governing the transfer of personal data to third countries or international organisations follow the basic principle that the transfer may only take place if both the controller and the processor comply with the conditions laid down in Chapter V.[166] The conditions for allowing transfers can be grouped into transfers with an adequacy decision;[167] transfers by way of appropriate safeguards;[168]transfers by way of binding corporate rules (BCRs);[169] and subject to derogations.[170]

5.7.1 Positions

EUROCHAMBRES explicitly welcomes those provisions that facilitate international data transfers as being essential to the growth and competitiveness of the European digital economy. Examples are the rules on transfers by way of BCRs, and the rule that no prior

[165] Ibid, p. 12 et seq.

[166] Article 40 GDPR.

[167] Article 41 GDPR.

[168] Article 42 GDPR.

[169] Article 43 GDPR.

[170] Article 44 GDPR.

authorisation is necessary when using standard data protection clauses.[171] EUROCHAMBRES notes that they facilitate international data transfers, which are important because such flows are essential to the growth and competitiveness of the European digital economy. At the same time, EUROCHAMBRES calls for further simplification and clarification of the procedures for international data flows, pointing out that the European Commission has granted a mere twelve third country adequacy decisions since 1995 because of the complexity of the undertaking.[172]

Also, in order to not hinder data flows unnecessarily, safeguards (Article 42) and derogations (Article 44) should permit data transfers even where the European Commission finds that the data protection level analyzed is inadequate. Currently, Articles 42 and 44 are ambiguous in regards to whether they apply only in cases where no adequacy decision has been taken or also to negative decisions.[173]

Moreover, EUROCHAMBRES asks that standard data protection clauses devised by DPAs and BCRs could be adopted under a shorter procedure than the consistency mechanism, as anything else would seriously hinder the free flow of data.[174]

EDRi, in contrast, feels the GDPR would be too permissive in permitting data transfers abroad. While the Directive has a general prohibition on transferring data abroad unless certain requirements are met, the GDPR permits transfers provided enumerated conditions/safeguards are met. The main problem with the GDPR, so EDRi, is that the safeguards are not specific enough, so that misinterpretation is a serious risk.[175]

Similarly to EUROCHAMBRES, EDRi believes the adequacy rule is too bureaucratic and that it does not sufficiently guarantee that the third state has truly an adequate level of data protection. EDRi also points out that experience shows that standard clauses do not sufficiently protect personal data. Regarding existing adequacy decisions and the Safe Harbor framework, EDRi sees the Regulation as an opportunity to reform these, calling the Safe Harbor framework "*an unequivocal failure*".[176]

EDRi is also dismissive of binding corporate rules, saying they are opaque for data subjects and fail to deliver on their promise of "*control by the data controller over data that they have limited practical control over.*" The rules on BCRs would need to be revised and strengthened if they are not to end up being used to circumvent the data protection regime on grounds of promising/delivering too little protection.[177]

[171] Article 42 (2) (c) GDPR.

[172] EUROCHAMBRES, p. 6.

[173] Ibid.

[174] Ibid.

[175] EDRi, p. 22.

[176] Ibid, p. 22 et seq.

[177] Ibid, p. 23 et seq.

The derogations foreseen by the GDPR are too vague for EDRi, who warns that they could weaken the protection given to personal data. EDRi suggests that the legal ground claimed should require prior approval and that also be registered publicly.[178]

5.7.2 Effect on digital avatars

Chapter V will not have a major impact on digital avatars. Personal data can be transferred freely within the European Union. Currently, MyHealthAvatar does not foresee the transfer of data beyond the EU. However, were MyHealthAvatar or another digital avatar platform to expand beyond European borders, Chapter V GDPR will facilitate the transfer of personal data to third countries compared to the current regime under the Directive, which might possibly facilitate the development of digital avatars through the greater potential to take advantage of network effects.

5.8 Further avatar-specific comments elicited by the targeted survey

In order to understand in greater detail the stances with regards to digital avatars, we contacted those stakeholders likely most involved with the subject-matter. The questions we posed and the responses received are presented in Appendices 2 and 3, respectively. The key issues the survey was drawn up to canvass were to assess firstly whether the current and future data protection frameworks might be overprotective and inhibit research – basically the issue of (broad) consent. Secondly, we wanted to know how stakeholders would approach the balance between individual autonomy and protecting the individual, and whether they believe the draft GDPR succeeds in this. Thirdly, we sought to understand how the requirement of de-identifying data meshes with patient-centred health information. Finally, we were interested in learning how stakeholders would improve the process of obtaining approvals by research ethics committees.

Many stakeholders found it difficult to adequately reply to the survey questions because of the complexity of the issues involved and especially because the draft GDPR is still in a state of flux. The legislative process is ongoing, and current indications are that the Council and the Parliament have very differing views on those issues affecting research with sensitive data.[179]

In brief, stakeholders generally focussed on the issue of consent and warned that broad consent is a necessity for certain types of research. **EUROCOURSE** additionally warns that research requires high-quality data and that data provided by patients (who in general are medical laypersons) might be susceptible to inaccuracies.

Additionally, **EPHA** agreed to disseminate the survey on their website. As the legislative process advances and the final form of the GDPR solidifies, more detailed responses are expected. These will be taken into account by WP11 and subject to future report.

[178] Ibid.

[179] See eg http://www.statewatch.org/analyses/no-260-dp-reg-council-position-consolidated-dec-14.pdf.

TMF noted that some issues are still completely open due to the legislative process being ongoing. TMF believes that in some respects the GDPR and the Data Protection Directive are overprotective. Also, European-wide standards and templates are necessary with regards to ethical approvals.

6 Conclusion

The survey has shown that European stakeholders, i.e. patient organisations, regulatory authorities, and researchers, are in general positive about the draft General Data Protection Regulation. They all welcome the potential harmonization it would bring.

However, they also point out that there is a very real danger that some well-intended provisions might end up hampering the development of patient-centred health information in electronic format.

The key worries are that the GDPR will prohibit broad consent, which is seen as necessary for certain types of research, and that the GDPR will impose obligations upon data controllers that will be, from an administrative point of view, onerous to uphold without truly benefiting the spirit of data protection.

Also, the relationship between Articles 9, 81 and 83 GDPR is unclear and could lead to legal uncertainty, which would be to the detriment of the development of digital avatars and also how their role in medical research.

The right to erasure, the prohibition on profiling, and the introduction of the definition of the term pseudonymous data, on the other hand, are all legal developments that would not hamper digital avatars in any way. The right to erasure already exists to a certain extent, the right to object to profiling only means that users must be given the right to object to certain measures and also that automatic decisions based on data collected by digital avatars may not be taken (for example by insurances or physiscians).

Overall, none of the stakeholders believes that the issues poses are insurmountable. The stakeholders all suggest changes to the draft GDPR that would be feasible to introduce. Moreover, the stakeholders' suggestions and stances are overall harmonious. Regardless of whether patient organisations, regulatory authorities, or researchers, the issues raised and commented upon are similar.

7 Appendix 1 – Abbreviations and acronyms

BDSG	German Federal Data Protection Act
BCR	Binding Corporate Rules
BFB	Bundesverband der Freien Berufe
BPC	Belgian Privacy Commission
CDT	Center for Democracy and Technology
CEDPO	Confederation of European Data Protection Organisations
DPA	Data Protection Authority
EDRi	European Digital Rights
ENCR	European Network of Cancer Registries
EPF	European Patients' Forum
EPHA	European Public Health Alliance
ESIP	European Social Insurance Platform
ESMO	European Society for Medical Oncology
ESNG	European Social Networks Group
EU	European Union
EUROCOURSE	Europe Against Cancer: Optimisation of the Use of Registries for Scientific Excellence
GDPR	General Data Protection Regulation
ICO	Information Commissioner's Office
IT	Information Technology
LIBE	Civil Liberties, Justice and Home Affairs
TMF	Technology, Methods, and Infrastructure for Networked Medical Research
TTP	Trusted Third Party

8 Appendix 2 – Survey questions

Survey for Deliverable 11.2 of MyHealthAvatar - A Demonstration of 4D Digital Avatar Infrastructure for Access of Complete Patient Information (Grant agreement no: 600929)

1 What do we wish to know?

The idea behind digital health avatars is to offer individuals a possibility to collect and to store lifestyle and health information on the avatar. By this, the individual's health status can be represented digitally and the user can share the stored information with other users or treating doctors.

The concept, which aims at patient-empowerment, is hoped to improve the patient's lifestyle and, moreover, to facilitate clinical decisions by sharing lifestyle and other pertinent information with the treating doctor.

However, there are ethical and legal considerations that need to be considered, such as risks to patient autonomy and self-determination, as well as to the patient's anonymity and privacy interests and the danger of transparent patients.

Apart from the technical implementation of digital health avatars, the MyHealthAvatar project addresses these privacy concerns by defining a legal and ethical framework with robust guidelines intended to protect the individual. The legal and ethical framework will be based on current EU data protection law.

However, the draft GDPR Parliament's First Reading may include the rejection of the concept of broad consent, introducing definitions on "pseudonymous data" and "encrypted data", and setting up a complex web of interaction between Articles 9 (special categories of data), 81 (processing of personal data concerning health) and 83 (processing for historical, statistical and scientific research purposes). Of particular importance for medical research are the proposals that the currently existing exemptions on keeping data or using it for secondary purposes be abolished.

This survey will help give the project consortium a preliminary overview of the thoughts that European stakeholders such as patient organisations, regulatory authorities, and researchers may have in relation to the tension between patient empowerment and the current legal system that could hinder the development of digital avatars in the best interest of the individual patient.

The outcome of this survey will help European legislators to understand where data protection regulation supports and where it hinders the development of patient-centred health information in electronic format.

Please help us shape the future of MyHealthAvatar and similar projects by completing this questionnaire.

Thank you for your participation.

2 First aspect: Data Sharing

One function of digital avatars is to empower patients to share their data with other users of the platform or with treating physicians. Especially the latter could facilitate highly-tailored treatment for the individual and avoid cost and time intensive repeat medical examinations.
The draft GDPR would classify health information as a special category of data that is subject to a *prima facie* prohibition on processing. Only when certain requirements are met would it be possible to process such data – one of them being specific and explicit consent. By contrast, it should be noted that the Declaration of Helsinki appears more favorable towards the concept of broad consent.
Some argue that both the Data Protection Directive and the GDPR may be overprotective and inhibit researchers who need volunteers for research projects.

2.1 Question 1

Is it an issue that the user of a digital health avatar might wish to release all their data for research, but that there is a risk that this would be prohibited under the GDPR because the concept of broad consent might not supported by it?

2.2 Question 2

Do the current rules under the Data Protection Directive make it too difficult for patients to give consent to data processing for medical research purposes? If so, why and what would need to be changed to encourage patients to give consent?

2.3 Question 3

Would the draft GDPR hinder patient groups from sharing data amongst themselves, for example because of its requirement of specific and explicit consent as opposed to the more flexible notion of broad consent?

2.4 Question 4

Digital avatars can have functionalities such as entering, importing, storing and exporting medical data, medication lists, laboratory results and medical images. The information can also be shared with other users and doctors. One vision of MyHealthAvatar is to link data from social networks to the avatar, such as personal medical data, medication lists, laboratory results and personal medical images.
How might these functionalities threatened by the current rules and the draft GDPR? Are the respective rules overprotective?

3 Second aspect: Balancing individual autonomy and protecting the individual

Data protection frameworks not only seek to balance the privacy interests of the individual against the processing interests of entities that need to work with the data, they also seek to strike an appropriate balance between granting the individual adequate autonomy to decide how their data shall be used with protecting the individual from themselves. Today, an individual is frequently unable to fully understand and judge what use entities make of their data as well as the possible implications for them of inferences derived from their data.

3.1 Question 1

How would you balance the autonomy of the individual with the need to protect those data subjects who are unable to understand the consequences of their actions?

3.2 Question 2

How would you judge the draft GDPR in this context?

4 Third aspect: De-identification

The current rules foresee a strict de-identification of data so far as compatible with the purpose of use. A disadvantage of this is that de-identification makes it difficult to contact volunteers to give them feedback from research that has taken place. This raises the question if the need for de-identification is not too extreme.

4.1 Question

How do you place the requirement of strict de-identification within the balancing act of advancing development of patient-centered health information in electronic format against providing data subjects with an adequate level of data privacy and security?

5 Fourth aspect: Ethical approval

The Declaration of Helsinki states that in situations where it is impossible to obtain consent for research or where consent would threaten the validity of the research, the research may be done without consent, but subject to the consideration and approval of a research ethics committee.
Ethics reviews can sometimes be a slow process. Moreover, the opinions of research ethics committees in multi-centre research projects are not always consistent.

5.1 Question

How do you consider that the process of obtaining ethical approvals might be improved?

6 Final question

Are there any other points or issues you would like to highlight?

7 Appendix 3 – Heat map of stakeholders' positions

It must be noted that the heat map gives only a fairly broad indication of the positions stakeholders take and cannot reflect the frequently nuanced opinions that the position papers reveal. For example, while welcoming the overall dynamic towards harmonisation in the GDPR, some stakeholders also state at the same time that the amount of delegated acts is too high and would counteract harmonisation efforts.

	BFB	BPC	BITKOM	CDT	CEDPO	COCIR	DIGITALEUROPE	Ecommerce Europe	EDRi	EPF	EPHA	ESIP	ESMO	ESNG	EUROCHAMBRES	Eurocourse / ENCR	ICO	IMS Health	Insurance Europe	NHS	Science Europe	TMF
Harmon-isation																						
Definition of anonymous and pseudoymous data																						
Consent																						
Processing of sensitive data for scientific research (Arts 9, 81, 83)																						
Right to erasure																						
Profiling																						
Transfer beyond EU																						

	Legislation overall positive in balancing relevant interests (minor criticism possible)		Legislation is generally too weak (in under-protecting data subjects / achieving goals such as harmonisation)		Legislation is too strict/ other criticism (eg. health data use too difficult)