Gradus Vol 5, No 2 (2018) 348-354
ISSN 2064-8014

WHAT A WORLD IS COMING? GDPR, OF WHICH EVERYONE SHOULD KNOW

Terez Nemes[1*]

[1] Department of Methodology of Budapest Business School Budapest

Keywords:
GDPR
personal data
data management
regulation
Article history:
Received 01.August 2018
Revised 04.September 2018
Accepted 01.Oktober 2018

Abstract
Since May 25, 2018, fundamental changes will have to be made in the field of digitally managed data. This means, that any company, organization, institution, office or nonprofit organization has to change their practice by then. However, it seems that many of them do not perceive the weight of the tasks, and there are a few who have not learned about it. But it was two years since May of 2016 for the preparation. But nowadays everyone is talking about it. In this paper, we would like to think carefully about what is the General Data Protection Regulation (GDPR) and why is it so important from IT perspective?
The GDPR, regulations on the protection and the free movement of such data, personal data, constituted by the European Union. GDPR has direct effect and is mandatory in all Member States. After it has entered into force, this regulation is the most important rule in the treatment and protection of personal data in all member states, except when the GDPR permits itself. The sharp practice however, also leads to a high level of fines for those who do not comply with the rules, right from the first time. And it's easy to make mistakes. Even collecting old business cards or retrieving photos in searchable form can result in punishment. There are many questions, uncertain answers, and many situations seem unsolvable. For example, storing alumni students' information in an educational institution, or if there is no privacy policy at all...

1 Introduction

Nowadays personal data of individuals represent monetary value in the IT economy. These data often provide payment options for free services or discounts for online products or services. At the same time, individuals do not seem to be fully aware of the value of their personal data. [1]

"…it should in time be understandable in broad principle by everyone, not just a few scientists." These words were written by Stephen Hawking about complete theory. But in everyday life the same quote should apply to using personal data. Data protection is a simple thing, is not it? A lot of different information about a person is accumulated, and databases are created in countless places. It would be good to know and control who, when and for what to use these data and information and for what purpose, but it may also be impossible to do so. From the proper linking of databases, a personality profile can be compiled, so everybody can be frustrated by the possibility for any purposes. But if a personality profile would be useful for detecting a crime that is closely related to us? In that case, maybe it would seem useful. But who decides on what principles? Obviously, the decision cannot be entrusted to IT professionals working with data. A correct and consistent decision is needed for legislation. Everybody has to aware of the responsibility that exists because of the data that is being

* Corresponding author. Phone.: +36 30 592 8933
E-mail address: nemes.terez@uni-bge.hu

stored. As known to many, The General Data Protection Regulation (abbreviation: GDPR) is a regulation of the European Union that protects the personal data of natural person residing in the EEA, ensures and governs for free flow of information between Member States. [5] The Regulation entered into force on 24 May 2016 and applies after a two-year grace period from 25 May 2018. Interestingly, international law practice has hitherto been unconventional, an extending regulation, and therefore mandatory for organizations operating in non-EEA countries. The new regulation aims to establish a solid and coherent legal framework, strong enforceability and close co-operation and coherence between Member States. [7] Enhance data protection awareness and ensure the widest possible enforcement of information self-determination law. The EU has precisely set the GDPR to avoid uncontrolled distribution and use of personal data in order to protect their personal data. Legislation on data protection prepares and supervises the use of well-trained lawyers. But there are many special IT situations that these lawyers simply cannot be prepared for. There is a lot of uncertain, difficult-to-resolve situations in the practice that IT faces and they need to find solutions to them. My aim is, that this paper examines the problems encountered by the introduction of GDPR from the point of view of IT professionals.

2 Problems encountered after the introduction of GDPR

The deadline for implementation passed, May 25, 2018 The EU data management regulation, the GDPR has come into force. We might think that time has passed, the solution is ready to be applied. But unfortunately, the situation is not so simple. Many people are aware of the responsibility for stored data, but their understanding of the task and solving the problems they encountered is far more difficult than the law-makers who were drafting the law. It seems likely that this is not the end of the road, but the confrontation of unresolved situations, the timing of interpretations and the likely changes and refinements. It also appears that a much wider range of new regulation is affected than ever before. There are many who have not even used the two years of preparation. [6] They are trying to solve the task at the last minute, fearing the threat of high fines. It was evident that the last days before the entry into force of the GDPR took place in the enchantments of the data management rules. Users can get to know the millions of millions of people involved in privacy and data tracking. Of course, the question is whether every addressee really knows what's going on around it. An example of this is on May 25 and the next day many posted privacy policies on websites. It seemed that many of the privacy policies sent did not meet the letter of the law, but it did not take much in the spirit of the law. It may be that most of the people in the privacy statement all only understood that they had received ten or more emails per day in their mailbox or had come to their eyes as a popup window and spoke of updating or requesting all the rules. One of them may have offered rewards for co-operation or one of the conditions set out, they were not legitimate either. Part of the problem is that only a few people read the privacy policies and if so, they can only be roughly read. In addition, if they were to read the displayed data management information, sometimes people do not understand the full text. Moreover, if they can read and understand the information provided, it still may not be aware of the consequences of the information. Finally, even if they understand the consequences, the policies and settings may not be offered the options they wish to use. Lastly, long and complicated, but legally correct, data management declarations proved to be ineffective due to the users. Experience suggests that the impact of dumping was not very positive, neither in terms of data protection nor business. The letters are opened by about a third of the recipients, not necessarily read all, and very few people sign up for newsletters, for example. Many people do not even see what they should do by asking for a letter. I think many users ignored of these letters or pop-up windows so they do not know exactly what they will not receive any more information about. A great torrent of letters and information has only just failed to understand of users that is really what it is.

As a requirement, it would be imperative to clarify that policies should be concise and easy to understand. The more information they provide to people without actually having to read and understand the whole content. [2]

In sum, experience has shown that the companies involved are often faced with serious difficulties in understanding and addressing technology-related situations from GDPR. And users are not really able to use the possibilities that the GDPR has suddenly pressed into their hands.

3 GDPR from the perspective of data controllers

In Article 5 of GDPR sets out 7 basic principles for the processing of personal data, which are the following:

- lawfulness, fairness and transparency
- purpose limitation
- data minimization
- accuracy
- storage limitation
- integrity and confidentiality
- accountability

A serious problem for the controller is to ensure the compliance GDPR, since in most cases need to think about data management practices over the ground.

Basic tasks of data controllers:

- must correctly establish the legal basis for data handling
- must enter detailed privacy information into the employment contract or privacy policy
- must request individual contributions to handle the data
- must perform an impact assessment before high-risk data processing
- keep track of data management activity
- for some companies, an internal data protection officer should be appointed
- in the event of the unauthorized data processing or destruction or loss of data, the employer has a duty to report to the supervisory authority

The principle of data saving should be used as soon as possible. In other words, it is necessary to examine the extent to which the information and the amount of data stored is necessary for decision making. [5]

A law firm recommends lawyer's eyes, that there are five initial steps to make before considering measures to take to achieve compliance. [4] These are:

- Assess whether or not you will fall within the scope of the GDPR.
- Understand the new compliance obligations, decide how to comply with them and assess their operational impact.
- Identify new responsibilities and risks and consider how to address those risks.
- Understand the market, in particular what data controllers will require from processors moving forward and what your competitors will be willing/not willing to agree to vis-à-vis data controllers.
- Devise a strategy for negotiating processing agreements.

However, the introduction of GDPR goes beyond the updating of the privacy policies. Data controllers should also think about the functioning of back-end systems and ensure that all aspects of personal data are protected as efficiently as possible. May 25 to be considered as a privacy incident if any hardware containing personal data controller is in the wrong hands, such as servers, corporate notebooks or even a thumb drive. For example, if an office is stolen one of these data storage devices. Because of the requirements of GDPR, IT professionals should do their utmost to ensure that data storage devices are physically secure as well as that personal data stored on them cannot be accessed after the device has been stolen. For example, for computers with personal data, it is recommended to use strong password and drive encryption or to create possible maximum physical protection for servers. An entrepreneur who stores a database server with tens of thousands of users' personal data in his own home uses more risk than ever before, since it is a data controller that is subject to stricter rules. Compliance with the safety guidelines is also evaluated due to GDPR. In terms of compliance with GDPR's encrypted USB drives are the ideal solution for portable storage devices. With the introduction of GDPR, there was a serious financial incentive to alleviate the risk of data leakage.

But how to prepare IT professionals involved. What can IT staff do to strengthen GDPR compliance and avoid security incidents? What IT needs to do for IT security.

- Exactly regulate the privileges of personal files, folders, and libraries, that is, only those colleagues can access the information that they have access to.

- Regularly update operating systems, applications and virus scanners, firewalls that can prevent or at least make it more difficult to access unauthorized access to data stored in the company.
- Update the hardware and associated companies, including Wi-Fi, routers, NAS-firmware regularly.
- Sensitive storage media use encrypted data storage, desktops, laptops, or hard disk servers, pendrive, external hard drives.

The new regulations concern all institutions that handle personal data, including educational institutions. The special situation of educational institutions also raises several questions. Impose a fine of up to a school where a teacher or administrative staff lose a USB stick, which can be found in students' personal data. Such a case may also constitute a security incident which entails a notification obligation. With these solutions it is obviously necessary for IT professionals perform their duties due to GDPR compliance as well. Businesses can be punished that scraps down data carriers, servers, computers, laptops, and mobile phones to stay on them, data on their customers or their associates. Repair shops can not manage personal data in the faulty devices. Every company must surely start with the data of employees, they cannot only be in the secretary's computer, the folder saved on the desktop. It should also be forgotten that CVs and emails from applicants can only be sent back and forth between a human political manager and a company manager. These personal data must be handled safely in the same way. Similarly, customers, partners, and buyers should also be treated. These personal data cannot be collected in the mailbox as the starred letters. To prevent this information from being stolen by an unauthorized person and not to make copies of it without any trace, it is not permissible to store the data in a simple folder, or whatever is stored in the e-mails, so that the data is in a moment can be transmitted without trace. Data collection can count on the business card storage, or use of corporate team building events in the photos as well. The problem is that if they are sorted in searchable form, they are already considered to be data management. Problems may profiling, the drone recording as well. A simple website may also be covered by DGPR, whether it is a Facebook Like button or a newsletter subscription, but there are less eye-catching data management such as a source code embedded tracking code. For these, personal information can be obtained from the business, for example, when subscribing to a newsletter, name, email address. In this case, it has to be complied with the provisions of GDPR. From a regulatory point of view, the IP address is also considered as personal data.

It is impossible to send unsolicited newsletters, direct marketing materials automatically. Prior consent is required to send newsletters and promotional material. The contribution, according to GDPR, can only be achieved through active behavior. This should be considered if the site visitor clicks the contributing field. It is not acceptable, for example, to practice that the square is ticking and the visitor can only leave it in the form of a consent or inattention. For private individuals to send legitimate direct marketing messages only on prior consent. However, according to the rules, the explicit request of the consent is also considered as direct marketing if the main content of the message is the request for consent. The concept of consent is defined by the GDPR in the following rather cautious way: The consent of the will of concerned voluntary, specific and informed, and a clear signal to indicate by means of a statement or confirmation unmistakably expressive act concerned to consent to treatment of personal data relating to him or her. The contribution by this is correct when active, so the person himself subscribes to check the checkbox, so it excluded the possibility that the subscriber's gaze accidentally overlook above a pre-checked boxes. The contribution also sets a requirement that has to be based on adequate information. For this reason, it is recommended to place a link to a web page, newsletter or e-mail address, and a check box in which the subscriber declares that he or she has been informed. In addition, it is important that the possibility of unsubscribing is also visible, and can be found quickly within the site. When unsubscribing, it is not recommended asking for new personal information. After unsubscribing, the user's personal data must be permanently deleted from all databases and useful when it is automatically done. But in such cases, for example, what happens to backups made to a serial access device. How the removal will happen?

According to the GDPR, cookie IDs are also suitable for identifying natural persons, thus covering the scope of GDPR. The use of cookies should therefore be given clear and accurate information in

the privacy policies of the site and the user must explicitly contribute to the use of the site cookies. Indeed, to give him or her an opportunity to change the decision, that at some point he or she can decide, it no longer contributes to the use of cookies. The cookie handling problem may be that when a visitor goes up to the site and the system checks whether his or her computer has a cookie for this website, which means that he or she has already accepted acceptance or not. It may happen that we've already looked at a cookie on his or her computer before he or she can even contribute.

According to the GDPR, the data controller and the data processor are responsible for the damage caused by data processing, so we also need to keep in mind that the data management practices of our business partners in this field are also appropriate. The partners involved in data processing must be carefully selected and monitored. The contract also rigorously settles data protection issues. Only outsourced data can be transmitted to an external partner for data processing, which is strictly necessary for the particular project or operation. If there is a way, the data must be aliased or anonymized. Correctly handling data, encrypting, preserving, destroying, or restricting access rights is a much simpler task when digitized than the documents stored on paper. A data no longer needed should be deleted immediately. It is important too, that the expiration of the retention obligation deriving from the legislation and the date of the cancellation obligation in the case of personal data documents. That is, if the retention obligation has expired, retention cannot be resumed by the organization based on the GDPR, the document must be deleted.

Problems can be, for example, the cancellation of student data in educational institutions. What can be legally deleted and what is not. For example, deleting alumni students must be resolved.

4 GDPR from the perspective of users

The rights of those concerned are governed by Articles 12-22 of GDPR. [5] These are the following:

- The right to transparent information
- Right of access by the data subject
- Right to rectification
- Right to erasure (‘right to be forgotten’)
- Right to restriction of processing
- Right to data portability
- Right to object
- Automated individual decision-making, including profiling

What counts as personal data?

Personal data is any information about a natural person that directly or indirectly identifies or identifies an individual. This includes IDs (such as ID cards, tax IDs, health insurance IDs, driver's license number, and passport number), name, nickname, username for internet registration, name-registered e-mail address, or GPS coordinate data, for example. Personal data is height, weight, hair color, spoken language, or other attribute that can be grouped by whom these attributes apply. [5]

There are also some special data.

Special data are particularly sensitive data which are only subject to very limited use. This includes, but is not limited to, health data (medicines, illnesses, final reports, and medical certificates), data on harmful passion (smoking, drug dependence), biometric data (such as fingerprints, retina), genetic data, racial or ethnic origin, political opinions, religious convictions, and sexual orientation. It is not self-evident, but it is also a special fact that someone has a trade union or a party membership. [5]

What is data management?

Collecting, requesting, capturing, organizing, tagging data is considered to be data management. All the provisions of data protection apply to those who only ask for information, but do not store or just look into personal information. Therefore, if a postal service only asks for a visitor's personal identity card as a check and does not record any data, it also performs data processing as it has access to the personal data and has known them. In the same way data manipulation is the modification, use, transmission, disclosure, linking, or even deletion of data. [5]
Collecting, using and managing personal data may only be for a definite, clear and legitimate purpose. Data management targets must be marked in the data management information by data

category and each data can only be managed for the purposes assigned to them, and cannot be used for any other purpose. For example, if an e-mail address is requested to register at a webshop, then the webshop will not be entitled to post any newsletter, bid, or sell it to anyone else at this web address. Every individual has the right to request that his data be deleted by the data controller if he so requests. This deletion has to deal with everything, so personal data will have to be deleted everywhere, as if there were never any data at that company. A cancellation request may be denied if the data is required to comply with a legal obligation.

There are many issues that are still the topic of the IoT. IoT devices often collect huge amounts of data without the stakeholders being aware of it. Smartphone sensors can be used to determine user mood and health status, stress level, bipolar disorder, family and job status, smoking habits, Parkinson's disease, sleep patterns, physical activity. They are particularly sensitive data. [3] Third parties with access to these smart things may use this information for purposes that the user does not agree with. For example, they may be relevant to prospective employers who may have undesirable conclusions from them. Other data controllers are increasingly using the Internet of Things to monitor people's online behavior as well. Users are often unable to prevent profiling because the collection of personal data cannot be verified on the IoTs. For example, in the case of the internet of things, who would such a data controller be? The household that has installed it and operates it? Or who receives the data on the gadget and makes decisions on that?

An example would be a problem of real life. A source of the problem may be that, in the case of less conscious users, some online media may restrict users' freedom of choice by persuading them to use a particular service regardless of the social or economic consequences they have. The first day of the entry into force of the GDPR, Facebook would be punished by 3.9 billion and Google by 3.7 billion euros, [6] Max Schrems, an activist for the protection of personal data, who has long criticized these companies for gathering a lot of personal information about their users. He thought he had already given the legal environment to report them. Google and Facebook believed that they had redesigned their system and judged that they adhere to all points in the new regulation. Max Schrems want to prove in court that it is not so. The GDPR text clearly states that users should actively agree to handle their data and not force users to do so. According to Schrems, Facebook and Google avoid the rules that their services are allowed only and only if the user clicks at one click to collect different kinds of data. This is clearly a compulsion, according to the activist. "They certainly know they are breaking the rules, they do not even try to hide it," said the activist at the Financial Times. In other words, service providers may not refuse the provision of digital services, following the contribution to personal data processing, which is necessary to fulfill the contract. In fact, if customers accept the compensation for the data and subsequently withdraw their consent to the processing of unnecessary personal data, it cannot be denied the provision of the digital service. As known to many, Mark Zuckerberg tangentially mentioned in a congressional hearing that Facebook is thinking of a paid version for those who do not want to pay for their service with their personal information. It would be worth analyzing who and in what proportion would be willing to pay for the various services available on the Internet in order to be more secure with their data.

5 Conclusion

May 25, 2018 EU data management regulation, The GDPR has come into force. For this, the mandatory regulation applicable in all Member States was highly needed due to the unified management of data. But there are a lot of issues that are occurring during practical application. Often, solving these problems is not possible with legal knowledge alone. The law enforcement practice of GDPR regulations is still missing and not all its issues are fully elaborated. Often, specific IT problems arise when applying the Regulation, which also require IT skills. GDPR interpretation of concepts may change in light of the information technology issues. In this paper, I tried to rethink possible problems with an informatics eye. Nowadays, the level of data protection awareness in some areas is rather low. An important consequence of the compliance with GDPR can be that major data protection incidents can no longer be concealed because they have to be reported to the data protection authority and promptly every possible action must be taken to mitigate the damage. This obligation can also increase data security awareness. By keeping GDPR, companies may be trusted

and more customer-friendly. The private users are concerned they might be more prudent in relation to the sharing of personal data. Perhaps they may also have the right to erase their personal information in the past on the web at all times and from the website. IT professionals can use their practical solutions to help to develop more efficient and cleaner law enforcement practice.

References

[1] Paul de Hert, Vagelis Papakonstantinou, The new General Data Protection Regulation: Still a sound system for the protection of individuals. Computerlaw&securityreview 32 (2016) 179–194.
[2] Sandra Wachter, Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR Computerlaw&securityreview 34 (2018) 436–449.
[3] Gianclaudio Malgieri, Bart Custers, Pricing privacy – the right to know the value of your personal data. Computerlaw&securityreview 34 (2018) 289–303
[4] Colin Tankard What the GDPR means for businesses, Network Security, ISSN 1353-4858 June 2016.
[5] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016, Official Journal of the European Union, Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML, last seen on 27 May 2018
[6] The Big GDPR Question-Answers, Available: https://7blog.hu/gdpr/, last seen on 27 May 2018.
[7] EU GDPR Information Portal, Available: https://www.eugdpr.org/ last seen on 11 June 2018.