eHAction

Joint Action supporting the eHealth Network

Report on best practices and approaches on data protection at national level

WP 7 Overcoming implementation challenges

26/09/2019

Version 0.7a

16th eHN meeting, November 2019

For Discussion

Grant Agreement nº 801558

Co-funded by the European Union's Health Programme (2014-2020)

Work Package 7 is intended to provide the eHealth Network with valuable practical recommendations, guidelines and priorities on three of the most critical issues concerning the eHealth European ecosystem: interoperability, data protection and data and sys

CONTROL PAGE OF DOCUMENT	
Document name	Report on best practices and approaches on data protection at national level
Work Package	WP 7 Overcoming implementation challenges
Dissemination level	CO
Status	Draft
Author(s)	Jiri Borej Milan Cabrnoch Jakub Geier Tomas Bezouska
Beneficiary(ies)	Ministry of Health of the Czech Republic

Dissemination level:

PU = Public, for wide dissemination (public deliverables shall be of a professional standard in a form suitable for print or electronic publication) or CO = Confidential, limited to project participants and European Commission.

REVISION HISTORY				
Version	**Date**	**Author**	**Organisation**	**Description**
0.1	21/09/2018	Tomas Bezouska	MZCR	Outline of the document
0.1.1	23/09/2018	Milan Cabrnoch	MZCR	Revision of the first draft of the document
0.1.2	24/09/2018	Tomas Bezouska	MZCR	Revision of the first draft of the document
0.2	04/03/2019	Tomas Bezouska	MZCR	Update of the document based on current progress of the project
0.3	21/03/2019	Vivian Brincat, Hugo Agius Muscat	MFH	QM review
0.3.1	27/03/2019	Tomas Bezouska	MZCR	QM revisions settlement
0.3.2	20/05/2019	Tomas Bezouska	MZCR	Update of the time-schedule and related information based on conclusion of the LC meeting in Brussels on April 17th, 2019
0.4	04/09/2019	Jakub Geier	MZCR	Update of the document based on the results from the questionnaire.
0.5	13/09/2019	Jakub Geier	MZCR	Update and revision of the document with the conclusions of WP 7.2 F2F Meeting in Prague on September 11-13th, 2019
0.5a	19/09/2019	Hugo Agius Muscat, Vivian Brincat	MFH	QM review
0.6	20/09/2019	Jakub Geier	MZCR	Revision after WP 7.2 amendments
0.7	26/09/2019	Jakub Geier	MZCR	Minor adjustments & clarification
0.7a	14/10/2019	Jakub Geier	MZCR	Final adjustments

Table of Contents

Table of Figures

Acronyms and Abbreviations

Acronym	Description
CBeHIS	Cross-Border eHealth Information Services
eHAction	eHAction – 3rd Joint Action supporting the eHealth Network
eHN	eHealth Network
EHR	Electronic Health Record
EHRxF	Electronic Health Record exchange Format
eP/eD	electronic Prescription / electronic Dispensing record
EU	European Union
GDPR	General Data Protection Regulation (EU) 2016/679 - a regulation in EU law on data protection for all individuals within the European Union (EU) and the European Economic Area (EEA).
ICT	Information and Communication Technology
ID	Identification
JAseHN	Joint Action to support the eHealth Network
HP	Health Professional
MS	Member State
PAC	Patient Access – An eHDSI Use Case enabling the patient to access and understand what the Health Professional has recorded in the PS or eP, in order to participate in his or her own care, and/or to improve the information he or she gives to another Health Professional
PS	Patient Summary
WP	Work Package or Work Plan

Executive Summary

Common aim of the eHAction is to support accessible high-quality healthcare services for all people in European countries. The main objective of the Joint Action supporting the eHealth Network is to promote and strengthen the use of ICT in health development, from applications in the field to EU governance and strategies implementation. Reflecting the increasing importance of eHealth as a resource for health services and public health, given their ease of use, broad reach and wide acceptance from citizens. Task 7.2 is a minor but important part on the effort to reach that objective.

Task 7.2 focuses on data protection in healthcare. The main challenge today is GDPR implementation and its implications for cross-border healthcare. Document "*Report on best practices and approaches on data protection at national level*" represents the main deliverable of Task 7.2. The aim of this document is to point out the specific situation and show approaches on data protection in healthcare at national level and the situation that new requirements of the GDPR bring to eHealth.

This document describes the situation in personal data protection in healthcare, the implementation of the GDPR in healthcare in the Member States and the impact of this implementation on eHealth and on healthcare provision itself.

Since the healthcare industry is one of the most personal-data-heavy industries and processing of personal data lies at the core of most tasks handled by all the subjects operating in this field, the implementation of GDPR principles and requirements in specific regulations, standards and procedures of the industry was paramount to the successful adoption of the GDPR.

On a national level there are significant differences in the approach to providing a uniform regulation of healthcare, both in terms of financial and organisational levels and in terms of extent and methods of regulation of healthcare sector. This has a tremendous impact on the implementation of the GDPR both in national legislation and in the general practice of processing of personal data in healthcare.

For collection of data on GDPR implementation in the individual countries and its influence on eHealth and healthcare provision, we carried out a survey based on structured questionnaires.

We found relevant groups of respondents in every country. For the survey it was important to have information both from the state authorities as well as from the healthcare providers (and payers). The state authorities were: Ministry of Health, National Personal Data Protection Body, National eHealth institution and the eHAction partner (if it was not one of the above). Representatives of healthcare providers and payers were hospitals of three different levels (university, large and regional), associations of primary care providers (doctors) and health insurance agencies. After gathering the data from respondents, we proceeded to the analysis of data gathered and discussed the findings with all WP7.2 members in the face-to-face meeting.

After analysing gathered data there have been identified many different national practices. The analysis shown many different national practices of GDPR implementation. However, due to the specific legislation and experience in the healthcare sector of each country, it is misleading to choose best practice, especially since there is no recommended methodology for GDPR implementation in the healthcare sector. That is why we have chosen examples with the most detailed description or the ones with helpful approach or opinion.

We found, inter alia, that GDPR has increased the attention paid by healthcare professionals to work with personal data. The basic idea of GDPR "*to harmonize rules on Personal Data Protection across all*

EU Member States" is broadly accepted, however due to a number of exceptions and varying national legislation the goal is far from accomplished.

There is a low awareness of citizens and health professionals about rules of personal data protection as well as rights and obligations of individual subjects in handling of this data. Most health professionals lack digital health literacy. They often suffer insufficient knowledge of rights and obligations introduced by personal data protection in clinical practice.

As a key outcome of this document we recommend to the eHealth Network to:

- Support systematic awareness-raising of citizens and healthcare professionals in terms of proper personal data handling in healthcare and of the importance of the right to access health information.
- Support activities for health professionals and healthcare providers, focused on explaining the importance of proper handling of sensitive personal data and on benefits of proper sharing and exchange of information for quality, efficiency and safety of healthcare, even on the legal aspects of healthcare providers protection.
- Endorse the establishment of a general framework for education of health professionals in undergraduate and postgraduate education, and lifelong learning on personal data management and protection in healthcare, as well as on patients' rights.
- Develop, in cooperation with the European Data Protection Board, interpretations and guidelines for the implementation of GDPR in specific healthcare environments. Those guidelines should be clear, intelligible and actionable.

Introduction of the General Directive raises awareness we all pay to personal data and its protection. To fulfil the expectation to improve and harmonise the data protection rules across Europe for the good of patients and citizens a lot must be done. We have to prevent the inappropriate measures on data protection to block or complicate the use, exchange and sharing of medical data in primary as well as secondary use. There is a plenty of challenges and opportunities to continue this work on EU and member states level.

Introduction

Common aim of the eHAction is to support accessible high-quality healthcare services for all people in European countries.

The quality of healthcare services depends *inter alia* on the continuity of care, sharing, and transfer of information between healthcare providers. It is crucial for quality of care that doctors making decisions have access to all relevant existing information which can help them to decide better and to avoid mistakes. It is in the direct interest of patients.

The quality and success of healthcare depends on the relationship and cooperation between the doctor and the patient. Cooperation is based on two principles: information and trust. For patients to be fully cooperative participants in decisions and in care, they need to have the appropriate information and understanding, and to have trust in their doctor.

In healthcare one deals with a lot of personal and sensitive information. People are coming to doctors, telling them their deepest secrets, concerns, and fears. Patients have a full right to expect that doctors will treat their secrets very intimately.

There is a big challenge ahead: finding a balanced way to ensure that information is shared and transferred while being protected reliably.

The eHAction project's objective is to provide support to the eHealth Network. The eHealth Network is here to help the European Union find a best way to use electronic services and tools to meet this big challenge.

Task 7.2 is a minor but important part on this way. Task 7.2 focuses on data protection in healthcare. The main challenge today is GDPR implementation and its implications for cross-border healthcare.

This document represents the main deliverable of Task 7.2. The aim of this document is to point out the specific situation and show approaches on data protection in healthcare at national level and the situation that the new requirements from GDPR brings to eHealth.

The topic is addressed in 5 steps:

1. Review of the GDPR in general and review of its impact on healthcare stakeholders;
2. Characteristics of main points and requirements of GDPR adoption in the healthcare sector;
3. Proposal of a set of relevant recommendations/policies for successful completion of GDPR adoption in the healthcare sector;
4. Outlining collaborative instruments for related information and education at present and in future dealing with the GDPR topic in healthcare settings.
5. Foresight: vision and mission of the future fulfilment and development of the GDPR.

The task is motivated by both urgent needs to support GDPR adoption in the healthcare sector and the realisation of the GDPR's potential to achieve comprehensive respect for human rights for healthcare provision practice in the long term.

Scope

This document exclusively describes the situation in personal data protection in healthcare, the implementation of the GDPR in healthcare in the Member States and the impact of this implementation on eHealth and on healthcare provision itself.

The document does not address the issue of sharing and transfer of health information and personal data between countries.

In the document, we do not assess which country is better or worse in the protection of personal data in healthcare, nor do we assess which country more or less implements the general regulation (GDPR) in healthcare.

As best practice and approaches, we chose interesting or inspiring examples from individual countries, as provided by respondents in their questionnaire replies.

We consider information obtained in the framework of the questionnaire survey to be confidential and we will not present it in any way other than anonymously, without mentioning the author and institution.

Short overview of Personal Data Protection

The area of Personal Data Protection has been regulated on the EU level since October 1995 by Directive 95/46/EC of the European Parliament and of the Council on the Protection of individuals with regard to the processing of personal data and on the free movement of such data.

This Directive drew up some basic rules on Personal Data Protection but most of the regulation was delegated to the national level and left to be solved by national legislation. That resulted in various approaches towards Personal Data Protection and problems have arisen especially in cross-border data sharing and processing of data in multiple countries.

With growing exchange and transfer of Personal Data related to the expansion of the digital economy, and increased mobility of both people and services, it has become necessary to synchronise the approach on Personal Data Protection among the Member States and to harmonize level of Personal Data Protection in reaction to growing risks of misuse or mishandling.

In response, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, or GDPR) was created and came into effect on 25th May 2018.

This new regulation defines among other things:

- key principles of personal data protection;
- rights of the data subject;
- controller and processor of personal data and their obligations;
- transfers of personal data to third countries or international organisations;
- independent supervisory authorities.

A two-year period was set for adaptation of national legislation to the new Regulation as well as for its application in Personal Data processing methods and tools of every subject acting as a controller or processor.

Since the healthcare industry is one of the most personal-data-heavy industries and processing of personal data lies at the core of most tasks handled by all the subjects operating in this field, the implementation of GDPR principles and requirements in specific regulations, standards and procedures of the industry was paramount to the successful adoption of the new Regulation.

On a national level there are significant differences in the approach to providing a uniform regulation of healt, both in the terms of financial and organisational levels and in the terms of extent and methods of regulation of healthcare sector, which has a tremendous impact on the implementation of the GDPR both in national legislation and in the general practice of processing of personal data.

Guiding Principles and Methods Used

For collection of data on GDPR implementation in the individual countries and its influence on eHealth and healthcare provision, we carried out a survey based on a questionnaire. The electronic questionnaire was composed to cover the main topics of interest.

We found the relevant groups of respondents in every country. For the survey it was important to have information both from the state authorities as well as from the healthcare providers (and payers).

The state authorities were: Ministry of Health, National Personal Data Protection Body, National eHealth institution and the eHAction partner.

The representatives of healthcare providers and payers were: hospitals of three different levels (university, large and regional), associations of primary care providers (doctors) and health insurance agencies.

Responding groups/Types of respondents:

eHAction Participant	State authorities
Ministry of Health	
Government agency	
National Data Protection Institution	
University hospital	Healthcare providers & payers
Large hospital	
Regional hospital	
Organisation representing the Primary Care Doctors	
Payer (Health Insurance provider, National Health Insurance body)	

We asked the eHealth Action partners to help us with the identification of relevant respondents in individual countries. Having the contact details, we addressed respondents directly. Not all countries provided us with the contacts of respondents. In this case, we asked the eHAction partner to distribute the questionnaire to relevant respondents in their respective country on our behalf.

The full questionnaire was distributed to the state authorities' respondents. A reduced version of the questionnaire was distributed to healthcare providers and payers.

After gathering the data from respondents, we proceeded to the analysis of data gathered and discussed the findings with all WP7.2 members in the face-to face meeting in September 2019 in Prague.

We have identified many different national practice. However it is impossible to pick the best, as each country has its own specific legislation and experience in the healthcare secotr. That is why we have chosen the examples with the most detailed description or a very helpful approach or opinion.

Survey – Collection of data

There were several areas of interest covered by the survey. Each one was tackled by a series of questions which covered some of the key aspects of the General Data Protection Regulation and its implementation at the national level, both in the general legislation and with special focus on healthcare services and its providers.

The following areas of interest were defined:

- Legislation
    - National legislation on Personal Data Protection
    - Legislation implementing GDPR on national level
    - Other relevant regulations
    - Enforcing GDPR
    - National legislation on health records
- Key impacts of GDPR implementation on healthcare
    - Lawfulness of Personal Data processing in healthcare
    - Patient data, healthcare documentation, electronic health records in practical use
    - Access to patient data
    - Execution of rights of the data subject
    - Practical impacts of GDPR on health records
- Known challenges for implementing GDPR in the health sector

In total 17 countries participated in the Survey. There was at least one participant in each of the countries. Views, thoughts, and opinions expressed in the survey belong solely to the respondent, and not necessarily to the respondent's organization, member state or other group. For the list of the participanting countries see attached Appendix D.

Summary and Discussion

National Legislation on Personal Data Protection prior GDPR

Questions number 1-3

13 eHAction countries answered

eHAction Participant	0
Ministry of Health	9
Government agency	4
National Data Protection Institution	5
Total number of answers	*18*

All respondents indicated that they had legislation in place on Personal Data Protection prior to the GDPR. Some of the countries had a specialised law before accession to the EU; others incorporated the standards with the *acquis communautaire* (i.e. Directive 95/46/EC). Most of the legislation already had the dual system: the rights of the data subjects on one side and obligations of the data controllers on the other. However only two of the countries stated that they had a specific law on the rights of patients.

Example - LATVIA

We had a Personal data protection law (Law which was transposing the Directive 95/46/EC). Personal data protection issues where regulated in several field specific laws, for example Law on the Rights of Patients (in particular Article 10 link). Please note that there were more specific legal acts on data protection in Latvia prior the direct application of the GDPR please elaborate if you need a excusive list of all the relevant norms..

Legislation implementing GDPR on national level

Question numbers 4-9

13 eHAction countries answered

eHAction Participant	0
Ministry of Health	9
Government agency	4
National Data Protection Institution	5
Total number of answers	*18*

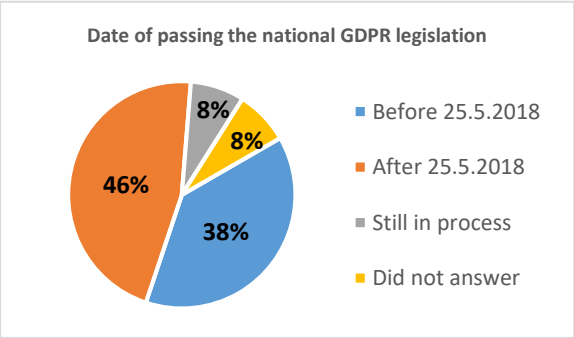

Figure 1 - Date of passing the national GDPR legislation

All but one respondent indicated the GDPR is now fully implemented. Despite the two years implementing period ended on 25th May 2018, six EU Member States disclosed a later date of passing the national legislation. In some countries, the existing legal acts had to be modified in order to comply with the GDPR. This does not mean there is an obligation to introduce a new national legislation. The GDPR gives a possibility to adapt the current one.

eHAction countries were asked to describe the framework of the national data protection legislation. Among the specific areas covered by the national legislation (in addition to those covered by GDPR) were mentioned: direct marketing; deceased people; press, journalistic or academic purposes; archiving in public interest; research; employment; justice; banking; finance; insurance; health.

Example - AUSTRIA

The Federal Data Protection Act (as lex generalis*) regulates topics such as the fundamental right to data protection (as a constitutional provision), the data protection officer, data processing for specific purposes (e.g. archiving purposes in the public interest, scientific or historical research purposes or statistical purposes), the national supervisory authority, remedies, liability and penalties.*

The Federal Health Telematics Act (as lex specialis*) specifically regulates data security measures for processing electronic health data by healthcare providers, i.e. data security measures for all forms of (directed and undirected) communication, and even stronger data security measures for electronic health records (as a form of undirected communication, i.e. data access irrespective of location or time).*

Other regulations

Question numbers 10-12

13 eHAction countries answered

eHAction Participant	0
Ministry of Health	9
Government agency	4
National Data Protection Institution	5
Total number of answers	*18*

All respondents indicated there is other relevant legislation to the GDPR which is applicable for the healthcare sector. Although GDPR is applicable itself, it is incorporated into the many national laws. Some countries also created specific protocols and good practice documents.

Example - LITHUANIA

The Regulation gives the Member States a degree of flexibility to lay down their rules, including the processing of specific categories of personal data (sensitive data). The following laws are relevant to processing health data; such rules are laid down in the Law on the Patients' Rights and Compensation of Damage to Health; Law on Health Systems; Law on Health Care Institutions; Law on Health Insurance; Pharmacy Law; Law on Human Tissues, Cells, Organ Donation and Transplantation; Law on Mental Health Care; Law on Ethics of Biomedical Research; legislation on Protection of Health; and others.

Implementing legislation regulates the processing of health data in registers and information systems and the processing of health data in separate healthcare processes in more detail.

Enforcing GDPR National Supervisory Authority according to Article 51 of GDPR

Question numbers 13-14

16 eHAction countries answered

eHAction Participant	0
Ministry of Health	9
Government agency	7
National Data Protection Institution	5
University hospital	3
Large hospital	1
Regional hospital	6
Organisation representing the Primary Care Doctors	0
Payer (Health Insurance provider, National Health Insurance body)	5
Total number of answers	*36*

All respondents answered the question regarding who is the supervisory authority according to the Article 51 of GDPR. The designated institutions follow the countries' self-governance specifics – i.e. federalist countries have a Federal Commissioner. Some countries linked the name of the institution with the personal body and named the institution Information Commissioner or Data Protection Ombudsman, rather than Data Protection Inspectorate or Data Protection Commission.

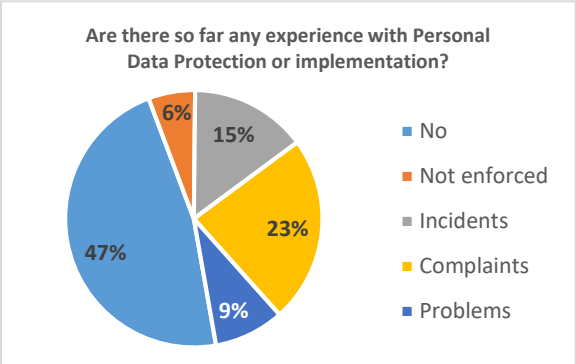

Figure 2 - Experience with Personal Data Protection

Several countries (healthcare providers) mentioned problems arising with the implementation: "*Problems have been encountered with the determination of roles in the clinical trials of medicinal products, i.e. whether the manufacturer of medicinal product as the sponsor of the trial and the hospital are jointly liable processors, or responsible and authorised processors. Each contracting party construes the GDPR to their benefit. Different interpretation often also proceeds from the fact that the sponsor originates from another country*".

Next to this, a problematic ambiguous term was identified in GDPR, e.g. 'in large extent', 'style of processing', 'context', etc., enabling different interpretations and causing misunderstandings.

Also, the first complaints have already been made by individuals: mostly about the data processing done by healthcare providers, which generated a large amount of work for the national data protection Institutions.

Since the GDPR has been applied, some incidents have already been reported. Their nature is very broad:

- health service provider did not inform data subjects about phone call recording;
- poor processing of paper medical records: the proper physical security was not secured;
- a psychiatric hospital revealed information about a patient's private life to journalists;
- patients were blackmailed: data stolen from a plastic surgery clinic;
- complaint against a health professional due to non-eligible access to healthcare documentation;
- a large hospital published patient data in the press;
- a stolen computer included patient data;
- a university hospital's invoices included patient data.

There was an opinion that the deadline for data breach notification according to Art. 33 should be longer. It is often not possible to confirm a breach in 72 hours; more time is needed for analysis and evaluation.

Example - ESTONIA

In accordance with the General Data Protection Regulation (GDPR) in force in Europe and the Personal Data Protection Act (IKS) in force in Estonia, the citizen has the right to review the activities related to their data. A data tracer offers this possibility. Different measures can be envisaged to ensure transparency and lawful processing. In Estonia, for example, a Personal Data Usage Monitor has been implemented (overview of when and why a citizen's data has been processed by a public authority). The Monitor is designed to interface with public sector information systems that keep and process personal data in their own databases.

Such good practices can also be applied in the private sector. This kind of communication allows for greater transparency, but also decreases the data processor's responsibilities in data processing.

National legislation on Health Records

Question numbers 15-21

13 eHAction countries answered

eHAction Participant	0
Ministry of Health	9
Government agency	4
National Data Protection Institution	5
Total number of answers	*18*

The set of questions regarding national legislation on health records should not be considered as a follow-up study in terms of the 'Overview of the national laws on electronic health records in the EU Member States (2016)'[1].

Legislation on health records is significantly different among the eHAction countries. For example: Law on health documentation and records; Law on the rights of the patients; Law on Health Systems; Health Identifiers Act; Regulation on information system of eHealth services; Act on electronic processing of social and healthcare data; etc.

The diversified way of keeping and protecting EHRs leads to individual application of GDPR rules to each register or database.

Example - SLOVENIA

Healthcare Databases Act is major legal basis for data processing in healthcare. Databases in healthcare are specified in details, including comprehensive description of personal data being collected. For each database, the legal purpose of data processing is stipulated. Data controllers and eligible users are identified per database, as well as eligibility of data exchange between the databases. All healthcare providers are mandatory users of national eHealth services.

There are also implementing regulations of Healthcare Databases Act:

- *Rules on authorisations for data processing in the Central Registry of Patients Data: user's rights and access policies or national Healthcare professionals have acces Patient Summary only. Medical doctors have access based either patient's choice of personal GP, an active referral or patient's consent. Further restricions are applied depending on medical speciality of the querying versus speciality of record origin so that access to most sensitive documentation (such as psychiatry) is strictly controlled;;*
- *Rules on the prohibition of access to the patent's data in the Central Registry of Patients Data: Patient's right to forbid access to their Patient summary;*
- *Order determining the types and retention periods of medical documentation in the Central Register of Patients Data;*
- *Rules on the conditions, deadlines and method of integration and use of the eHealth system for mandatory users: information security rules for healthcare providers using eHealth services.*
- *Health Care and Health Insurance Act: Article 79 defining databases and datasets for health insurance, their purpose and eligible users, and data protection requirements (e.g. secure and encrypted data transfer).*
- *Rules on health insurance card, professional card and authorisations for data processing: Rules to access personal data in the national health insurance databases (controlled by Health Insurance Institute of Slovenia). According to Art. 4, access to personal data is based on simultaneous use of a patient's health insurance card and health professional's card. Article 30 defining data elements and the respective user rights per data element.*
- *Rules on authorizations and Rules on prohibition are technically implemented on national EHR system via real-time auditing users and queries. It has to be taken into account that this approach vastly increases*

[1] https://ec.europa.eu/health/ehealth/projects/nationallaws_electronichealthrecords_en

complexity of related ICT systems and applications. It requires substantial resources and may be challenging to maintain. Also, ammendments of legislation may be required when introducing new databases, datasests, services or user gropus

Key impacts of GDPR implementation on healthcare

Question numbers 22-26

16 eHAction countries answered

eHAction Participant	0
Ministry of Health	8
Government agency	7
National Data Protection Institution	4
University hospital	3
Large hospital	1
Regional hospital	4
Organisation representing the Primary Care Doctors	0
Payer (Health Insurance provider, National Health Insurance body)	5
Total number of answers	*32*

Respondents were asked to provide a short description of impacts on rights, obligation and/or other aspects of GDPR implementation in particular groups listed below. They commented on work with patient data, healthcare documentation, electronic health records, etc. in connection with the provision of healthcare services.

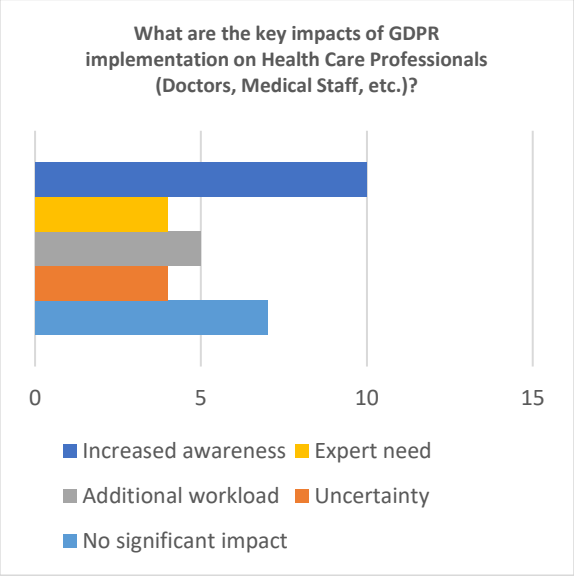

Figure 3 - Key impacts of GDPR implementation on Health Professionals

Main target groups:

1) Health professionals
2) Emergency healthcare providers
3) Healthcare providers
4) Healthcare insurance providers
5) National authorities and organisations collecting patient data; healthcare documentation; electronic health records

The following set of questions was answered by all types of respondents. More than one answer per respondent was allowed and all respondents were asked to give an opinion on key impacts on each target group.

Answers were sorted into the five groups according the topic: Increased awareness; Expert need; Additional workload; Uncertainty; No significant impact

Key impacts on **(1) Health Professionals**:

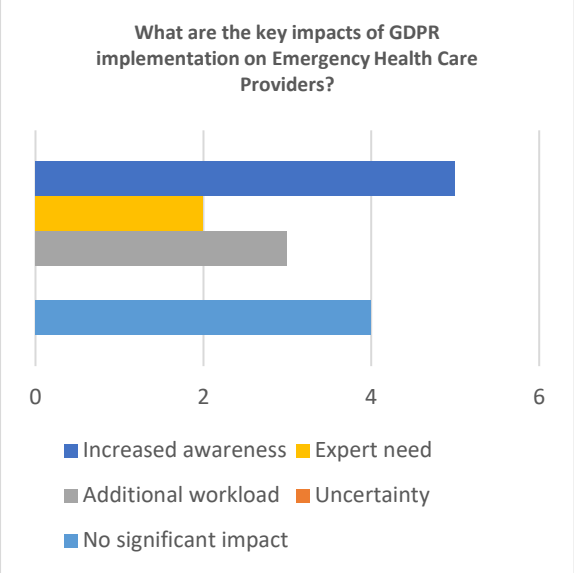

Figure 4 - Key impacts of GDPR implementation on Emergency Healthcare Providers

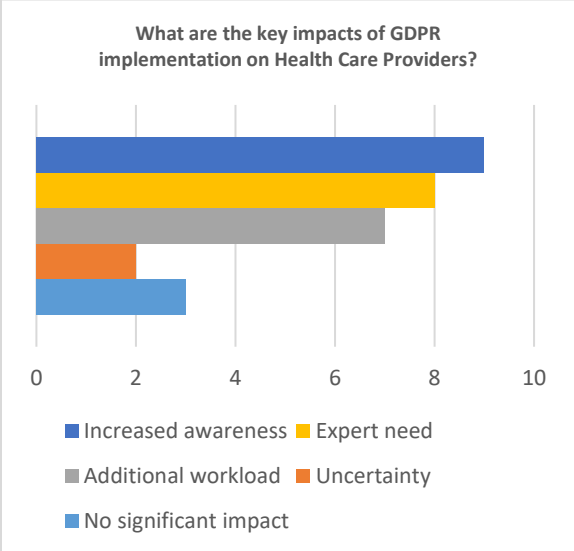

Figure 5 - Key impacts of GDPR implementation on Healthcare Providers

Uncertainty about the obligations, lack of data protection literacy, extensive use of external data protection consultancy (with often misleading results). Lack of legal certainty, especially regarding secondary use of data.

Most often impact was increased awareness. The other impacts were equally notable.

Key impacts on **(2) Emergency Healthcare Providers**:

Additional workload, lack of the data protection specialists, increased awareness in handling of the data.

Similar to the previous target group, here increased awareness was also the main impact. From the other impacts uncertainty is clearly visible as absent..

Key impacts on **(3) Healthcare Providers**:

New demands for personal data assistant and personal data processing agreements, more information to patients regarding processing of the data, implementation costs, weak understanding on who is the data controller or processor, disclosure of patient data for research purposes, lack of legal certainty in anonymisation and secondary use of data.

Key findings: A great risk for the future once the fines are imposed. No room for remedy. Generally underestimated threat.

Healthcare Providers identified the most often impacts on increased awareness, need of experts and additional workload.

Key impacts on **(4) Healthcare Insurance Providers**:

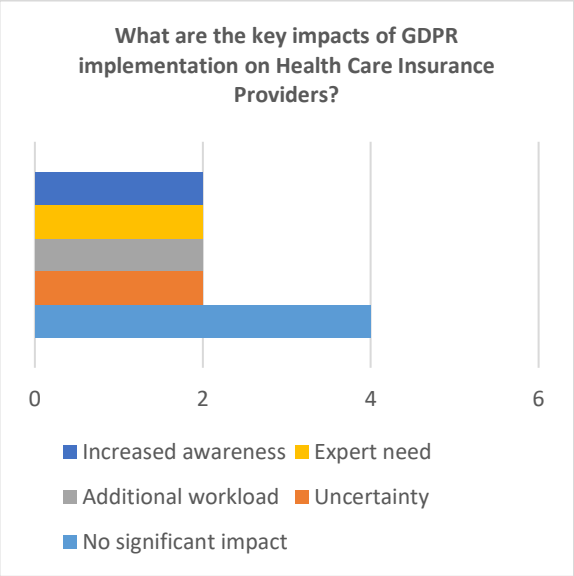

Figure 6 - Key impacts of GDPR implementation on Healthcare Insurance Providers

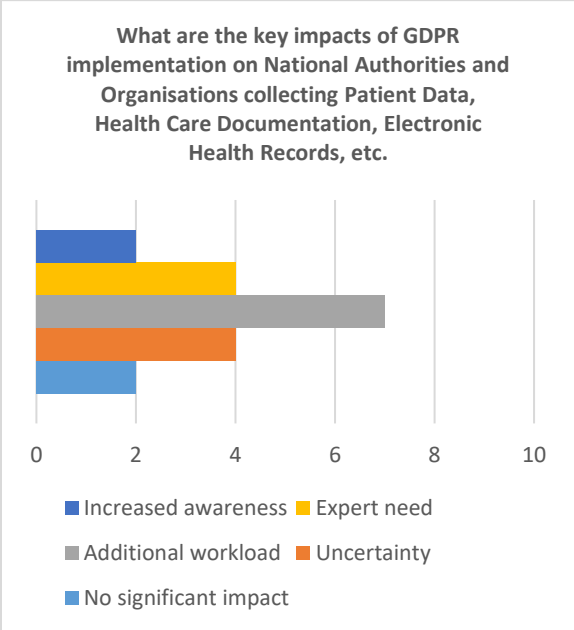

Figure 7 - Key impacts of GDPR implementation on National Authorities and Organisations

Lack of legal certainty, understanding of the provisions of health records, ensuring the data minimisation principle, changes to contracts, consent management, creation of Obligation Register, creation of a new process for Personal Data Breaches, updating the Data Protection Statements for all products.

Key findings: There is a misconception that insurance companies do not have to follow GDPR because they have specific rules for the protection of personal data.

This target group provided only a few answers. However no significant impact prevails.

Key impacts on **(5) National authorities and organisations collecting patient data; healthcare documentation; electronic health records; etc.**:

Carrying forward necessary secondary legislation, many legislative acts still being revised and amended, increased importance to health data often leads to withholding without reason (even though the state authorities have the right to receive it), increased complexity of the administrative processes, pseudonymisation problems, dual practice.

The most often impact on national authorities and organisations results in additional workload.

Lawfulness of Personal Data processing in Healthcare

Question numbers 27-45

16 eHAction countries answered

eHAction Participant	0
Ministry of Health	7
Government agency	7
National Data Protection Institution	3
University hospital	3
Large hospital	1
Regional hospital	6
Organisation representing the Primary Care Doctors	0
Payer (Health Insurance provider, National Health Insurance body)	4
Total number of answers	*31*

In this set of questions, the respondents were asked to fill the question matrix with multiple answers. Each respondent indicated what the key legal basis is for Personal Data processing in healthcare according to GDPR in case of particular types of providers.

The explanatory power of the results may have been limited to the extent that each respondent was representing a certain group of respondents – and therefore his knowledge of the legal basis for other groups may have been limited.

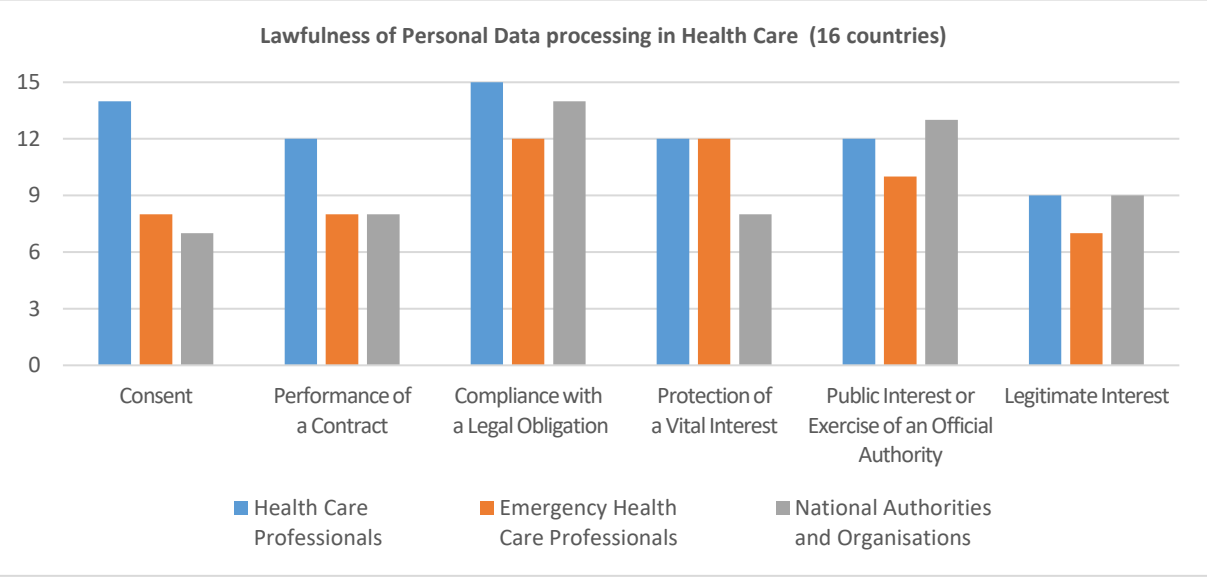

Figure 8 - Lawfulness of Personal Data processing in healthcare

What is clear from the results is that the main legal basis for Personal Data processing is 'compliance with a legal obligation'. The second-rated instrument is 'public interest' or 'exercise of an official authority'. Third-rated was 'protection of a vital interest'.

Consent is a legal basis with a very different result in the terms of practising group. This instrument is largely used by health professionals; however emergency health professionals or national authorities and organisations are rather bound with different instruments.

Some observations were made by the respondents:

- Patients using statutory health insurance often have their data processed on the basis of a legal obligation, while patients with private insurance have their personal data processed on the basis of a contract or consent.
- In accordance with national data protection law, processing of health-related data in the public sector is only allowed when a legal basis exists, and consent-based processing is only legal if stipulated by law. In the private sector, consent may be the adequate basis for healthcare data processing.
- Consent should not be the commonest legal ground here for personal data processing. Lawfulness rather originates from the grounds of contract and legal obligation. Consent can be the case, for example, for science/research participation as the basis for voluntary personal data processing.

Example - CROATIA

Providing public healthcare is in particular based on law and numerous regulations. In a specific situation, considering the activity it performs, the hospital can lay lawfulness of Personal Data processing on protection of a vital interest. The same applies also to public interest or exercise of an official authority. Legitimate interest is a legal basis for processing Personal Data by video surveillance.

Patient Data, Healthcare Documentation, Electronic Health Records in practical use

Question numbers 46-53

16 eHAction countries answered

eHAction Participant	0
Ministry of Health	8
Government agency	7
National Data Protection Institution	4
University hospital	3
Large hospital	1
Regional hospital	6
Organisation representing the Primary Care Doctors	0
Payer (Health Insurance provider, National Health Insurance body)	5
Total number of answers	*34*

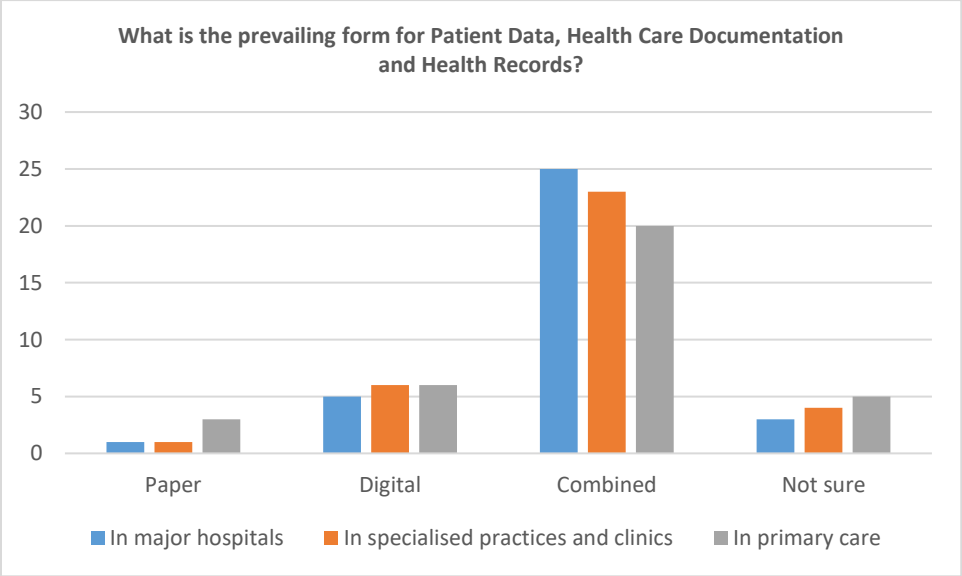

Figure 9 - Prevailing form for Patient Data, Healthcare Documentation and Health Records

Respondents were asked to identify regulatory obligations related to the use, handling, exchange, sharing and storage of patient data, healthcare documentation, and health records. In total, they have identified more than 40 legal norms which can be divided into several groups:

Laws on Healthcare Provision
Act on Biobanks in Healthcare
Act on International Threats to Human Health
Act on Quality and Safety Standards in the Management of Human Bodies
Act on Register of National Vaccination Programs
Blood Safety Law
Health Care Services Act
Health Services Organisation Act
Hospital Law
Law of Obligations Act
Law on Dental Medicine
Law on Health Care Institutions
Law on Health Documentation and Records
Law on Health Systems
Law on Market Organisation in Health Care
Law on Medical Practice
Law on Medical-Biochemical Activity
Law on Patients' Rights and Health Damage
Law on Physiotherapy Activity
Law on Psychological Activity
Law on Quality and Safety Standards in the Handling of Human Tissues and Cells
Medical Practitioners Act
Medicines List Act,
Midwifery Act
Nursing Act
Patients Right Act

Prescription Register Act The Medicines Act	Health Data and Information Act Health Data Register Act Information Security Act Law on Supplementary Provisions for Processing of Personal Data in Health Care Patient Data Law Pharmacy Data Layers Protection of Documents and Archives and Archival Institutions Act
Laws on Health Insurance	**Subordinate (Secondary) legislation**
Compulsory Health Insurance Act Health Care and Health Insurance Act Health Insurance Law Law on Health Insurance	**Internal guidelines**
Specialised laws on Electronic Healthcare	
Act on Electronic Health Record Act on Electronic Processing of Social and Health Care Data Act on Health Telematics Client Rights Act for Electronic Data Health Care Databases Act	

The above mentioned legal norms regulate the use, handling, exchange, sharing and storage of patient data, healthcare documentation, and health records.

For example in Estonia, fulfilment of the documentation obligation proceeding from the Health Services Organisation Act and the composition of relevant collected data was valid also before the enforcement of the GDPR. After the enforcement of the GDPR, national legal acts were amended. In the course of amendment, most attention was paid to the specification of the composition of collected data and the terms of data storage. Before, it was preferred to store data permanently, or no special attention was paid to the terms, and data was deleted according to the need of the hospital, rather than the purpose of collection.

One of the respondents pointed out a problem which may occur in federalised states. The sectorial law is both on federal and on a state level. Sometimes the state law on data protection and hospital law significantly differ.

In another state the biggest challenge was to ensure a full transmission of medical records to the central eHealth system. Some documents are mandatory to transfer, however not all healthcare institutions comply with this regulation. For example in Lithuania, according to the Order by Minister of Justice on the Approval of Civil Statutory Registers and Civils Statements and Forms and Other Documents a certificate of birth of a child and medical death certificate must be sent to the central eHealth system, paper documents of registration of these events are no longer existent. Lack of full compliance with the regulation is due to several reasons, such as heavy workload (especially at primary care level), and lack of digital health skills.

In general, all stakeholders must comply within the framework of the legal norms. The obligations on the side of the regulator is not only to provide clear legislation, but also to design the ICT infrastructure accordingly and observe the application of the law.

Since all respondents indicated the existence of specialised laws beside the GDPR, the question on the legal practice without a specialised law become obsolete/irrelevant.

The next question asked how the GDPR and related legislation have affected the use, handling, exchange, sharing and storage of health records (e.g. were there any processes or tools that had to be modified significantly or are no longer available due to GDPR implementation). The respondents agreed on the following answers:

- The implementation of GDPR led to increased awareness of data protection risks.
- Stricter issuance of medical records, greater protection of personal data of patients and staff.
- The GDPR has raised standards in data sharing, especially for special category data.
- Given the fact that the processing of health data was well regulated before the Regulation, there was no need for any major changes. It could be claimed that after the implementation of the GDPR, more attention is paid to the implementation of data subject rights and health data security requirements. This also applies

to the proper identification of the data subject and the strengthening of the security of the information systems related to health data.

- More data is processed automatically in information systems, with greater responsibility for both the controller and the processor. However, this is not to do with the Regulation, but with the digitisation of health data and the increasing reuse of it in the treatment process of patients.
- Only data necessary for each specific purpose is processed. Personal data is not made accessible to an indefinite number of staff without the individual's intervention.
- Stricter personal data processing policy.

Example - CZECH REPUBLIC

The Health Services Act provides for the obligation for each physician to provide the other attending physician with all information necessary to ensure continuity of healthcare. At the same time, it obliges each physician to always provide information about the healthcare provided to the registering physician of the patient, which the patient is free to choose.

A group of respondents representing non-state respondents mostly answered that no changes or only a minor change have been noticed after the introduction of GDPR. The other group, containing the government bodies, often mentioned GDPR brought stricter rules on the handling of health records.

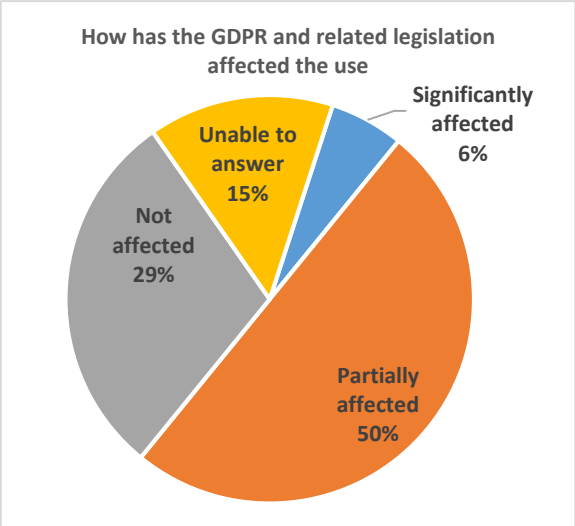

Figure 10 - Affection by GDRP or related legislation

Despite most of the responding countries having implemented changes in their national legislation as a result of the GDPR, some are still facing challenges with adapting the relevant primary and secondary legislation. Here are the examples of challenges from these respondents:

- Many domestic laws governing particular healthcare activities contain provisions for the management, storage and exchange of information from health records. It is necessary to align this practice with the provisions of the GDPR.
- Development of the process for setting the terms of data storage and rules for the deletion of data. Assessment of what should be stored based on legal acts, and how to ensure the deletion of data or the anonymisation thereof, if necessary, after the expiration of the term.
- Development and implementation of the process of impact assessments related to data protection; in addition, development of rules for the notification of violations – who and when should be notified.
- The regulation of chief processor and authorised processor shall be added to the already concluded cooperation contracts. This requires negotiations and agreements with contract partners; the problem lies in the varying interpretation of the GDPR.
- A question has arisen with whom and when should the hospital conclude the data processing contract between the chief processor and authorised processor. Considering the difficulties in assessing roles, specifying the obligations of parties in contracts is also complicated.
- Cross-border exchange of health data (between the federal states) and secondary use of data.
- Data interchange between health institutions.
- Raised standards meant that everybody had to address this in their contracts, customer consent and claim forms.

- Significant challenges in terms of funding and resources to improve legacy systems.
- Data Protection Officers in large organisations are also finding it difficult to have the level of access and oversight required to ensure compliance.
- Challenge is to ensure that all areas where hospital data is received and transmitted are monitored in the hospital.

Many respondents mentioned also personal and financial demands.

Access to Patient Data

Question numbers 54-55

16 eHAction countries answered

eHAction Participant	0
Ministry of Health	9
Government agency	7
National Data Protection Institution	5
University hospital	3
Large hospital	1
Regional hospital	6
Organisation representing the Primary Care Doctors	0
Payer (Health Insurance provider, National Health Insurance body)	5
Total number of answers	*36*

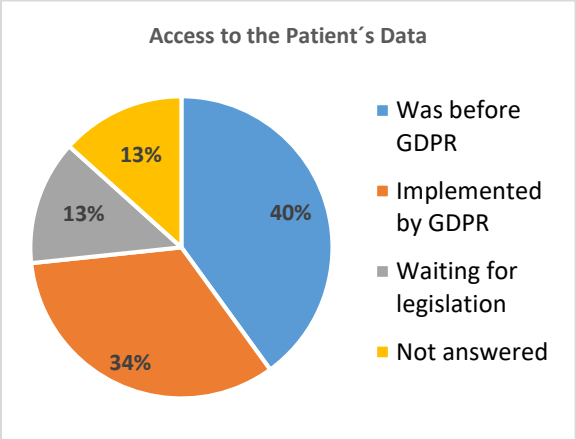

Figure 11 - Access to the Patient´s Data

The graph shows the situation regarding the implications of GDPR and related legislation on patients' access to their own patient data, healthcare documentation, and electronic health records.

In 6 of the 15 countries, the legislation already allowed certain access to patient data. However it may have been connected to a fee or there was a lower standard of authentication. 5 countries answered that GDPR improved access to the patient data, while 2 are still waiting for the legislation.

Respondents' answers differ in the question of accesssing patient data, healthcare documentation and health records without the patient's consent. There is a variety of solutions implemented in their national legislation.

- Attending doctor and medical staff
- Preventive work, invitation to the regular appointments
- Health insurance providers (lawful when necessary and appropriate)
- Access for insurance, employment and pension services
- In specific cases and to the extent necessary to protect patient's interests
- State institutions upon written request
- General practitioner when holds a general consent resulting from contract
- Emergency health professionals
- Financial and medical audits authorised by auditing doctors
- Inspectorial supervisions
- Domestic processing of healthcare data
- Patient summary is accessible to all health professionals (including nurses, physiotherapists, etc.)

Example - SERBIA

The processing by the competent authorities for special purposes as the processing of genetic data, biometric data for the purpose of unified identification of a natural person, data on health status is permitted only if it is necessary, with the application of appropriate protection measures for the rights of the person to whom the data relate, in one of the following cases:

treatment is necessary for the purpose of preventive medicine or occupational medicine, in order to assess the working ability of employees, medical diagnostics, provision of health or social care services, or management of health or social systems, based on the law or on the basis of a contract with a healthcare professional, if processing is done by a party or under the supervision of a healthcare professional or other person who has a duty to keep a professional secret prescribed by law or professional rules;

processing is necessary in order to achieve public interest in the field of public health, such as the protection against serious cross-border threats to the health of the population or the provision of high standards of quality and safety of healthcare and medicines or medical devices, based on a law providing adequate and specific measures for the protection of rights and the freedom of the person to whom the data relate, especially with regard to keeping a professional secret;

processing is necessary for the purposes of archiving in the public interest, for the purpose of scientific or historical research and for statistical purposes, if such processing is proportionate to the achievement of the goals that are intended to be achieved, with respect to the substance the right to protection of personal data and if it is ensured the application of appropriate and special measures for the protection of the fundamental rights and interests of the person to whom this information relates.

Patient ID

Question number 56

16 eHAction countries answered

eHAction Participant	0
Ministry of Health	8
Government agency	7
National Data Protection Institution	5
University hospital	3
Large hospital	1
Regional hospital	6
Organisation representing the Primary Care Doctors	0
Payer (Health Insurance provider, National Health Insurance body)	5
Total number of answers	*35*

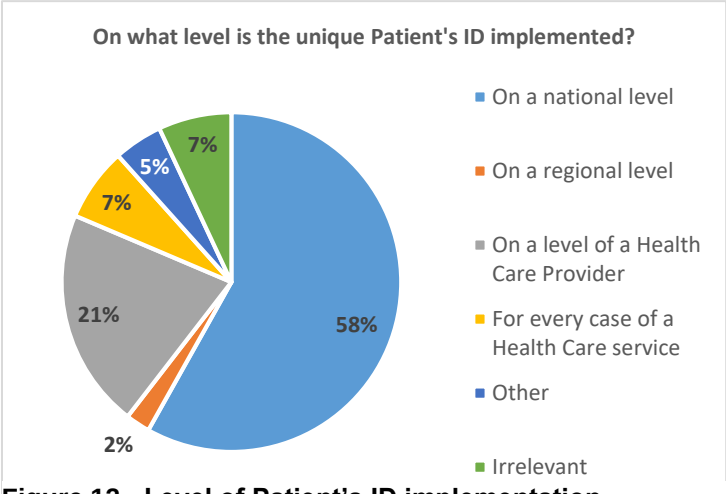

Figure 12 - Level of Patient's ID implementation

Respondents were ask to identify the level on which the unique Patient's ID is implemented. Multiple answers were possible.

The results shows that the respondents representing government groups mostly answered the first option (on a national level), while repondents from various hospital indicated the Patient's ID was implemented on a level of a Healthcare Provider, and at the same time on a national level.

A great inconsistency was also visible. When more respondents from one country anwered the question, the results were different.

The use of the Patient's ID on the national level is the vital condition for ensuring cross-border interoperability of healthcare services. The application of GDPR needs to take this into account when our target is healthcare digitalization.

Example - CZECH REPUBLIC

The Czech Republic uses unique Patient IDs on a national level. This number is automatically given to all Czech nationals. It is used not only in healthcare but also in a variety of situations in banking, employment or when communicationg with the authorities.

Execution of Rights of the Data Subject

Question numbers 57-59

16 eHAction countries answered

eHAction Participant	0
Ministry of Health	8
Government agency	7
National Data Protection Institution	5
University hospital	3
Large hospital	1
Regional hospital	6
Organisation representing the Primary Care Doctors	0
Payer (Health Insurance provider, National Health Insurance body)	5
Total number of answers	*35*

In the case of rules for execution of the right to rectification, it depends on where the data is stored, and who the data controller/processor is. In general, the patient has a right for rectification based on Art. 16 of the GDPR. When we speak specifically about healthcare data, many countries accept this and regulate only the procedure of rectification (i.e. the authorised can be a health professional; legal service and Quality Office for Health Services; rectification upon written application to the DPO).

However, some respondents indicated the right for correcting data proceeding from the GDPR does not apply if, for example, the patient does not agree with their diagnosis or with the data (health parameters) collected during the provision of healthcare services. The hospital cannot correct health data only based on the opinion of the patient, but the patient is entitled to ask a different opinion from another provider of healthcare services. The patient is entitled to request the change of diagnosis e.g. in court. This is the case when specific national legislation exists.

Moreover, in one country patients cannot claim the rectification of their healthcare documentation. Healthcare providers are lawful users and processors of the data. The right of rectification is limited to specific data or situations (e.g. obvious mistakes, such as wrong patient ID assigned to a document; participation in voluntary surveys; etc.). The right to rectification is executed directly in the interaction of patient with the respective healthcare provider.

When it comes to the execution of the right to erasure, the respondents answered similarly to the previous question. The process of whom to contact when filling a form is identical with the rectification. However the right to erasure (to be forgotten) is not always well understood by patients. Healthcare providers retain data where consent is not the lawful basis for processing and also for the defence of their practice. The right to erasure is not an absolute right and this needs to be balanced with a retention policy. In fact, healthcare providers may retain personal data to comply with statutory and regulatory obligations, to manage legal claims, and for other business requirements.

Article 17 of the GDPR has very limited use. The right may be applicable in case the patient pays in full for the healthcare services; in case of participation in a voluntary survey; and in case of data collected with consent.

The same applies for the right of access. In many states there is specific legislation. What must be taken into account is that not all health data are yet digitalised. Then it is difficult for patients to access the data.

This right is the most applied from the above mentioned.

Practical impacts of GDPR on Health Records

Question numbers 60-64

16 eHAction countries answered

eHAction Participant	0
Ministry of Health	8
Government agency	7
National Data Protection Institution	5
University hospital	3
Large hospital	1
Regional hospital	6
Organisation representing the Primary Care Doctors	0
Payer (Health Insurance provider, National Health Insurance body)	5
Total number of answers	*35*

The respondents stated that there are several implications that prevent certain stakeholders in healthcare from full implementation of the GDPR.

- Complexity of institutions (activities, scope of authority)
- Public interest
- Well-being of patients
- Cultural resistance from within the health sector
- No general guidelines for the processing of personal data throughout the health system
- Inconsistency of the national law with the GDPR
- Inconsistency of law enforcement

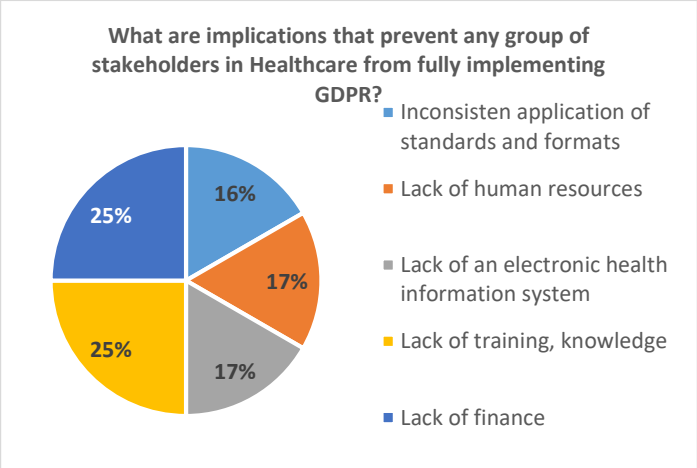

Figure 13 - Implication preventing from full implementation

The following causes were mentioned more than twice: inconsistent application of standards and formats, lack of human resources, lack of an electronic information system, lack of training and knowledge, lack of finance.

In contrast with the above-mentioned, almost all Ministries of Health indicated that there is no problem preventing stakeholders from full implementation.

The rest of the respondents see the problems as sectional: it touches all areas.

Respondents were very divided on the question of inadequate costs or other types of induced resource consumption connected with GDPR implementation. The incoherence was visible not only on the country level, but also among different groups of respondents inside the country.

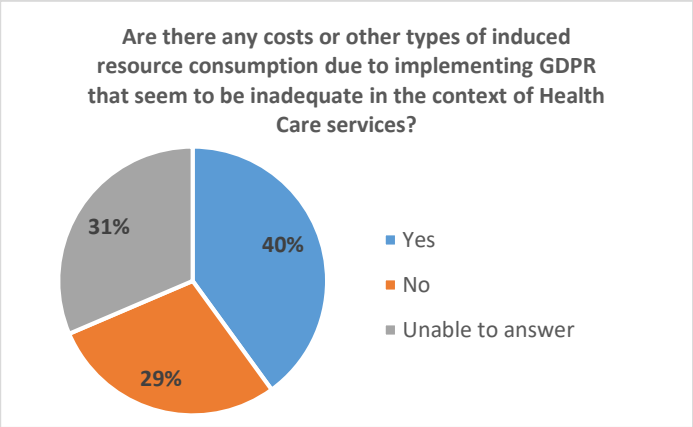

Figure 14 - Existence of inadequate costs for GDPR implementation

Among the costs arised during the implementation the respondents mentioned: software updates, new positions, consultancy, legal analysis, general administration (revision of contracts, human resources).

However, not many respondents were able to say what the exact cost of GDPR implementation was. Mostly they said that the costs were very high, without mentioning the exact figure. The most accurate answer was provided by a hospital. In case of a large university hospital, the sum was €3,600,000 (+ € 250,000 annually). On the contrary, a government agency responsible for eHealth stated €70,000.

Multiple obstacles were mentioned. Many of them were already mentioned before: implementation of an integrated information system, personal capacity, lack of training for front office personnel, lack of resources, lack of harmonisation on a state level, lack of employees, lack of application practice, growth of bureaucracy.

The last question in this block was devoted to the expected benefits of the GDPR and related national legislation. The respondents often mentioned better organisation and security of the data, trust of clients, awareness, transparency, clear responsibilities, but only a few mentioned unified rules on the EU level. The question might be also understood as a wish of the respondents, based on their actual needs.

In order to keep the full information value and show the respondents' undestanding of benefits of GDPR, the list of the anonymised responses has been attached (Appendix B).

Example - CROATIA

In conflict and borderline situations, preference is given to ensuring efficient healthcare.

Known challenges for implementing GDPR in Health Sector

Question numbers 65-67

16 eHAction countries answered

eHAction Participant	0
Ministry of Health	9
Government agency	7
National Data Protection Institution	5
University hospital	3
Large hospital	1
Regional hospital	6
Organisation representing the Primary Care Doctors	0
Payer (Health Insurance provider, National Health Insurance body)	5
Total number of answers	*36*

The last block of questions was devoted to the key issues and challenges related to implementing GDPR in the health sector. There was a variety of responses, and often the point of view was shared across the responding groups. Below are the main topics. Full and detailed information on the challenges has been attached (Appendix C).

- Legal questions (harmonisation, competences, public interest)
- Scientific & research questions (anonymisation, limitation of use, additional consent)

- Security (protection & exchange of data, traceability)
- IT (implementation of software, connecting databases)
- Personal questions (capacity, knowledge, funding)
- Health professionals (bureaucracy, authentication, authorisation, operational rules)
- Patients (refusing consent, complaints)
- Data protection authority (enforcement, audits)

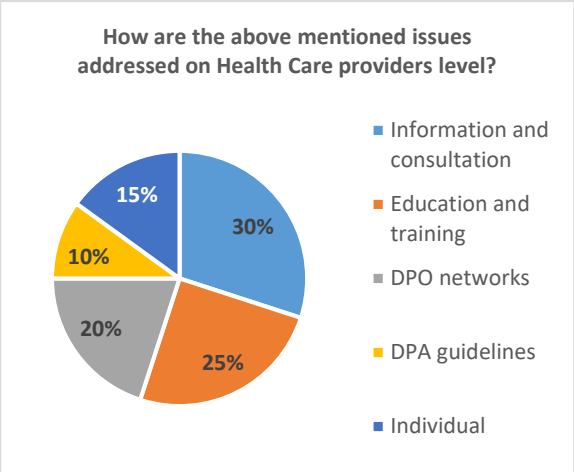

Figure 15 - Tackling of GDPR issues

The following graph shows how respondents face the issues of GDPR implementation.
Government respondents were asked how they address the above-mentioned issues on national legislation.

The most-used solution is to amend or regularly review the national legislation – often with help of the stakeholders. Among other instruments are: educational awareness and IT competence, formation of an ad-hoc expert group to identify problematic areas, establishing a specialised body to improve systems and services, proper choice of DPO.

In some countries, the oversight of private healthcare providers is not equivalent to that of state-owned providers.

We can assume that most countries have applied a complex approach and not one single solution. This is visible from the shares of the corrective measures.

Example - CZECH REPUBLIC

At national level, the state promotes the proper handling of personal data in healthcare through a coherent educational programme for health professionals and other non-medical professionals in healthcare implemented by the Institute of Postgraduate Education. The Institute carries out specialised education in the field of personal data protection and medical documentation for healthcare workers and managers of healthcare facilities. It also implements a systematic programme of upgrading qualifications for healthcare DPOs.

Conclusion & Recommendations

The following conclusions were made based on the analysis of data gathered through questionnaires and other resources:

CON-01. Individual countries give different degrees of importance on the protection of personal data in healthcare provision. Different levels of preparedness were identified among the Member States.

CON-02. The idea of the GDPR "*to harmonize rules on Personal Data Protection in all EU Member States*" is broadly accepted, however due to a number of exceptions and varying national legislation the goal is far from accomplished.

CON-03. Healthcare providers' management have not yet accepted full responsibility to manage sensitive personal data. State authorities often place obligations without supportive guidelines, rules and financial support.

CON-04. GDPR rules introduced new barriers for scientific activity (secondary use of data).

CON-05. There is a low awareness of citizens and health professionals about the rules of Personal Data Protection as well as the rights and obligations of individual subjects in handling of this data.

CON-06. Most health professionals lack digital health literacy. They often suffer insufficient knowledge of the rights and duties introduced by Personal Data Protection in clinical practice.

CON-07. There is a contradiction in the perception of GDPR costs: state authorities see none, while health professionals face high expenses. National authorities are not supportive to healthcare providers in creating the conditions for GDPR implementation and leave its application to healthcare providers and health professionals. This has a negative impact on the level of data protection.

CON-08. The complexity of GDPR implementation, lack of clear guidelines and penalty threats place health professionals in an uncertain situation. This leads to fear, and results in much lower willingness to share information and negative impact on treatment.

CON-09. In contradiction to the original intention of harmonisation of rules, some of the recommendations which have been published at EU level are not easily applicable to all Member States, which have specific national legislation. It is problematic to give a general recommendation at EU level, which needs to be subsequently transposed into national legislation.

Based on the information gathered and evaluated, we recommend to the eHealth Network to take the following steps:

REC-01. Support systematic awareness-raising of citizens and health professionals in terms of proper personal data handling in healthcare and on the importance of the right of access to health information.

REC-02. Support activities for health professionals, focused on explaining the importance of proper handling of sensitive personal data and on the benefits of proper sharing and exchange of information for quality, efficiency and safety of healthcare.

REC-03. Endorse the establishment of a general framework for education of health professionals in undergraduate and postgraduate education, and lifelong learning on personal data management and protection in healthcare, as well as on patients' rights.

REC-04. Develop, in cooperation with the European Data Protection Board, interpretations and guidelines for the implementation of GDPR in specific healthcare environments. Those guidelines should be clear, intelligible and actionable.

REC-05. Encourage the establishment of national consultation and information centres for management of sensitive personal data in healthcare.

REC-06. Encourage further development of standards and guidelines for health information exchange, for example, the standardised patient summary and discharge report.

REC-07. Support cross-nation cooperation of DPOs in sharing of good practice and especially creation of guidelines for working with sensitive personal data in healthcare.

REC-08. Raise the responsibility of healthcare management to assure that health professionals know how to deal with sensitive health data and know processes and rules in medical practice related to the GDPR.

REC-09. Endorse the introduction of more precise responsibilities of healthcare provider management about responsibilities for setting internal rules for handling of health data.

REC-10. Stipulate the secondary use of health data. It is necessary to find a balance between the protection of the patient privacy and secondary use of health data for academic purposes.

References

National Data Protection legislation prior the GDPR:

1. **Ireland, Republic of.** Data Protection Act 1988. *electronic Irish Statute Book .* [Online] [Cited: 4 September 2019.] http://www.irishstatutebook.ie/eli/isbc/1988_25.html.
2. **Latvia, Republic of.** Personal Data Protection Law. [Online] [Cited: 4 September 2019.] https://likumi.lv/ta/en/en/id/4042-personal-data-protection-law.
3. **Lithuania, Republic of.** Law on Legal Protection of Personal Data of the Republic of Lithuania. *REGISTER OF LEGAL ACTS.* [Online] [Cited: 4 September 2019.] https://www.e-tar.lt/portal/en/legalAct/TAR.5368B592234C/nXrXPXRvgP.
4. **Slovenia, Republic of.** The Law on Personal Data Protection. *Legal Information System.* [Online] [Cited: 4 September 2019.] http://pisrs.si/Pis.web/pregledPredpisa?id=ZAKO3906#.

Legislation implementing GDPR on the national level:

5. **Estonia, Republic of.** Personal Data Protection Act. *Riigi Teataja.* [Online] [Cited: 4 September 2019.] https://www.riigiteataja.ee/en/eli/523012019001/consolide.
6. **Serbia, Republic of.** Закон о заштити података о личности. *Pravno Informacioni Sistem.* [Online] [Cited: 4 September 2019.] http://www.pravno-informacioni-sistem.rs/SlGlasnikPortal/eli/rep/sgrs/skupstina/zakon/2018/87/13/reg.

Appendix A: Questionnaire

Survey Question	Comment
Identification and contact details	**Basic identification of the survey respondent for the possibility of further clarification of provided responses or follow-up questions if necessary.**
E-mail address	Contact information
Full Name	Contact information
Institution / Organisation	Contact information
Type of Institution / Organisation	Some of the questions are specific in relation to the type of the institution for which the answers are collected, identification of the institution/organisation type aims to help with the interpretation of such answers.
Work Phone	Contact information
National Legislation on Personal Data Protection	**This section focuses on information regarding national legislation on personal data protection**
Was there (in your country) any legislation regarding personal data protection in place prior to GDPR? If so, please provide a short description (up to 1000 characters) and an English translation where possible.	According to Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, each EU member state was required to have personal data protection law in place, the legislation was of varying nature and extent, the question aims to gather information on the state of personal data protection regulation before GDPR was introduced.
Legislation implementing GDPR on national level	**This section focuses on information regarding national legislation on personal data protection**
Is there any legislation implementing GDPR in place as of today? If so, when was it passed? Please provide a short description (up to 1000 characters) and an English translation where possible.	GDPR expects member states to implement country-specific legislation addressing particular areas defined within GDPR as well as any other areas national legislation would consider relevant. The question aims to gather information on such legislation.

Survey Question	Comment
If not, is it planned to pass such legislation and in what time frame? What is the key reason for the delay?	National legislation is expected to be passed by GDPR itself to adjust particular areas according to the needs of individual member states. The question aims to find out what the time frame is for such legislation to be passed and what the main reasons are if it was not passed during the implementation period of GDPR.
What does / will the legislation regulate within the framework for national regulations defined by GDPR? (which particular areas of personal data protection prescribed for national regulation by GDPR are addressed, what other areas not defined by GDPR are covered)	This question aims to find out the specific areas regulated by the national legislation.
Is there any relevant legislation other than GDPR and its implementing legislation or any generally implemented standards relevant for personal data protection in the healthcare sector in place? If so, please provide a short description (up to 1000 characters) and an English translation where possible.	This question aims to find out the specific areas regulated by other local regulatory frameworks.
Enforcing GDPR	**National supervisory authority according to Article 51 of GDPR**
Which is the supervisory authority responsible for monitoring the application of personal data protection legislation on the national level?	This question aims at identifying the national supervisory authority as described in Article 51 and the following articles of the GDPR.
Are there so far any experiences or other outcomes of problems / issues / incidents / infringements / penalties regarding the Personal Data Protection legislation and its implementation? If so, please provide a short description (up to 1000 characters) and an English translation where possible.	This question aims to find out whether there are so far any results of the regulatory oversight by the National Supervisory Authority in terms of identified breaches of personal data protection and what were the consequences of the identified misconduct.
National Legislation on Health Records	**This section is focused on legislative regulation of health records and patient data**
Is there any specific legislation regarding patient data, healthcare documentation, electronic health records, etc.? If so, please provide a short description (up to 1000 characters) and an English translation where possible.	This question aims to find out what legislation applies to handling of patient data.

Survey Question	Comment
What are the key provisions of the above-mentioned legislation in terms of data formats and standards of patient data, healthcare documentation, electronic health records, etc.? Please provide a short description (up to 1000 characters)	This question aims to find out specific impacts of legislation related to handling of patient data on formats and standards applicable to this data.
What are the key provisions of the above-mentioned legislation in terms of handling and use of patient data, healthcare documentation, electronic health records, etc.? Please provide a short description (up to 1000 characters)	This question aims to find out specific impacts of legislation related to handling of patient data.
What are the key provisions of the above-mentioned legislation in terms of exchange and sharing of patient data, healthcare documentation, electronic health records, etc.? Please provide a short description (up to 1000 characters)	This question aims to find out specific impacts of legislation related to sharing and exchange of patient data.
What are the key provisions of the above-mentioned legislation in terms of storage and disposal of patient data, healthcare documentation, electronic health records, etc.? Please provide a short description (up to 1000 characters)	This question aims to find out specific impacts of legislation related to storage and disposal of patient data.
Key impacts of GDPR implementation on Healthcare **Please provide a short description (up to 1000 characters) of impacts on rights, obligations and/or other aspects of GDPR implementation on particular groups listed in questions below regarding their work with patient data, healthcare documentation, electronic health records, etc. in connection with providing healthcare services.**	**This section is focused on key impacts GDPR has on particular groups of professionals or organisations in healthcare.**
What are the key impacts of GDPR implementation on health professionals (doctors, other health professionals, etc.)? (Should this question be irrelevant to your organisation, please indicate so)	This question relates to health professionals.
What are the key impacts of GDPR implementation on emergency healthcare	This question relates to emergency healthcare providers.

Survey Question	Comment
providers? (Should this question be irrelevant to your organisation, please indicate so)	
What are the key impacts of GDPR implementation on healthcare providers (hospitals, clinics, medical practice owners, pharmacies, etc.)? (Should this question be irrelevant to your organisation, please indicate so)	This question relates to healthcare providers.
What are the key impacts of GDPR implementation on healthcare insurance providers? (Should this question be irrelevant to your organisation, please indicate so)	This question relates to healthcare insurance providers.
What are the key impacts of GDPR implementation on national authorities and organisations collecting patient data, healthcare documentation, electronic health records, etc.? (Should this question be irrelevant to your organisation, please indicate so)	This question relates to national authorities and organisations.
Lawfulness of personal data processing in healthcare. Please provide a short comment (up to 1000 characters) • Consent • Performance of a contract • Compliance with a legal obligation • Protection of a vital interest • Public interest or exercise of an official authority • Legitimate interest	What is a key legal basis for personal data processing in healthcare according to GDPR in case of particular types of providers (tick all that apply as major legal reasons for personal data processing in healthcare)? • Health professionals • Emergency healthcare providers • National authorities and organisations
Patient Data, Healthcare Documentation, Electronic Health Records in practical use	**This section is focused on the use of patient data in each phase of its lifecycle.**
What is the prevailing form for patient data, healthcare documentation, health records? (paper/digital/combined) • in major hospitals • in specialised practices and clinics • in primary care	This question aims to find out the extent of patient data digitisation.

Survey Question	Comment
What regulatory obligations (other than GDPR related) are in place related to the use / handling / exchange / sharing / storage of patient data, healthcare documentation, health records (e.g. compulsory exchange, storage or use in certain situations)?	This question aims to identify key legislation and other regulations applicable to patient data.
How are the above-mentioned obligations related to the use / handling / exchange / sharing / storage of patient data, healthcare documentation, health records fulfilled in practice?	This question aims to identify how key legislation and other regulations are applied to patient data.
If there is no particular regulation besides GDPR in place, how are obligations related to the use / handling / exchange / sharing / storage of patient data, healthcare documentation, health records fulfilled in practice?	This question aims to identify what key principles are applied to patient data in situations where there is no applicable legislation.
How has the GDPR and related legislation affected the use / handling / exchange / sharing / storage of Health Records? (e.g. were there any processes or tools that had to modified significantly or are no longer available due to GDPR implementation?)	This question aims to identify what the key impact of GDPR on the above-described legislation and its implementation was.
Are there any challenges in implementation of GDPR and relevant national legislation in terms of patient data, healthcare documentation, health records and its use / handling / exchange / sharing / storage?	This question aims to identify what problems are met during the implementation of GDPR and related national legislation.
Access to Patient Data	**This section is related to the access of patient data in various circumstances**
What are the implications of GDPR and related legislation on patients' access to their own patient data, healthcare documentation, electronic health records?	This question aims to find out how patients' access to their own data is granted.
How is the access to patient data, healthcare documentation, health records without the consent of the patient implemented in the legislation?	There are certain situations when it is not possible to obtain patients' consent to access their medical history and other personal data. This question aims to find out what tools, procedures or other measures are implemented to circumvent patient consent in

Survey Question	Comment
	such situations and what protective measures are in place to prevent misuse of such tools and procedures.
On what level is a unique Patient ID implemented? • Patient ID unique on a national level • Patient ID unique on a regional level • Patient ID unique on a level of a healthcare provider • Patient ID unique for every case of a healthcare service • Other	This question aims to find out whether there is some form of unique Patient ID implemented and on what level is it unified / shared.
Execution of Rights of the Data Subject	**This section is related to personal data other than data on the course and outcomes of provided health care services.**
What defines rules for execution of a right to rectification (please describe how the right is implemented by healthcare providers)?	Question related to the right to rectification according to Article 16 of the GDPR.
What defines rules for execution of a right to erasure (please describe how the right is implemented by healthcare providers)?	Question related to the right to erasure according to Article 17 of the GDPR.
What defines rules for execution of a right of access (please describe how the right is implemented by healthcare providers)?	Question related to the right of access by the data subject according to Article 15 of the GDPR.
Practical impacts of GDPR on Health Records	**This section is related to implications and impacts of implementing GDPR in the healthcare environment**
What are challenges that prevent any group of stakeholders in healthcare from fully implementing GDPR?	This question aims to find out whether there are any problems preventing the full implementation of GDPR.
Are there any excessive costs or other types of induced resource consumption due to implementing GDPR that seem to be inadequate in the context of healthcare services? (either in context of your organisation or in healthcare sector in general)	This question aims to find out if the full implementation of GDPR is prevented by lack of available resources.
What is the estimated cost of GDPR implementation? (Please state cost relevant to	This question aims to quantify the overall cost of GDPR implementation (analysis, change of processes, information systems, etc.) and the

Survey Question	Comment
your institution, or nationwide if you are a ministry or a government agency)	increase of operational expenditure related to GDPR adoption.
Are there any other obstacles to GDPR implementation (e.g. personnel capacity, cybersecurity issues, etc.)?	This question aims to find out if there are any obstacles preventing full GDPR implementation and compliance other than direct financial costs.
What are the expected benefits to be derived from the general adoption of GDPR and related national legislation?	This question aims to find out what benefits may arise from GDPR implementation.
Known challenges for implementing GDPR in the Healthcare Sector	**This section aims to identify key problems related to implementing GDPR (obstacles, challenges and problems addressed during the implementation) and key problems related to GDPR being implemented (complications and problems in day to day operations resulting from GDPR implementation).**
What are the key issues and challenges related to implementing GDPR in the healthcare sector?	This question aims to identify main challenges in the healthcare sector.
How are these issues addressed at the healthcare providers level?	This question focuses on issues at the level of particular organisations and their perception of GDPR.
How are these issues addressed on national level and in national legislation?	This question focuses on issues at the national level in terms of policy and legislation and the challenges faced.

Appendix B: Benefits of the GDPR identified by respondents

What are expected benefits derived from the general adoption of GDPR and related national legislation?

- Harmonisation on federal and state level (state data protection and hospital laws); if done properly.
- Better organisation and security of data. Trust of clients.
- We have no information regarding this question.
- No major changes, so no major expected benefits. A level of awareness of this area was however raised among the patients and general public.
- In general, more transparent processing of personal data and greater emphasis given to protecting the fundamental rights of individuals.
- Health data is processed more transparently and responsibly. More and more health care professionals and other members of staff gain new expertise on personal data protection, patients are more interested about protection of their personal data. Since the Regulation came into effect, the culture of personal data protection has attained very high standards.
- The expected benefits derived from the general adoption of (this poorly formulated) GDPR is indeed questionable, and those derived from related national legislation is compliance with GDPR (and thus avoidance of an infringement proceeding before the ECJ).
- Raising of awareness.
- More emphasis on data protection rules, more transparency in Europe
- Compliance, higher levels of security, more reliable systems, protection of privacy, implemenation of data protection principles.
- Increased awareness of individual's privacy rights, of importance and value of personal data. Increased awareness of cyber security requirements, resulting in harmonisation of processes and practices.
- The principles and rules on the protection of individuals with regard to the processing of their personal data should respect their fundamental rights and freedoms, and in particular their right to the protection of personal data, regardless of the nationality or residence of individuals. The implementation of the General Data Protection Regulation will contribute to the establishment the area of freedom, security and justice, and the economic union, economic and social progress, strengthening and rapprochement of economies in the internal market and the wellbeing of individuals. Strengthening and detailed determination of the rights of respondents and obligations of those who process and determine the processing of personal data, as well as the equal powers of monitoring and ensuring compliance with the rules for the protection of personal data and equal sanctions for violations in Member States, will ensure the effective protection of personal data across the Union.
- Common attitude to data protection.
- Defined rules for health data collection, procesing, security, protection and use.
- A safer and more robust environment, awareness of the importance of patient's rights for protection of their data.
- A reinforcement of the data protection/privacy rights, customer in control of their own data.
- Data controllers will have to be much more specific regarding the purpose of data processing; they will need to provide more detailed descriptions to data subjects about the processing of their data.
- Above all, we are facing problems because the existing national legislation is not fully harmonized with GDPR. In our opinion, there are benefits in terms of raising awareness of all stakeholders. Patients are more cautious of the importance of their personal data.
- To establish and guarantee secure access and exchange of health data on a national level.
- Unknown
- The importance of ensuring the protection of personal data has been demonstrated and the regulation of personal data protection has been harmonized.
- A clear legal basis for both sides - our organization and supervisory authority.
- Secure data processing.
- In our view the main benefits are unified rules on personal data processing at EU level and a clear definition of personal data processing – any operation of personal data (Article 4, 2). Also, an important role of Data Protection Officer. GDPR counseling and education of the employees is a permanent activity in our organisation.

- Satisfaction.
- Protection of private life, greater trust in CASMB regarding the protection of personal data/informations.
- Greater security of personal information and bigger concern while working with personal data.
- Increased awareness and vigilance in the treatment of personal data. Review of systems.
- An advantage should be the better protection of personal data based on common European rules. E.g. in trials of medicinal products, parties of different countries shall proceed from the same rules and the same source document. Otherwise, a party should study and interpret the national law of the country of the other party in each case, and the dispute would be longer and more complicated.
- More focus on personal integrity, legal compliance, data protection.

Appendix C: Key issues identified by respondents

What are key issues and challenges related to implementing GDPR in Health sector?

- Lack of harmonisation on state level (state data protection and hospital laws); legal uncertainty of care providers (lack of capacity and knowledge); uncertainty about the validity of consent in provider - patient setting; legal uncertainty regarding anonymisation of health data
- Hospital and Medical centers legislation to include GDPR legislation and security issues.
- The GDPR compelled data controllers by way of doing internal audits to review how they collect personal data, for what purpose and etc. One of the biggest challenges is finding personnel with knowledge of how the health sector should process personal data. Also, the health sector has to invest in personal data protection training so that staff knows how they should act so that the requirements of the GDPR would not be infringed. There are challenges regarding day to day work of health care service providers, e. g., should patients be called out loudly by name and surname; should health records be kept near hospital beds and etc.
- None since no major changes were introduced. Additional employee in charge for the area.
- The disparate nature of service provision across sectors (public health, private health, voluntary hospitals). The lack of connected health information systems.
- Literacy of healthcare staff and patients in this field. Lack of human resources at local level, lack of resources to ensure proper monitoring.
- Even from MoH perspective too early to answer because GDPR often unclear, only few literature and hardly any jurisprudence yet.
- Data protection officers.
- Resources. Complexity of the GDPR.
- Lack of human and financal resources. Lack of competences.
- Many laws regulating particular healthcare activities contain provisions on the management, storage and exchange of data from medical records and it is necessary to align it in practice with the provisions of the General Data Protection Regulation.
- Patients refusing to consent slow down or even stop healthcare services.
- Medical studies organization with limited access to patient data
- Good understanding on all actors in health care system (patients, health providers, health managers, analysts…) of importance and benefits.
- Supervisory authority considers possibility to look and read patient's data in health databases problematic because it is one of the major concerns and problems that also receives DPA's attention due to data subject's complaints (if patients find out or consider their data has been looked in the databases unlawfully/without purpose/just out of curiosity).
- On the one hand, the biggest challenge is to ensure data security and effective supervision. Supervisory authority considers possibility to look and read patient's data in health databases problematic because it is one of the major concerns and problems that also receives DPA's attention due to data subject's complaints (if patients find out or consider their data has been looked in the databases unlawfully/without purpose/just out of curiosity). To do this, the controller needs to improve the traceability of data processing - for example, to ensure the traceability of his / her processing through the display of logs, to create control mechanisms that are based on loges and automated, etc. It is certainly helpful to share different new technical solutions here. The availability of resources is different for different service providers. This is the question of whether and to what extent the public sector itself can take the lead role to help. The restriction of different rights, where certain roles see only the kind of information that they need, helps to avoid excessive or unintended data processing. At the same time, however, it is highly dependent on the resources of the service provider and who is currently using the information system. The ability and knowledge of different providers is definitely different. From the ministry's point of view, it is important to have guidelines and certification processes that harmonize different ways and methods.
- No clear guidelines on how the GDPR must be enforced, no clear testing and certification possibilities. Costs. Lagging eID discussions - we need decisions on this topic to be able to move forward. No standardized solutions on authentication , authorization, consent, logging. Prioritisation by management, costs of compliance, dependence

on a few big suppliers, no certification for organisations, no certifcation for DPOs, lack of authority and measurements taken by the AP.

- To obtain consent for additional use of patient's data is challenging.
- Identification of personal data being collected; analysis of the existing data protection state-of-the-art; taking organizational and technical measures related to personal data handling
- Existing national legislation will have to be harmonized with GDPR in order to enable easier implementation of GDPR in practice. A unanimous interpretation and understanding of GDPR needs to be achieved. There is a need to provide information to and raise awareness of data users, data processors, data controllers (all stakeholders – healthcare insurance providers, healthcare service providers and insured persons/citizens)
- User authentication and authorization by means of digital certificates. Challanges related to certificate management.
- A resilient approach to cyber security. Breach detection and prevention. Malware protection. Cyber resilience.
- There are probably a few aspects to mention: finance, human resources, lack of common practice, lack of staff working with patients, lack of knowledge and skills in personal data protection, lack of knowledge and skills of patients and their relatives in the area of personal data protection.
- There is almost no possibility to consult with supervisory authority with specific questions, there is a lack of official explanation in documents. Some explanation documents of the Article 29 Working Party are too late or still do not exist. We implemented GDPR requirements based on our understanding of GDPR, some consultations with private consultants. We are not sure that everything is implemented correctly, as no audit from supervisory authority we had.
- Ensure efficient and fast health care while respecting the privacy policy.
- Our organisation has 8 business units operating on 14 locations. It is of utmost importance that equal data processing practices are performed everywhere, and it is a challenge to ensure unified principles in all organisational units. Another issue is destruction of documents. Although we have well defined means of destruction, there are no clear rules for retention periods according to GDPR. (This issue refers to documents other than healthcare documentation, as for the later retention periods are clearly defined by national legislation.)
- How to fully protect personal information, especially when there is conflict between the public interest and the protection of personal data of a patient.
- Keep awareness at a high level. Vigilance when systems and applications change. Building integrity protection in a constitutive way poses special challenges, such as in connection with information transfer from the healthcare sector.
- Before the enforcement of the general regulation, the hospital ordered an audit for assessing compliance of the available documentation with the requirements of the general regulation. The conclusion submitted by the auditor has provided the basis for developing operational rules. At the same time, there could be a common national standard or policy for hospitals, which would provide the hospitals with common instructions for processing personal data. This would simplify the assessment of risks and the implementation of measures. Based on prior experience, it can be said that hospitals implement the general regulation differently. For example, in the case of contracts with a similar content, the data protection regulation has been implemented in different ways in various Estonian hospitals. Thus, a situation arises where the same personal data of patients are protected differently within the framework of the same contract (for a service, etc.).
- Lack of time and personnel resources

Appendix D: List of countries participated in the Survey

17 countries participated in the Survey:

Austria
Croatia
Cyprus
Czech Republic
Estonia
Finland
Germany
Ireland
Latvia
Lithuania
Netherlands
Portugal
Romania
Serbia
Slovakia
Slovenia
Sweden