VARSTVOSLOVJE, Journal of Criminal Justice and Security, year 20 no. 4 pp. 414–433

The Impact of the EU General Data Protection Regulation (GDPR) on Mobile Devices

Domen Hribar, Miha Dvojmoč, Blaž Markelj

Purpose:

The purpose of this paper is to examine novelties introduced by the European Regulation (2016/679) on the Protection of Natural Persons with Regard to the Processing of Personal Data (GDPR) and its key impacts on mobile device users. The paper also presents some of the main changes affecting both natural persons and legal entities. Further, certain issues that might occur while implementing the Regulation are raised together with the degree of individuals' awareness of the need to protect the personal data stored on their mobile devices.

Design/Methods/Approach:

For the purpose of this paper, we reviewed the legislation, Slovenian and international literature, brochures and media stories in the field of personal data protection. We also used a questionnaire to determine the degree of awareness of the importance of protecting personal data among the general population.

Findings:

The findings show that no revolutionary changes are introduced. Nevertheless, quite a few novelties concern data controllers and processors. In particular, penalties for breaching the GDPR are now much higher. Individuals' rights are strengthened and easier to control. In contrast, data controllers and processors are subject to more stringent duties and legal obligations. These changes also apply to mobile device users. The research findings show that individuals are relatively well aware of the concept of personal data; however, the scope of their knowledge shrinks as this concept becomes increasingly complex. Familiarity with the new Regulation (2016/679) having been introduced at the EU level was claimed by 55% of the respondents (N = 195).

Research Limitations/Implications:

The limitations stem from the selective choice of the GDPR's impact on mobile device users. More important influences are emphasised.

Originality/Value:

The findings will help both individuals and legal entities understand the changes brought to the area of data protection and tackle them more successfully.

UDC: 004.056:[342.7:621.391]

Keywords: personal data protection, GDPR, Personal Data Protection Act, mobile devices

Vpliv evropske Splošne uredbe o varstvu osebnih podatkov (GDPR) na mobilne naprave

Namen prispevka:

V prispevku smo predstavili ključni vpliv evropske uredbe (2016/679) o varstvu posameznikov pri obdelavi osebnih podatkov na uporabnike mobilnih naprav. Poleg vpliva smo predstavili ključne spremembe, ki vplivajo tako na fizične kot tudi na velik delež pravnih oseb. Poudarili smo določeno problematiko, s katero se organizacije srečujejo. Hkrati smo prikazali stanje ozaveščenosti ljudi o varstvu osebnih podatkov na mobilnih napravah.

Metode:

Prispevek temelji na pregledu zakonodaje ter domače in tuje literature, brošur in medijskih člankov na področju varstva osebnih podatkov. Izvedli smo tudi anketo, kjer nas je zanimala ozaveščenost o pomembnosti varstva osebnih podatkov.

Ugotovitve:

Na področju je prišlo do številnih novosti, ki so spremenile način upravljanja in obdelave. Predvsem se bodo povečale globe za kršitelje. Pravice posameznika bodo podkrepljene in lažje nadzorovane. Po drugi strani bodo upravljavci in obdelovalci dobili veliko novih dolžnosti. Spremembe veljajo tudi za uporabnike mobilnih naprav. Ugotovitve raziskave so pokazale, da ljudje sorazmerno dobro poznajo pojem osebni podatek, vendar se to znanje s kompleksnostjo pojma zmanjšuje. Udeleženci so v 55 % (N = 195) odgovorili, da vedo za prihod nove uredbe (2016/679).

Omejitve/uporabnost raziskave:

Omejitve so pri selektivni izbiri vpliva uredbe na uporabnike mobilnih naprav. Poudarjeni so pomembnejši vplivi.

Izvirnost/pomembnost prispevka:

Ugotovitve prispevka bodo pomagale tako posameznikom kot tudi organizacijam pri dojemanju sprememb in zato lažjem spoprijemanju z njimi.

UDK: 004.056:[342.7:621.391]

Ključne besede: varstvo osebnih podatkov, GDPR, Zakon o varstvu osebnih podatkov, mobilne naprave

1 INTRODUCTION

The present paper focuses on mobile devices and the way in which the new personal data protection legislation affects their use. This field is extremely broad and complex, which is why the paper only concentrates on certain more significant changes. Mobile devices are placed at the forefront simply because we can hardly envisage our everyday lives without them. Further, mobile devices can hold personal data that must be protected under the GDPR. If the device is

lost or stolen that constitutes a data breach. While data breaches are common, they are easier with mobile devices. This example shows that mobile devices are a weak link while trying to comply with the GDPR. Mobile devices include, among others, devices with a built-in adapted operating system. They also encompass devices able to transfer data and access the Internet wirelessly (Markelj & Bernik, 2016). Mobile device use is extremely widespread across the globe (GSMA Intelligence, 2018). The available figures are extremely high and refer to the quantity of data transferred at the global level. The need to protect such data is therefore in the interest of anyone conducting any transaction that involves any type of information.

Naturally, not all pieces of information are equally important. The value of a piece of information depends on numerous factors linked to one another, thus creating or increasing the value of information. That is why the State recognises, inter alia, that information related to individuals is a fundamental element in guaranteeing human rights and freedoms. This type of information is known as personal data and denotes "any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (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) [GDPR], 2016, Article 4). Personal data thus includes a great deal of information regarding an individual. After all, the colour of one's hair also constitutes personal data. It is also important to distinguish between protected and unprotected personal data. The 'identifiability' of natural persons plays a considerable role in making this distinction (Bolognini & Bistolfi, 2016). Information regarding natural persons not falling in the scope of the definition of personal data and, in particular, not meeting the identifiability condition does not belong to the category of protected personal data (Article 29 Data Protection Working Party, 2007). The mentioned Regulation does not apply to such information. Therefore, the Regulation only applies to information that meets the criteria listed in the personal data definition, especially the identifiability condition. With respect to identifiability, the question of who determines whether a person can be distinguished from all other individuals is crucial. Above all, the concept of identifiability must be considered in the broadest possible sense and not merely on the basis of one's own capabilities (Informacijski pooblaščenec, 2017a). The rules enshrined in the GDPR therefore apply to clearly defined cases. For instance, these rules do not need to be followed where a natural person keeps a database containing personal data for their own use. On the other hand, natural persons are not allowed to process certain types of personal data that are prescribed in other legal acts.

Mobile devices and the data stored on them are crucial for our everyday lives. The fact such data may fall into the hands of unauthorised persons is

therefore highly undesirable. The loss or unauthorised processing of any data, both conventional information as well as data stored on any information and communications technology devices (henceforth: ICT devices), is extremely unpleasant. This is particularly problematic when considering the use of ICT devices where data protection issues are even more complex. Mobile devices are exposed to various, unique risks. For instance, a mobile device is easy to lose, which potentially jeopardises all the data stored on it. Apart from external risks, individuals also tend to transfer large quantities of data whose origin, reliability and security are unknown (Hettrich, 2015). For instance, we all use various applications that are downloaded to our mobile devices, yet we are unaware or may not even care about the type of data being collected about us. Such applications often collect data they should not be collecting or may actually require less data for their normal functioning, meaning they are in full breach of the principle of minimisation (Pedro, 2016).

2 THE GDPR IN BRIEF

In April 2016, the European Parliament and the Council adopted the General Data Protection Regulation (GDPR, 2016) and the Directive on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences (Informacijski pooblaščenec, n. d.). Both legal acts pay considerable attention to the processing and management of personal data. This paper focuses merely on the GDPR, which entered into force in May 2018. The fact that technological development has brought numerous changes in the past few years was one of many arguments underpinning adoption of the GDPR. In fact, the cyber world is developing, changing and spreading extremely fast, thus demanding necessary amendments to the applicable legislation. Such legislative amendments must not restrict further development, but create an environment in which individuals are able to trust the already guaranteed human rights and simultaneously use modern technologies to freely conduct their business. The GDPR also increases the level of individuals' rights, thus serving the interests of the people. Personal data protection is extremely important for the protection of human rights and so must find its place among other fundamental rights in such a way that it will strike the right balance with other rights and freedoms.

Slovenia is in a somewhat better position than other countries, which are still dealing with a larger number of more complex issues. It must be stressed that the new GDPR contains standardised provisions for the entire territory of the European Union (EU). Hence, the level of personal data protection in countries, such as Malta, Poland and the Czech Republic, is lower than in Slovenia since they have been facing several unresolved issues already at the level of legislative discussions (Baker McKenzie, 2017). Article 38 of the Constitution of the Republic of Slovenia (Ustava Republike Slovenije, 1991) defines certain fundamental rights of individuals concerning the protection of personal data, e.g. the right to be informed of the fact that personal data related to individuals are being collected and the right to judicial protection). Personal data protection is also regulated

by the current Personal Data Protection Act (Zakon o varstvu osebnih podatkov [ZVOP-1-UPB1], 2004), which has many similarities with the new GDPR (yet also several inconsistencies, which raise the problems discussed in the conclusion of this paper). The GDPR also contains provisions on the protection of children, an area not regulated until now. Children constitute a vulnerable group which is unaware of the potential consequences of personal data collection and processing. As such, they are subject to extra protection in numerous articles of the GDPR (GDPR, 2016). For instance, the GDPR defines the age limit for acquiring a child's consent for personal data processing. Organisations therefore violate the law if they process personal data of children below the defined age limit without having first obtaining the consent of the holder of parental responsibility (Ministrstvo za pravosodje RS, 2017).

3 FUNDAMENTAL CHANGES

Even though some similarities between the current Personal Data Protection Act (ZVOP-1-UPB1, 2004) and the new GDPR may be observed, the latter introduces a series of fundamental changes. These impact the retention, processing and management of personal data, as well as the rights of individuals. Changes in the area of personal data protection can be divided into two distinct parts. The first encompasses the rights of individuals, while the second refers to data controllers and processors.

3.1 Changes Relating to the Rights of Individuals

- Greater control and a more effective exercise of control;
- Easier access to one's own personal data;
- The right to be forgotten;
- The right to information regarding the retention period of personal data;
- The right to data portability;
- The right to judicial protection and sanctions;
- Individuals must not be subjected to measures based solely on profiling, analyses or predictions obtained by the means of automated processing (Informacijski pooblaščenec, 2017b).

The right to be forgotten, which may be described as a novelty in the field of personal data protection, is merely an extension and a stronger version of the right of individuals who wish to withdraw their consent for the processing of personal data on the basis of a legal act. The right to erasure is defined in Article 32 of the Personal Data Protection Act (ZVOP-1-UPB1, 2004), albeit under a slightly different name. This field has now been altered so that it is easier for individuals to invoke their right to be forgotten and to implement their requests for erasure faster (GDPR, 2016). The same conclusion was reached by Mantelero (2013) who stated the right to be forgotten was not a revolutionary change in the current rules since Article 12 of Directive 95/46/CE (a predecessor of the GDPR) had already given a similar right. The changes thus mainly relate to the way in which this right can be invoked. The Personal Data Protection Act (ZVOP-1-UPB1, 2004) prescribes that individuals must prove that personal data were incomplete, inaccurate or

obtained unlawfully. On the other hand, the GDPR (2016) does not contain the same requirement. This new aspect may be a thorn in the side of organisations not only because they are now required to prove that the request for erasure was unjustified, but also due to the much higher fines the GDPR introduces. The impact of this change and some specific examples are presented in the following sections.

A similar situation occurs with the right to judicial protection and sanctions. Article 34 of the Personal Data Protection Act (ZVOP-1-UPB1, 2004) provides for the judicial protection of individuals' rights and the possibility of instituting administrative proceedings against certain decisions taken by data controllers. In this respect, the change refers to the fact that individuals now have to right to lodge a complaint without prejudice to any other administrative or legal remedy (GDPR, 2016). Individuals have thus obtained additional remedies for invoking their rights.

3.2 Changes Relating to Data Controllers and Processors

- Collecting personal data on the basis of consent – consent shall be provided in the form of a clear and plain language declaration and contain a clear affirmative action, which the processor must be able to demonstrate;
- The withdrawal of consent must be as easy as giving consent;
- Data controllers must consider the principles of data protection by design and by default;
- Data controllers must provide individuals with transparent and easily accessible information about the processing of their personal data;
- Obligatory notification of a personal data breach;
- Designation of a data protection officer;
- Records of processing activities;
- Prior impact assessments (Informacijski pooblaščenec, 2017b).

The applicable Slovenian law already contains a provision similar to that in indent four. Under Article 30 of the Personal Data Protection Act (ZVOP-1-UPB1, 2004), individuals have the right to be informed about the personal data relating to them. At the same time, they have the right to have their data erased if they are incomplete or inaccurate or were processed contrary to the ZVOP-1-UPB1 (2004). The novelty is that access to data is easier and simpler, with data having to be presented in an easily understandable manner. This will facilitate the operation of certain companies. If a company conducts business in several countries, the control over individual branches will be exercised by the headquarters. This will enable simpler and more consistent control operations. It will also lead to a decrease of administrative and other burdens (Voss, 2014), particularly because the GDPR applies to the entire EU territory.

4 MOBILE DEVICES AND THE GDPR

The GDPR's impact is also observed in mobile applications, particularly in relation to consent and the right to be forgotten. As mentioned, the GDPR (2016)

introduces specific conditions for giving consent to the processing of personal data. Consent must be given "in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language" (GDPR, 2016, Article 7). At the same time, the GDPR stipulates that it must be as easy to withdraw as to give consent. Some applications have already been updated in order to adjust to these conditions. This is mainly shown in the numerous requests for renewed consent. Data controllers were particularly busy with verifying the existing forms of consent (GDPR, 2016). On the other hand, this change does not pose any particular challenge for individuals but enables them to obtain information more easily and facilitates their decision on whether to continue using a specific application. This change also brings advantages for data controllers and processors since they have used this opportunity to obtain an overview of data previously collected by organisations. The approval for the processing of data has been strengthened with respect to children, who are a more vulnerable group that is presumably unaware of all potential risks arising from the sharing of personal data. According to the GDPR, children below a certain age must obtain the consent of a holder of parental responsibility to use certain applications, while such consent must not be conditional on excessive conditions set by the controller (Ministrstvo za pravosodje RS, 2017), which would prevent the child's participation in or use of an application. Social media use is a case in point. Another question here is how exactly the consent based on obtaining the parental agreement is verified (Tikkinen-Piri, Rohunen, & Markkula, 2018). Significant problems also relate to verifying the age limit. Therefore, it will be neither easy nor inexpensive for organisations to determine the actual age of users. The issue of consent might become even more complex upon the merging of different databases. The collection of certain types of data does not require individuals' consent since they are not considered personal data. However, after a given period or after databases are merged individuals may become identifiable, demanding direct application of the GDPR (2016).

Sullivan and Burger (2017) emphasise the spread of EU policy to other areas, particularly the fact EU wishes to expand its influence to third countries, thus creating a future data protection system at the international level. Users may be affected by the websites or mobile applications of providers not headquartered in the EU. Gilbert (2016) finds that the GDPR (2016) does affect companies without their headquarters in the EU when their services are used by individuals in the EU. One can thus presume that certain products or services are no longer present in the EU market or their presence has either dramatically decreased or being unlawfully provided.

Irrespective of the presence of services within or outside the EU, the new GDPR provides the clearer and more transparent processing of personal data, meaning that individuals may expect fewer unwanted advertisements, unsolicited calls and e-mails (DPOrganizer, n. d.). Data controllers will have to closely monitor how the right to erasure is being implemented as it may happen that certain information that ought to have been erased will remain in databases (Voss, 2017). For instance, "Moneysupermarket", an English company, sent 7.1 million e-mails to consumers who had previously stated they no longer wished

to receive e-mails from the company (Information Commissioner's Office, 2017). A fine of GBP 80,000 was imposed on the company. Eation (2017) claims that had the new GDPR been applicable at the time the company would have faced a fine of GBP 12.6 million for the same infringement. Apart from substantial fines, the mentioned author stresses the quality of the data, which are gradually becoming inaccurate. Users who use their mobile devices for business purposes must ensure their databases are up to date. The easiest way to achieve this is to enable remote access without the possibility of transferring personal data. In the future, remote access will become increasingly widespread. This will have a special impact on the migration of databases since data can become inaccurate quite quickly. However, if remote access is the only type of access to such databases, data controllers find it easier to update personal data, while the risk of abuse falls. Companies will mainly be obliged to check where and what type of data are stored on mobile devices, where (backup) copies of such data have been created and are being processed. Following an impact assessment, an additional level of security will have to be implemented. This is why the GDPR (2016) promotes the pseudonymisation of personal data. Additional issues relate to when smartphones used for both private and professional purposes are lost. This is acutely problematic when devices contain personal data. In this case, employees are obliged to inform their employers about the misappropriation, unauthorised access to or loss of data (Sire, n. d.). In order to avoid fines or inconvenience caused to their clients, employers are advised to erase the data remotely (Ledino, 2012). These options are regularly used in everyday practice.

Voss (2017) also notes that Article 34 of the GDPR obliges data controllers to inform individuals of a personal data breach when that breach is likely to result in a high risk to the rights and freedoms of private individuals. In terms of mobile applications, it is likely the individuals informed of such a breach will lose their trust and stop using the application. De Hert and Papakonstantinou (2016) contend such notifications would be extremely rare. They believe the relevant provisions obliging that individuals be informed of data protection breaches are quite vague since they allow a great deal of leeway for data controllers to avoid such communications.

Ducato (2016) stresses that some changes may also arise in relation to cloud computing. She finds that the environment surrounding cloud computing might become more complex, especially because of transparency and accountability obligations. Both data recipients and data controllers were forced to introduce certain changes. For instance, companies conducting business transactions via mobile devices and simultaneously storing the data in a cloud are a case in point. Personal data entered into the device and stored in the cloud pose a challenge to data controllers, particularly in terms of the device's security. Companies will have to conduct an impact assessment to determine whether additional security features are needed to guarantee the required level of protection (GDPR, 2016). If the data are to be uploaded and stored directly in the cloud, individuals will have to be informed about the location of data storage. If devices are used for both private and professional purposes, individual files must be protected through additional means and unauthorised access to personal data by third parties

prevented. Even though the Personal Data Protection Act (ZVOP-1-UPB1, 2004) already required this level of security, the new GDPR imposes much higher fines for infringements. Therefore, violation of the GDPR may result in a maximum fine of EUR 20 million or 4% of the total worldwide annual turnover for the preceding financial year (GDPR, 2016). High fines will thus 'encourage' data controllers to handle personal data much more cautiously.

5 RESEARCH RESULTS

The research study presented here relied on a questionnaire available via the *www.1ka.com* online application. Respondents could provide answers between 9 January 2018 and 10 March 2018. A total of 246 questionnaires was partially completed. Not all respondents provided answers to all questions, which is why the N figure for individual answers varies and is presented below the respective results.

Table 1: Overview of answers related to the concept of personal data

Answer	No. of answers	*N* (%)
1 (No, I have never heard of that)	0	0%
2 (It sounds familiar)	29	12%
3 (I have heard about it)	21	9%
4 (I know what personal data are)	195	79%
Total	*N* = 245	100%

Table 1 shows the respondents' perception of the concept of personal data. The question was answered by 245 respondents. All respondents claim to be familiar with the 'personal data' concept in one way or another. No one indicated being unfamiliar with this concept. In fact, the overwhelming majority of respondents (79%) stated they knew the exact meaning of the concept of personal data.

Table 2: Overview of answers related to personal data

	YES	NO	Not sure	*N* (%)
Tax identification no.?	196	6	1	203
	97%	3%	0%	100%
Height?	90	94	15	199
	45%	47%	8%	100%
Name and surname?	181	15	4	200
	91%	8%	2%	100%
Facial image?	147	33	17	197
	75%	17%	9%	100%
DNA?	186	6	9	201
	93%	3%	4%	100%
Today's weather?	1	187	7	195
	1%	96%	4%	100%

	YES	NO	Not sure	*N* (%)
Fingerprints?	190	6	5	201
	95%	3%	2%	100%
Username for an online forum?	84	87	26	197
	43%	44%	13%	100%
No. of inhabitants in a country?	2	188	5	195
	1%	96%	3%	100%
Dental X-ray image?	155	29	13	197
	79%	15%	7%	100%
Religious belief together with eye colour and the status of a city councillor (in Ljubljana)?	89	76	33	198
	45%	38%	17%	100%

Table 2: Continuation

Table 2 shows answers to the question of whether the specific information described above constitute personal data. The differences in the number of answers are relatively small. The biggest difference amounts to 8 answers, which is negligible given the highest number of answers, i.e. 203. The responses show that all data with the exception of "today's weather" and the "number of inhabitants in a country" constitute personal data. A large majority of respondents (90%) thus recognised the two types of data that are not considered personal data and marked them accordingly. The name and surname category actually consists of two separate items of personal data since any information related to an identified individual is considered personal data. This category should therefore be split into two parts. The majority of respondents, i.e. more than 90%, provided correct answers to the more unambiguous questions such as "tax identification number", "name and surname", "DNA" and "fingerprints". They were slightly more hesitant with "dental X-ray image" and "facial image", however, three-quarters or more of the respondents answered correctly. Respondents' opinions diverged more with respect to an individual's "height", "username for an online forum" and "religious belief together with eye colour and the status of a city councillor (in Ljubljana)". All three categories attracted the highest number of "not sure" answers. At the same time, respondents' opinions on whether this type of information constitutes personal data seem to be split. Most respondents gave correct answers with respect to the last category, yet this question also had the biggest share (17%) of "not sure".

	YES	NO	*N* (%)
Personal identification no.	152	48	200
	76%	24%	100%
Information on sexual orientation	142	57	199
	71%	29%	100%
Vehicle registration plate details	60	136	196
	31%	69%	100%

Table 3: Overview of answers regarding special categories of personal data

Table 3: Continuation

	YES	NO	*N* (%)
Tax identification no.	148	52	200
	74%	26%	100%
Year of birth	83	114	197
	42%	58%	100%
Political opinion	105	89	194
	54%	46%	100%

Table 3 presents answers concerning certain types of sensitive personal data now, i.e. after the entry into force of the new GDPR, referred to as special categories of personal data. Again, the difference in answers is relatively small, whereas the largest difference is six answers. Among the listed personal data types, only "information about sexual orientation" and "political opinion" are considered special categories of personal data, while the remaining data types are classified as conventional personal data. With respect to sexual orientation, 71% of the respondents answered correctly while 54% of them gave correct answers for political opinion. Interestingly, 42% of the respondents believe that year of birth falls in the special category of personal data.

Table 4: Overview of answers regarding the question of risks to security

Unlikely	Less likely	Neither likely nor unlikely	Likely	Highly likely	Total: [*N*]
0	31	40	92	32	195
0%	16%	21%	47%	16%	100%

Table 4 shows whether the abuse of personal data may result in a serious risk to individuals' security. The question itself was not specified in any further detail, leaving the interpretation up to individual respondents. Almost 50% of the respondents believe the abuse of personal data would likely lead to a serious risk with regard to individuals' security. All 195 respondents agree that such events are likely to some degree.

Table 5: Overview of answers regarding the collection of personal data

	1 – I do not know	2	3	4	5 – I know very well	Total
Who collects your personal data?	12	31	85	53	17	198
	6%	16%	43%	27%	9%	100%
Which personal data are collected?	9	27	75	57	17	195
	5%	14%	38%	28%	9%	100%
What is the purpose of the data collection and processing?	15	51	58	54	17	194
	8%	26%	30%	28%	9%	100%
What is the extent of the data collection?	17	51	76	37	13	194
	9%	26%	39%	19%	7%	100%
Can your data can be transferred to a third party?	22	31	65	48	28	194
	11%	16%	39%	25%	14%	100%

Table 5 shows how well the respondents are informed of the above elements when downloading mobile applications to their mobile devices. We were particularly interested in whether they knew who collected their personal data, which personal data were collected, what was the purpose of processing that data, what was the extent of the data being collected and whether their data could be transferred to a third party. Respondents were asked to provide their answers on a 5-point Likert scale. The table shows that the distribution of answers concentrates somewhat around average values. The opinions of the respondents were not extremely divergent, meaning they either did not know the answers to the above questions or knew them very well. Nevertheless, a slight tendency towards more affirmative responses, particularly with respect to "who collects your personal data", may be observed. The answers in Table 5 correspond to those shown in Table 6, which contains information regarding the respondents' awareness of the statements below. No two questions in the table actually appeared alongside each other in the questionnaire.

	I am aware	I am not aware	*N* %
Who collects your personal data?	124	70	194
	64%	36%	100%
Which personal data are collected?	130	66	196
	66%	34%	100%
What is the purpose of the data collection and processing?	105	89	194
	54%	46%	100%
What is the extent of the data collection?	73	119	192
	38%	62%	100%
Can your data be transferred to a third party?	122	68	190
	64%	36%	100%

Table 6: Overview of answers regarding the awareness of the collection of personal data

Tables 5 and 6 provide the same choice of possible answers, with the only difference being in the answers. In Table 6, respondents could answer by selecting "I am aware" or "I am not aware". The results show strong correlations with the answers in Table 5 for each question posed. When an answer in Table 5 lent towards "I don't know", the answer in Table 6 fell into the "I am not aware" category. For instance, with respect to the question "What is the extent of the data collection?", 62% of the respondents stated they were unaware of the extent of the data being collected, as presented in Table 6. Most respondents answered the same question by choosing answers closer to the "I don't know" category, as shown in Table 5. We were also interested in determining what respondents were willing to do to ensure additional protection of their mobile devices. The results are given in Table 7.

Table 7: Overview of answers regarding respondents' willingness to adopt additional measures

	I am not willing at all	I am not willing	I am neither willing nor unwilling	I am willing	I am absolutely willing	N %
Antivirus software	8	10	23	90	65	196
	4%	5%	12%	46%	33%	100%
Additional data encryption	2	20	36	89	45	192
	1%	10%	19%	46%	23%	100%
Education in the field of mobile device security	5	12	40	90	46	193
	3%	6%	21%	47%	24%	100%
Data archiving	4	13	48	94	34	193
	2%	7%	25%	49%	18%	100%
Adoption of best practices when using a mobile phone	2	6	28	104	53	193
	1%	3%	15%	54%	27%	100%

Table 7 shows the respondents' willingness to take extra measures to boost the security of their mobile devices. Differences between answers are relatively small, which does not affect the potentially different interpretation of the results. Respondents could choose between antivirus software, additional data encryption, education in the field of mobile devices' security, data archiving, and the following of best practices when using their mobile phones. The results show the respondents are relatively strongly inclined towards the "I am absolutely willing" option for all of the questions. They expressed the greatest willingness to use antivirus software solutions and adopt best practices, while the respondents were the least willing to use additional data encryption solutions.

Respondents were also asked what they would do if their personal data fell into the hands of unauthorised persons. We did not directly specify which type of data this would involve. Therefore, it was up to individual respondents to conceive a possible scenario. They could choose from several answers, including: "I would completely lose my trust in the organisation"; "I would file a lawsuit"; "Depends on the consequences"; "I would do absolutely nothing"; "I would not really care"; and "Other". The results show 43% of respondents stated they would lose their trust in the organisation, 38% said their reaction would depend on the consequences, and 17% stated they would file a lawsuit against the organisation. This question was answered by 195 respondents. We were also interested in

determining how many respondents were aware of the fact that the new GDPR, which would apply in all EU member states, was to enter into force in May 2018, with 107 out of these 195 respondents stating they were familiar with the upcoming regulation.

6 DISCUSSION

When examining the above results, one must first look at the situation as a whole. It is important to stress that the questionnaire aimed to measure the level of respondents' awareness of the personal data protection issue. The results show the respondents have a sufficient level of awareness and familiarity with this topic, at least as far as the basics are concerned. However, the greater the complexity of the issue, the greater the insecurity detected among the respondents. With respect to the first question, the vast majority of respondents stated they were familiar with the personal data concept. This was also demonstrated in the second question where they correctly selected "name and surname", "fingerprints", and other answers. When it came to "religious belief together with eye colour and the status of a city councillor (in Ljubljana)" and "username for an online forum", a large share of respondents either gave a wrong answer or was unsure of the answer. The fact is that any information related to an identifiable individual constitutes personal data. The phrase "any information" is key in this respect. As mentioned in the literature review, there is a difference between protected and unprotected personal data. A piece of information may constitute personal data, but it does not necessarily have to be protected according to applicable legislation. In this case, the issue of the identifiability of an individual must be considered since this is crucial for determining whether such personal data must be protected or not. Table 3 presents the respondents' answers on sensitive personal data (special categories of personal data) and clearly shows that most of them do not distinguish between conventional and special categories of personal data. Almost three-quarters of the respondents stated that their personal identification number belonged to the special category of personal data. Although it is true that the personal identification number reveals several items of personal data, it does not belong to the special category of personal data *per se* because it merely allows one to use it in order to access sensitive data. Nevertheless, the same argument could also be made for the combination of one's name, surname and address since these pieces of information may allow information related to individual's health records, criminal records and other data. Therefore, information revealing individuals' health condition falls into the special category of personal data, whereas the combination of those pieces of information related to an individual does not.

When asked whether the abuse of personal data could be a serious risk for individuals' personal safety and security, all respondents stated that some degree of likelihood does indeed exist. The notion that personal data abuse could result in a threat to personal safety and security is, among others, an indicator of awareness. This question did not contain any specific details about what type of abuse this would entail or which data would be affected. Respondents

were thus able to come up with their own scenarios. This question is directly linked to the question of data abuse where the respondents were again left to conceive various scenarios. Even though 38% of the respondents stating their reaction would depend on the consequences, this question was posed in such a way that presupposed a slight tendency towards a specific answer. Therefore, respondents had less freedom while answering it, mainly because the "I would lose my trust in the organisation" option appeared first on the list of possible answers and represented a relatively logical choice, which is why slightly less than 50% of respondents chose this answer. For a more realistic answer, we would have to either leave the interpretation up to individual respondents or define a very clear scenario entailing such an infringement. Tables 5 and 6 present a list of simpler concepts which were used to verify the accuracy or authenticity of the responses. The results show that respondents' answers correspond, thereby adding credibility to the research study.

The results presented in Table 7 show that most respondents are willing to make a considerable effort to protect their mobile devices. On the other hand, the findings of Bernik and Markelj (2014) paint an entirely different picture. In business spheres, the security of mobile devices is poor. This contradiction could be explained by presuming that while individuals may declare their willingness to improve the security of their devices, in practice they are less efficient when it comes to actually implementing security measures.

When the above findings are placed in the context of some of the most strongly emphasised issues and, indirectly, some of the most problematic areas, the following characteristics appear that should be considered when discussing or even providing personal data protection for mobile devices. Mobile devices have taken on the role of a mobile office used by individuals to carry out different tasks and achieve numerous purposes. As such, they are a challenge to and introduce extra dimensions in the sphere of personal data protection compared to other media that require due consideration. As mentioned, smart devices can impact the way individuals and organisations conduct their everyday tasks enormously. Applications facilitating, complementing or even replacing the current ways of conducting spare-time activities or work-related processes are being developed continuously.

The IT aspect of mobile device use enables or, in other words, requires an individual user to also provide their consent for the handling of data by third parties, for storing personal data on servers etc. Further, IT solutions give users the possibility to use cloud services, characterised by flows of large data quantities which are difficult if not impossible to control, and numerous other options. It seems there are endless possibilities which can quickly become uncontrollable and, among others, raise the question of traceability. Third parties must be clearly and explicitly listed as such whenever individuals are asked to give their approval for the processing of personal data. However, this raises another issue related to the format and type of consent that is one of the key aspects of the GDPR. In terms of mobile devices, spatial limitations or the desire for greater transparency and accessibility raise new questions about the acquisition of consent and thus bring new challenges for organisations and service providers. So-called drop down

menus do not comply with the GDPR because they mostly enable individuals to provide their consent without being informed or aware of the entire scope of access and all the entities with potential access to their personal data. Users neither have an immediate insight into such information nor an opportunity to opt-in since they are not required to open or access certain types of consent in their entirety. Therefore, they provide their consent based on incomplete information or, in some cases, on the opt-out method, which is plainly out of step with the GDPR principles (consent forms must not be filled-in as being 'approved' in advance). From a legal point of view, such consent is considered wrongly obtained by being acquired through means of a pre-completed choice which, for instance, may also include the "agree to all" choice, whereby individuals are unfamiliar with what the "all" actually means or entails.

The issues surrounding consent forms and the fact they contain absurd conditions for visiting websites or using applications should not be delved into any deeper because they vary from one website or application to another. The issues of consent could be discussed at length in a separate paper. In the end, it is up to the individual to decide whether they will consent to certain aspects they might not otherwise like for the sake of using a service or receiving content from a service provider, or whether they will fully give up visiting a website or using an application and find what they were looking for elsewhere.

Another important feature in this respect relates to the multifunctionality of mobile devices, which are not only used to store our own personal data but also the personal data of others. For instance, our mobile devices also store large databases of names and surnames, phone numbers and e-mail addresses of other individuals, photographs and videos containing the images of other individuals, as well as e-mails containing a wide array of contents, which might again include various personal data. Therefore, we are no longer responsible merely for our own personal data, but also for those of others. As such, we not only play the role of the user or an individual whose personal data are being handled, but also act as personal data processors. We collect, store and use all of the mentioned data for both private and professional purposes if our mobile device is used for work-related tasks. In doing so, we enable access to our mobile device (and its contents) to numerous applications, which demand we sign a series of consent forms and operate based on cooperation with third parties acting as processors of all (or some) of the aforementioned personal data. In addition, we use cloud services for which intrusions and data leakages are no longer inconceivable etc.

When expanding on the issues discussed above, one quickly sees the attractiveness of mobile devices stems from the simplicity and ease of their use; a single device can help achieve various goals, for instance travel, search for or even locate a device in the event of loss or theft. By turning on the device's location services, we enable the processing of personal data related to one's place of residence and work, favourite locations and routes travelled. Information technologies and their fast-paced development require users to possess ever-greater amounts of knowledge and, in some cases or to a certain extent, perform specific processes and actions which might be overwhelming for some, particularly given the multiplicity of these processes and the varying features

(mostly age-related) of different user populations. The average mobile device user cannot be expected to be familiar with all types of risks arising from use of the mobile medium. However, individuals (irrespective of their age and educational background) should be required to hold at least knowledge related to network services, which might prove too demanding for the general population. Users are familiar with, for instance, access to an unsecured wireless network, but are not necessarily familiar with every threat arising from connecting to such networks. Similarly, users may be familiar with receiving and opening e-mails, but might not have the necessary knowledge about different website types and the meaning behind various terms or abbreviations (e.g. the difference between http, https and other protocols). They may be familiar with the principles underlying the functioning of a touchscreen display yet, due to their impulsiveness, carelessness or lack of knowledge, might also click on pop-up windows informing them they have won a prize as the '1 millionth visitor' of a certain website or that their device has been infected with a virus.

The simplicity of use also relates to the variety of services we all carry out on our mobile devices, such as online banking services, enabling us to use our mobile phones to pay our bills with a couple of clicks or use our credit and debit cards to shop online. The scope of (in)security and threat is therefore extremely broad, while the consequences of improper use may be reflected in various areas.

The concepts of mobility and user awareness constitute a new element which raises a host of issues. Nevertheless, the former cannot be ignored or avoided since mobility is the key to mobile devices, while user awareness is something we must consider but predominantly depends on individual users. In light of the above, we could say that the share of individuals who leave their mobile devices unattended and uncontrolled, and do not use any of the default security features (lock screen, phone lock etc.), for whatever reason is quite problematic. On the other hand, new ways of protecting and increasing the security of mobile devices, such as unlocking a device by using identification services based on biometric identifiers, fingerprints, iris and facial features, give new possibilities for personal data processing. Therefore, one needs to master the art of striking the right balance between the various aspects of protection, security and privacy while ensuring the legality of one's business and other operations.

7 CONCLUSION

Personal data protection is a multifaceted field. Today, it affects almost every area of our everyday lives. Modern technologies are increasingly present and will therefore have an ever-greater influence of our future way of life, showing why the new GDPR has an important role to play in creating our future. By presenting and discussing some fundamental changes, this paper describes the elements introduced by the new GDPR and examines their impact on individuals and organisations. We find the GDPR does not introduce any 'revolutionary' changes but, if applied carefully, the GDPR will bring certain advantages for both individuals and companies. However, compliance with the Regulation will cause some inconvenience for those companies that fail to deal with personal

data consistently. On the other hand, for companies that have taken the personal data protection issue seriously, the new GDPR will not bring any major changes. Here, one must also consider the type of service a company is providing. The central part of the paper focuses on the way in which the GDPR will impact the users of mobile devices. Some organisations will restrict the use and processing of personal data on mobile devices. The GDPR (2016) also provides for greater control in the field of personal data protection. Yet, effective control cannot be achieved without individuals' cooperation, an aspect that can be strengthened by raising their awareness.

It is also clear that companies are making great efforts to conceal certain incidents, as recently occurred in the case of Yahoo (Fiegerman, 2017). Such practices could be prevented through a higher degree of awareness and reporting. Increased transparency will also contribute to greater respect for human rights and fundamental freedoms. By considering the available literature and limitations, this paper selectively presented some of the more important impacts of the GDPR on mobile devices. The examination of all impacts would require a longer and more comprehensive paper. Codes of conduct, case law, guidelines, rules, regulations and standards, which will be the real indicators of the GDPR's implementation in practice, will undoubtedly importantly impact the use of mobile devices. It will only be then that the objective impacts of the GDPR on mobile devices can be observed and analysed. Until then, we can only presume what might happen. The GDPR will have to be transposed to national legislation and implemented in member states' legal systems. Slovenia is already lagging behind here since an extraordinary session of the Slovenian Parliament rejected the amendments proposed to the Personal Data Protection Act (ZVOP-2). Therefore, one may ask what sanctions await Slovenia for not having adopted the amended Act. We expect the case law to have the strongest impact in this respect as it will resolve certain issues raised by experts in the field.

REFERENCES

Article 29 Data Protection Working Party. (2007). *Opinion 04/2007 on the concept of personal data*. Brussels: EC. Retrieved from https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf

Baker McKenzie. (2017). *GDPR national legislation survey*. Chicago: Baker McKenzie. Retrieved from http://www.bakermckenzie.com/-/media/files/insight/publications/2017/06/bk_itc_gdprsurvey_2017.pdf?la=en

Bernik, I., & Markelj, B. (2014). Zagotavljanje varnosti informacij z razumevanjem uporabnikovega ravnanja z mobilno napravo [Ensuring the security of information by understanding user behaviour on a mobile device]. *Varstvoslovje, 16*(1), 5–15.

Bolognini, L., & Bistolfi, C. (2016). Pseudonymization and impacts of Big (personal/anonymous) Data processing in the transition from the Directive 95/46/EC to the new EU General Data Protection Regulation. *Computer Law & Security Review, 33*(2), 171–181.

De Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law & Security Review, 32*(2), 179–194.

Ducato, R. (2016). Cloud computing for s-Health and the data protection challenge: Getting ready for the General Data Protection Regulation. V *2016 IEEE International Smart Cities Conference (ISC2)* (pp. 404–407). doi: 10.1109/ISC2.2016.7580803

DPOrganizer. (n. d.). *5 reasons for individuals to care about GDPR*. Retrieved from https://www.dporganizer.com/5-reasons-individuals-care-gdpr/

Eation, A. (September 13, 2017). *How to solve your CRM data quality problems before GDPR*. [Video]. Preact Limited. Retrieved from https://www.youtube.com/watch?v=gDUdlSX2DvA

Fiegerman, S. (September 7, 2017). The biggest data breaches ever. *CNNtech*. Retrieved from http://money.cnn.com/2017/09/07/technology/business/biggest-breaches-ever/index.html

Gilbert, F. (2016). EU general data protection regulation: What impact for businesses established outside the European Union. *Journal of Internet Law. 19*(11), 3–8.

GSMA Intelligence. (2018). *Definitive data and analysis for the mobile industry*. Retrieved from https://www.gsmaintelligence.com/

Hettrich, M. (2015). Data privacy regulation in the age of smartphones. *Touro Law, 31*(4), 981–1011. Retrieved from http://digitalcommons.tourolaw.edu/cgi/viewcontent.cgi?article=2681&context=lawreview

Informacijski pooblaščenec. (2017a). *Iskalnik po odločbah in mnenjih VOP: Določljivost posameznikov in osebnih podatkov* [Search engine for VOP order and views: Identifiable person and personal data]. Retrieved from https://www.ip-rs.si/vop/dolocljivost-posameznikov-in-osebnih-podatko-3031/

Informacijski pooblaščenec. (2017b). *Kaj prinaša nova Splošna uredba (EU) o varstvu podatkov?* [What does the new general data protection regulation (EU) bring?]. Retrieved from https://www.ip-rs.si/fileadmin/user_upload/Pdf/pripombe/Splosna_uredba_o_varstvu_podatkov-letak_maj_2017.pdf

Informacijski pooblaščenec. (n. d.). *Reforma evropskega zakonodajnega okvira za varstvo osebnih podatkov* [European general data protection regulation reform]. Retrieved from https://www.ip-rs.si/zakonodaja/reforma-evropskega-zakonodajnega-okvira-za-varstvo-osebnih-podatkov/

Information Commissioner's Office. (2017). *Moneysupermarket fined for ignoring customers' marketing email opt-outs*. Retrieved from https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/07/moneysupermarket-fined-for-ignoring-customers-marketing-email-opt-outs/

Ledino, J. (2012). How to remotely disable your los tor stolen phone. *PCmag*. Retrieved from https://www.pcmag.com/article2/0,2817,2352755,00.asp

Mantelero, A. (2013). The EU proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten'. *Computer Law & Security Review, 29*(3), 229–235.

Markelj, B., & Bernik, I. (2016). Vpliv raznolikosti podatkov na odvzem in preiskovanje mobilnih naprav v organizacijah [The impact of the diversity of

information on the seizure and investigation of mobile devices in organisations].*Varstvoslovje, 18*(1), 84–97.

Ministrstvo za pravosodje RS. (2017). *Osnutek zakona o varstvu osebnih podatkov (ZVOP-2)* [Draft of the Personal Data Protection Act]. Ljubljana: MP RS. Retrieved from http://www.mp.gov.si/fileadmin/mp.gov.si/pageuploads/mp.gov.si/novice/2017/september_2017/171004_ZVOP-2_status.pdf

Pedro, C. F. (2016). *Privacy in the smartphone age: A study on the privacy and data protection risks and violations of mobile applications* (Master's thesis). Tilburg: Law and Technology. Retrieved from http://arno.uvt.nl/show.cgi?fid=142089

Sire. (n. d.). *Are you prepared for the General Data Protection Regulation?* Retrieved from https://www.sire.co.uk/blog/are-you-prepared-for-the-general-data-protection-regulation

Sullivan, C., & Burger, E. (2017). "In the public interest": The privacy implications of international business- to- business sharing of cyber-threat intelligence. *Computer Law & Security Review, 33*(1), 14–29.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review, 34*(1), 134–153. Retrieved from https://www.sciencedirect.com/science/article/pii/S0267364917301966#

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) [GDPR]. (2016). *Official Journal of the EU,* (L 119).

Ustava Republike Slovenije [Constitution of the Slovenian Republic]. (1991, 1997, 2000, 2003, 2004, 2006, 2013, 2016). *Uradni list RS*, (33/91, 42/97, 66/00, 69/04, 68/06, 47/13, 75/16).

Voss, W. G. (2014). Looking at European Union data protection law reform through a different prism: The proposed EU General Data Protection Regulation two years later. *Journal of Internet Law, 17*(9), 12–24.

Voss, W. G. (2017). European Union data privacy law reform: General Data Protection Regulation, privacy shield, and the right to delisting. *Business Lawyer, 70*(1), 221–233.

Zakon o varstvu osebnih podatkov (ZVOP-1-UPB1) [Personal Data Protection Act]. (2004, 2005, 2007). *Uradni list RS*, (86/04, 113/05, 51/07, 67/07).

About the Authors:

Domen Hribar, MA in Criminal Justice and Security from the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. E-mail: domen.hribar@student.um.si

Miha Dvojmoč, PhD, Assistant Professor of Security Studies at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. E-mail: miha.dvojmoc@fvv.uni-mb.si

Blaž Markelj, PhD, Assistant Professor of Security Studies at the Faculty of Criminal Justice and Security, University of Maribor, Slovenia. E-mail: blaz.markelj@fvv.uni-mb.si