

Compliance Management of GDPR in Healthcare Environment (University Medical Centre Ljubljana Case)

Marko Zebec Koren

University Medical Centre Ljubljana, International School for Social and Business Studies,
Slovenia

marko.zebec-koren@mfdps.si; marko.zebec@kclj.si

Abstract. The article presents the starting points and activities of the University Medical Centre Ljubljana before and after European parliament adopted EU Regulation on Personal Data Protection in May 2016. UMC Ljubljana has designed/developed a four-dimensions scheme to help ensure compliance. Thus, we are dealing with the normative level, the procedural level, the technological level and the cultural level. Many of us are involved in the process of dealing with personal data. Many of us are involved in the process of dealing with our personal data, donating personal data, and sometimes selling it to corporations and institutions, at the same time. However, we can be the ones who in our professional environments encounter the personal data of other individuals and look at them, collect them, delete them, in short, process them. The EU regulation on personal data protection (with the "infamous" abbreviation GDPR) brings before us, on the one hand, a fundamental consideration of the nature and role of personal data and, on the other hand, a wealth of challenges, dilemmas, concerns and activities related to this area. The starting point in understanding the protection of personal data is "I am the owner of my personal data". To process personal data, each organization must have a legal basis. The collection and processing must be compliance with legal obligation, personal consent, contractual relationship, legitimate or public interest and protection of the vital interests of the individual. The collection and processing of personal data must be as small as possible and proportionate in regard to the purpose of the collection of the data. The data controller or processor of personal data must protect my data well enough. Thus, we can establish a framework here that gives us a tool in assessing and establishing the field of personal data protection.

Keywords: GDPR, compliance, personal data, data controller, data processor, 4-dimensions GDPR scheme

1 Introduction

The motive for writing the article was the challenge of taking over the DPO function at UMCL. I was faced with an extremely extensive and complex situation and the design of the GDPR model is actually a response to situation and an attempt to have a better control over the field. At the same time, the article is an opportunity to share good practices in academic and professional environment.

The main goal was to present the design, construction and implementation of the GDPR model.

In process of designing the model, we used the method of studying the relevant professional and scientific literature and our own analytical-synthetic consideration. We use periodic analyzes and on-fly changes to change and transform the model.

2 Quick introduction to Privacy

J. Moor –

” An individual maintains his privacy in relation to others if and only if the situation is such that individual is protected from interference, intervention and access to information.”

H. Arendt –

“private sphere is an area where the individual is safe and hidden from the world. If the private sphere narrows only to intimacy, the individual is left with only his own subjectivity, which leads to dehumanization, deindividuation of individuals and to “fatal, sterile passivation”.

E. Snowden –

“Data isn't harmless. Data isn't abstract when it's about people. It's not data that's being exploited, it's people that are being exploited. It is not data and networks that are being influenced and manipulated, it is you...” “The problem isn't data protection; the problem is data collection”

The starting point in understanding the protection of personal data is: “My data is my property”.

To manage and process them, we must have a legitimate purpose on unambiguous basis: in legislation, personal consent, contractual relationship, legitimate or public interest and protection of the vital interests of the individual. The collection and processing of personal data must be minimal and proportionate to the purpose. The controller or processor of personal data must protect my data well enough. Thus, we can establish a framework here that gives us a tool in assessing and establishing the field of personal data protection. These are four basic questions (urfragen):

1. For what PURPOSE do we process personal data?
2. Do we have a LEGAL BASIS for processing personal data?
3. Do we process personal data to the MIN. EXTENT possible (data minimization principle)?
4. How well do we PROTECT personal data?

The enactment of the regulation is one of the major social experiments of modern society (except of covid19), or at least in EU. At the same time, it may be the last serious attempt to preserve the privacy and anonymity of the individual as a human right and value.

The University Medical Center Ljubljana is probably one of the largest mass processors of personal data in Slovenia (530 million € budget, 8.700 employees, 2.200 Patient beds; 120 K In-patient admissions; 740 K Out-patient visits). Most personal data in our institution has the status of special categories of personal data (all health data is special personal data). We must handle, process and protect this personal data with particular care. This is not only a legal obligation, but also a fundamental ethical consideration and commitment of every individual employee in health care.

At the same time, it is true that for the vast majority of personal data that we process in healthcare, we already have a legal basis in sectoral legislation (Zakon o zdravstveni dejavnosti - ZZDe, Zakon o nalezljivih boleznih - ZNB, Zakon o zdravilih - ZZdr, Zakon o preskrbi skrvjo - ZPKrv, Zakon o lekarniški dejavnosti – ZLD, Zakon o zdravniški službi - ZZdrS, Zakon o duševnem zdravju - ZDZdr, Zakon o zbirkah podatkov s področja zdravstvenega varstva – ZZPPZ, Zakon o zdravstvenem varstvu in zdravstvenem zavarovanju - ZZVZZ, Zakon o pacientovih pravicah – ZPacP, ...). The transition to the postGDPR period was carried out efficiently and appropriately in view of the urgent requirements of the GDPR, and we all have a lot of work and efforts to ensure overall compliance. UMCL have a good normative framework, which was supplemented with a new Privacy Policy before the GDPR came into force.

This policy, which is the umbrella document and commitment of the organization, defines the methods of collecting personal data, the purposes for which we collect them, the security measures to protect them, the persons with whom we share them, the legal basis, the retention period and your rights regarding protection of personal data. The policy applies to all stakeholders: patients, visitors and companions, employees, employees of contractual partners, volunteers, and users of the website www.kclj.si.

Already in April 2018, a new function of the Data Protection Officer (DPO) was introduced, and a common e-mail address for information or requests regarding personal data was published on the intranet and on the website. All employees can contact the DPO with their questions, dilemmas and suggestions related to the field of personal data protection. Basic information on the GDPR and the impact on the operation of the UMCL can also be obtained by employees on the intranet. One of the DPO basic principle in handling GDPR in UMCL is: as little interference as possible in the processes of health care and other work/business processes. Of course, there is a dynamic tension here between ensuring legality and, on the other hand, implementing effective processes.

The novelty brought by the EU regulation is also Notification of a personal data breach to the supervisory authority. The deadline to proceed notification to the Information Commissioner is 72 hours. As soon as an incident/intrusion/removal is detected, it is necessary to start the procedures - In UMCL Ljubljana we have the procedures defined in the internal act of the UMCL Incident Management Policy (http://www.intranet.kclj.si/admin/dokumenti/000012bd-00002826-nd_ukcl_ip_0306_politika_upravljanja_varnostnih_incidentov_2015-10-05.pdf). When there is an inspection by the ICO, one of the key elements is the full cooperation of the institution with the Information Commissioner. In the process of inspection, it may be crucial that we act as meritoriously as possible, that we have prepared documentation, that we know how to justify the situation and the procedures we carry out convincingly enough.

For the purpose of establishing compliance with the EU regulation, a scheme with four basic levels was created at the UMCL - the normative level, the process level, the technological level and the cultural level (see Figure 1).

Reasons for building the GDPR model: to make a better control, a scale of the GDPR field, complexity of the GDPR field and specificity in HC environment (medical records, human dignity - delicate situations – abortions, HIV, COVID19...)

1. At the normative level, the focus is primarily on providing or updating personal consents for the processing of personal data and the harmonization of internal acts.
2. At the procedural level, we regularly encounter claims for the exercise of the rights of individuals guaranteed by the Regulation: The right of access of the data subject, the right to rectification, the right to erasure, the right to limit processing, the right to data portability, the right to objection and automated decision-making.
3. At the technological level, the GDPR introduces a more rigorous requirement to provide t. i. full audit trails. This means that any access to personal data files must also be recorded. All interventions of IT administrators must also be recorded. t. i. privileged users. UMCL introduced at the end of 2018. i. PAM system (Privilege Access Management). From 2019, we will try to implement in practice the requirements provided by the ISO 27001 standard (information security management system).
4. The GDPR also regulates the protection of unstructured personal data. At UMCL, we have a huge amount of data on our workstations, laptops, email inboxes, shared network folders. Personal data is in early excel spreadsheets, word documents and the like. At the level of raising awareness of the importance of personal data protection and education, each of us can move a stone or a rock. It is right that we are beacons and guardians of this human right and value. It doesn't matter what happens to our data. Who has access to them, what does he do with them, to whom does he (give) them. At UMCL, we provide intensive training at both the horizontal and vertical levels. All new employees listen to a lecture on the basics of information security and personal data protection. We are also thinking about other forms or.

methods of raising awareness and raising awareness (video clips, ...). One of the focus in GDPR course is also emphasis that insight (typical in clinical IS) is also the processing of personal data. Unauthorized access to personal data may result in termination of employment

2.1 GDPR in time of pandemic

Under the guise of an epidemic (COVID-19) standards are falling – looking for shortcuts in the field of privacy. Such as Tracking Apps (inter/intra national, interorganizational) without or on shaky legal ground and collecting personal data in stock, using thermographic cameras on entrance - integration with face recognition and T&A IT system.

Border GDPR cases in healthcare – example: covid19 questionnaire for outpatients. Are this data part of medical record? Is there established minimal set of personal data?

Digital - remote/analogue – in situ DPO activities

At the time of covid19, we at UMCL were forced to transfer some activities related to the field of personal data protection into digital/remote form.

On-line	Analogue	Both
Personal consent review, DPIA & DPA & Records of processing activities, Audit trails analysis, Meetings	Internal audits, In-situ ad hoc inspection, ICO inspection support	Education, GDPR issue advisory, Request management, Incident management, Notification of a personal data breach

Elements of a DPIA:

- Date of assessment
- Who made the assessment
- DPO
- Process name
- The purpose of the process
- legal basis for OP processing
- Source OP
- In which locations is the process of marking the OP carried out
- Who is affected by the processing of the OP
- data deletion process
- workflow description
- what is the risk for processors?
- What measures have been taken to insure entities and their rights?
- What additional measures will be introduced to ensure risk reduction / elimination
- Date of next inspection

Privacy by design / data protection by design:

For each new solution or project: there is a legal obligation to incorporate this concept - at the beginning of the preparation of the solution - not post festum.

Internal audit:

It can be unannounced!

According to various criteria:

- By organizational unit
- By form/type of medical documentation
- By problem sets (storage period, destruction, forms, research)
- By way of processing (acceptance-release, orders, discharge letters)
- By collections (archive, current collection)

2.2 Key points of managing GDPR in UMCL

- Raising awareness of personal data protection
- Reconsideration of concept: prevention vs. repression
- Close cooperation and frequent consultation with national ICO

3 Conclusion

More than two and a half years after the entry into force of the EU regulation, practices and precedents in the field of personal data protection are still being established.

This is one of the reasons why UMCL regularly escalates dilemmas and borderline cases to the Information Commissioner's Office and asks for his opinions and interpretations.

In addition, we are in contact with the Medical Ethics Commission, as one of the important entities in setting practices and precedents.

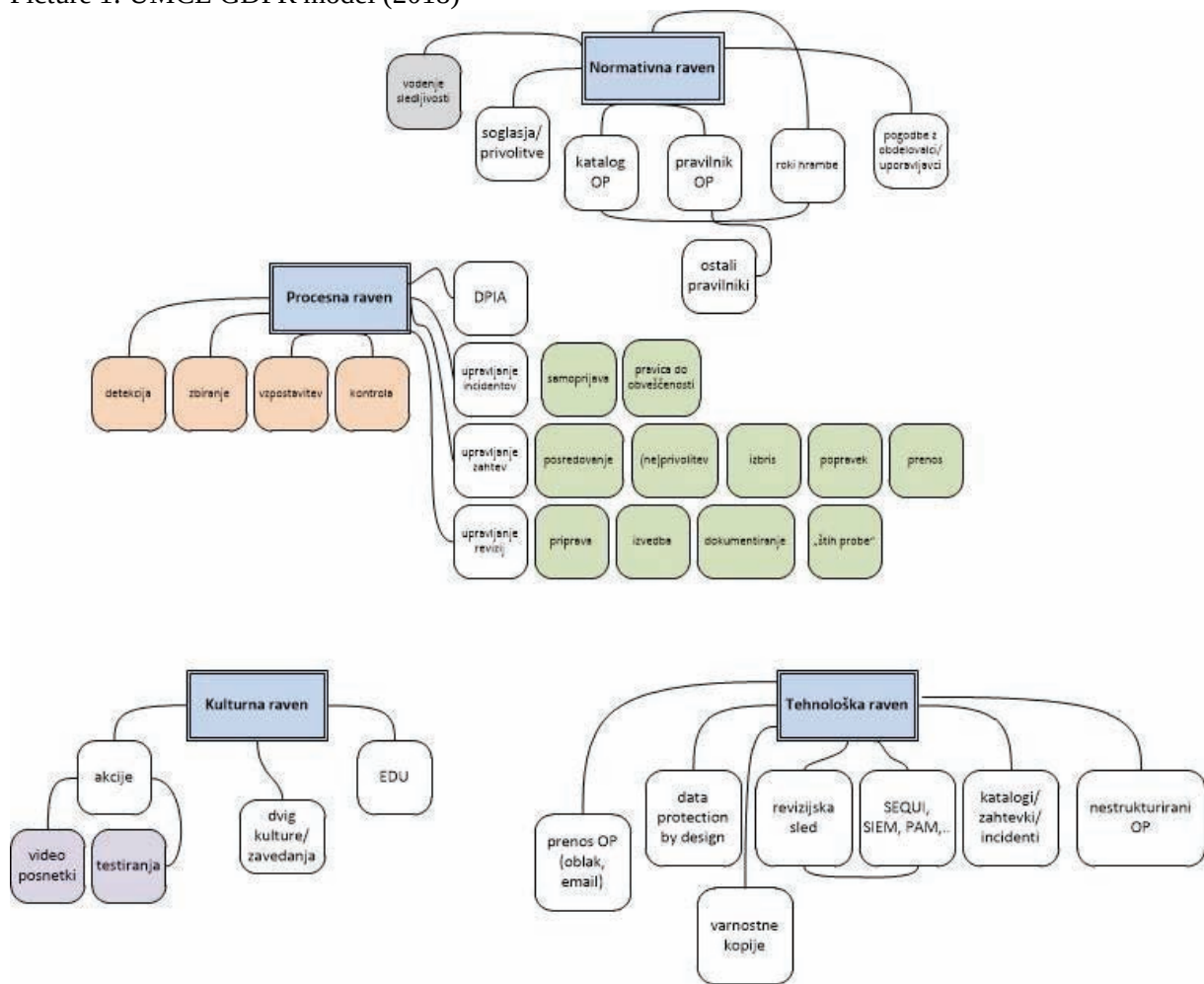
Inter Arma Enim Silent Leges."
"In times of war, the law falls
***silent.**"*

(Cicero)

Reference:

1. UREDBA (EU) 2016/679 EVROPSKEGA PARLAMENTA IN SVETA <https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX%3A32016R0679>
2. Marko Zebec Koren: GDPR – Moji podatki so moja last – primer UKCL In: Zbornik predavanj ZDRAVA USTA ZA ZDRAVO TELO 27. strokovni seminar 5. 4. – 6. 4. 2019 Grand hotel Primus Terme Ptuj; <https://www.zbornica-zveza.si/wp-content/uploads/2019/11/Zbornik-Zdrava-usta-za-zdravo-telo-2019.pdf>

Picture 1: UMCL GDPR model (2018)



Picture 2: GDPR model (2020)

