International Journal of Management, Knowledge and Learning | ISSN 2232-5697

How Individuals Care for Personal Data Protection When Using Online Services

Benjamin Lesjak
University of Primorska and Datainfo.si
Slovenia benjamin.lesjak@fm-kp.si

Mojca Čretnik
Nova KBM d.d., Slovenia
cretnikovam@hotmail.com

Purpose: Individuals have more mechanisms for personal data protection according to the new EU General Data Protection Regulation. Therefore, we researched the actions of individuals concerning the protection of their personal data when using online services.

Study design/methodology/approach: . We wanted to assess the awareness of individuals about the importance of personal data protection and if there are any differences regarding age, education and gender concerning personal data protection when using online services. We examined the individuals' rights in connection to personal data and connection to ICT use. In the empirical part, we collected several data regarding the behaviour of individuals, related to the protection of personal data.

Findings: We emphasized that at least age is one of the factors influencing the behaviour and added recommendations for improvement of protection of personal data in conclusions.

Originality/value: This paper is a revised and updated version of a Master thesis and its results with the title Personal data in the modern information society by Mojca Čretnik and mentor Benjamin Lesjak.

Introduction

Each individual has the opportunity to choose how much information about himself he will disclose to the public, to whom he will say something and how he will allow the use of information about himself in individual cases. The less an individual has the opportunity to control his private data, the less room for a choice he has and the harder it is to assume the image of an indeterminate man, which is essential for the normal functioning of modern democratic society (Bernard Korpar et al. 2018, 125).

Goddard (2017, 703) explains that personal data is that data that can directly or indirectly identify an individual, which includes web identifiers such as IP addresses, cookies, digital fingerprint, location data that can identify individuals.

Wagner DeCew (1997, 146–147) points out in his work that almost every transaction carried out with personal data is today recorded on a computer, and as a result, the routine collection and transmission of personal data in digitized form, with individuals it is difficult to determine whether information about them is being used and further processed.

Bernard Korpar et al. (2018, 277-278) point out that if individual personal data is published in a record and accessible to the public does not mean that it in case that the data is not personal data. On the contrary, personal data is always personal and any further processing of this data is regulated by personal data protection provisions. The processing of personal data, including the aggregation or creation of personal data collections, is permitted only if such processing is prescribed by law or the individual consents to such processing relating to his or her personal data. Personal data can therefore only be collected for specific and lawful purposes, from which

it can be concluded that there must be an appropriate legal basis for their processing, as only the law can adequately prescribe the purpose of personal data collection.

Article 6 of the General Data Protection Regulation defines the lawfulness of the processing of personal data and provides for six legal bases for the processing of personal data, namely: consent, a contract, legal obligation, the protection of the interests of life, the public interest or the legitimate interest.

Common to all the above legal bases, except for consent, is that the processing of personal data must be necessary to achieve the purpose, which means that the processing of personal data is targeted and its interference with individual rights is proportionate to the objectives set by the controller. it pursues data through such processing and if the same purpose cannot be achieved by milder encroachments on the rights and freedoms of the individual (Markovič et al. 2019, 67–68).

Bernard Korpar et al. (2018, 277) explains the importance of the principle of proportionality. An appropriate balance needs to be struck between different interests and constitutionally protected goods. Namely, in a democratic society, no human right can be absolute, since it already follows from the content of individual human rights that the right of one restricts the right of the other, as defined in the Constitution of the Republic of Slovenia. Cerar et al. 2009, by Bernard Korpar et al. (2018, 277) raise the question of how far it is permissible to protect the right of one individual without interfering with or restricting the right of another individual, to which the above-mentioned principle of proportionality provides an answer.

Bernard Korpar et al. (2018, 337) mentions as one of the fundamental principles of personal data protection the principle of definiteness and limitation of purposes, according to which the purpose of personal data processing must be clearly defined in advance and thus clearly predictable for the individual.

In the paper, we wanted to research the behaviour of individuals regarding personal data protection on a selected topic.

Individuals' rights and personal data protection

Burton et al. (2016, 6) explain that the General Data Protection Regulation strengthens the rights of individuals, ie. the right to information, the right to access personal data, the right to rectification, erasure, objection and the right not to be subject to automated decision-making, including profiling, and to bring many new rights for individuals.

In an age of fast-growing digital economy and big data, the individual's supervisory rights, as ensured by the protection of personal data, face many challenges. An important question is raised as to how and to what extent an individual can still establish control over personal data relating to him in the above circumstances (Bernard Korpar et al. 2018, 357). Ausloos, Veale and Mahieu (2019, 284) point out that the rights of the data subject are crucial in the new European data protection regime.

Hoofnagle, Van der Sloot and Zuiderveen Borgesius (2019, 88-89) explain that the rights of individuals were already defined by Directive 95/46 / EC of 1995 and that they also have their roots in constitutional instruments. However, the General Data Protection Regulation defines the rights of individuals even more deeply. Politou, Alepis and Patsakis (2018, 4) explain in detail other principles as defined by the General Data Protection Regulation, namely fairness, legality and transparency, the principle of purpose limitation, minimum data, accuracy, storage limitation, integrity and confidentiality and finally liability, which imposes the responsibility

for the compliance of the processing of personal data on the controller, who must also be able to prove such compliance.

The right of access to data is an important tool in the hands of the individual, with which he can monitor the operation of controllers and their compliance with the general principles governing the processing of personal data. Compliance with the basic principles as defined by the General Regulation on the Protection of Personal Data, such as the principle of minimum data size, accuracy, the principle of storage limitation, is easier to verify when exercising the right of access to personal data (Ausloos, Veale and Mahieu 2019, 285). The right of access to data has been extended by the new General Data Protection Regulation, to increase the fairness and transparency of the processing of personal data, as it allows data subjects to verify the lawfulness of the processing carried out on their personal data (Voight 2017, 150). Recital (63) of the General Data Protection Regulation explains that the data subject has the right to access personal data collected in connection with him and the right to simply exercise this right at reasonable intervals to be able to acquaint with the processing and verify its legality.

The right of access to personal data is exercised in two steps, with the individual having the right in the first step to obtaining confirmation from the controller whether personal data are being processed in relation to him, and if the controller processes the individual's personal data. (Voight 2017, 150-151).

It is also very important the self-awareness of an individual whose personal data he shares about himself on the World Wide Web or passes it on to other, third parties. Particular caution applies to the transmission of financial data, such as credit card number, etc. (Information Commissioner 2019, 6–10). Individuals very often naively rely on others to protect their privacy and personal data, but the fact is that in the first phase they can do the most in this area themselves (Information Commissioner 2015, 15).

Bernard Korpar et al. (2018, 357) explain that individuals ’control over the processing of personal data is an integral part of the right to the protection of personal data. Haskins (2018) gives some practical advice for the average individual and the protection of his or her personal data and recommends:

- that an individual protects the devices they use regularly with passwords. Mobile phones, laptops and tablets are easily lost or alienated from an individual. If such devices are not properly password protected, access to data on these devices is very simple;
- use strong passwords that are long and random (contain a combination of uppercase / lowercase letters, numbers and characters). Many individuals use the same and simple passwords for different devices/applications, which is risky behaviour;
- to set up two-factor identification on financial accounts and e-mail accounts. Most banks in online and mobile banking already require this, by entering a special code that an individual receives through another channel, e.g., to your mobile phone;
- performing online shopping and other financial transactions on secure online networks. It is recommended to use your device and a secure network (Wi-Fi);
- Regular software updates, including anti-virus software, operating system used, etc. Cyber threats change frequently, and many updates address such security issues;
- individuals should not send personal data by telephone or e-mail.

Be careful when opening e-mail attachments or clicking on forwarded links, as doing so may infect your computer with malware.

The Information Commissioner (2015, 6–9) also emphasizes the importance of updating the operating system and antivirus protection, as malware (viruses, worms, other malicious code) search for security holes in operating systems and, if detected, often allows them to do so. to

take control of an individual's computer or his or her cell phone. The measure also cites data encryption as an important protection measure, as the data that individuals have is stored on computer hard drives, memory cards in mobile phones, USB sticks and other media, most often in unencrypted form. The encryption process can ensure that unauthorized people will not be able to read our confidential messages or data.

ICT use and personal data protection

The use of modern information technologies increases the efficiency, speed of collection, storage, use and transfer of data. Both public and private institutions need a constant flow of data on individuals for the smooth performance of work or the provision of their services, which are an integral part of modern life. The provision of health services, social security, credit, insurance, and crime prevention and detection presupposes the availability of a significant amount of personal data as well as the willingness of individuals to provide that data (Wacks 2018, 121). Standards for the protection of personal data are becoming increasingly high, and companies and other organizations face an increasingly complex task to assess whether their data processing activities are legally compliant, especially in an international context. Data by its very nature today easily crosses borders and plays a key role in the global digital economy (Voight 2017, 1).

Ahtik et al. (2014, 10) point out that the widespread use of modern ICT, in addition to many opportunities, also brings new risks, citing the example of Internet accessibility of public databases, which increases the possibility of intrusion into them and thus misuse of personal data collected there.

The importance of information in modern information technology has increased significantly, as information has become a product in itself that can be traded in the information society and is legally protected. Information, from the point of view of the company, represents a special capital or value of the company, which in the knowledge society is measured by their "know-how" and not in production factors (such as machines, land) (Roszak 1994, 8, according to Kovačič et al. 2010, 26). Rapid technological development enables increased data storage capacity, which enables companies and other organizations to expand data collection, processing and interconnection. These companies and other organizations are increasingly using this data for various purposes, such as personalization of services, marketing, etc. Although new technologies and services benefit both businesses and individuals or consumers, they also pose serious risks to an individual's privacy. As a result, people's confidence in data collection and processing companies may decline, and a lack of trust may slow down the development of innovative uses and the development of new technologies if appropriate personal data protection practices are not implemented (Tikkinen-Piri, Rohunen and Markkula 2017, 135).

When using modern information technologies, the individual must know his rights and duties, as well as the rights and duties of others, i.e. controller and processors of personal data who have personal data of individuals (Turk and Vogrinčič 2019, 7). The Information Commissioner emphasizes that individuals must have the power to decide who is allowed access to their personal data and the right to clear information about what individual companies and other organizations will do with that data. Of course, the rights of individuals in terms of their decision-making power are limited to the extent that the collection of personal data is provided by law. In the first phase, individuals can do a lot for the security of their personal data by themselves with certain preventive measures, such as with caution in transmitting data to different service providers (Information Commissioner 2019, 4).

There are many technical possibilities for protecting privacy on the Internet, but it should be borne in mind that due to the nature of the Internet, the protection of one's own data is primarily the responsibility of the user himself. The development of modern information technologies is constantly bringing new and more effective tools that can encroach on individual personal rights, and on the other hand, new technology also offers a range of solutions that help individuals protect their interests regarding privacy and anonymity of individual activities (Makarovič et al. 2003, 114). Wacks (2018, 158) explains that to protect personal data, in the age of modern information technologies, appropriate support must be sought in technology as well as in legislation.

Also, recent studies among students (Zwilling et al. 2021) show that internet users possess adequate cyber threat awareness but apply only minimal protective measures usually relatively common and simple ones and such measures influence personal data protection as well.

Methodology and results

The survey was conducted based on questionnaires, which were used to determine the extent to which individuals are aware of the importance of protecting their own personal data and how well they know this area. We wanted to find out what the conduct practices are and whether individuals are taking appropriate measures and activities to secure their personal data.

In the study, we used the snowball sampling method. The survey questionnaire was active by publication on the survey web portal from 10 February 2020 and remained active until 3 March 2020 inclusive, when the survey was completed. Invitations to participate in the survey were also published on online social networks (Facebook). We received 228 completed survey questionnaires, which we then used in the data analysis.

We used mainly descriptive statistics when analysing respondents' data. With the statements where we encountered the lowest results by respondents, we tested results with Kolmogorov-Smirnov test, Kruskal-Wallis test and the Mann-Whitney test to determine the differences and examined in detail to explain the possible reasons.

71.9% of women and 28.1% of men answered the questionnaire. Most respondents are aged between 41 and 50 (34.6%), the least is over 61 (4.8%). Most respondents have completed secondary education or less (32.0%), the least have a doctorate (1.3%).

We were interested in how respondents see certain general statements in the field of personal data protection as described in Table 1. Respondents answered with a score from 1 (not true at all) to 5 (absolutely true). On average, respondents most agree that they confirm the offered cookies for access to the desired website (average = 3.89; SD = 0.86). On the other hand, they at least agree that when using online services, they read the terms and privacy policy (average = 2.37; SD = 1.06). The legislation protects internet users or enables better protection of their privacy by being properly informed about cookies and offered the opportunity to decide, but based on the received statements of respondents, it can be assumed that individual web users are generally poorly informed, as well as the tools that are available to them and with which cookies can be managed. As expected, our research also showed that the terms and privacy policy of web service users are often deliberately ignored, which can be attributed to longer texts, which can be time-consuming, perhaps even incomprehensible, too demanding, etc. for an individual user. The results obtained point to the fact that individual users simply come to terms with the fact that if they want to use a particular service, they must therefore accept the terms of use and privacy policy.

Table 1: Agreeing with general statements in the field of personal data protection

Statement	Median	Average	SD
To access the desired website, I confirm the offered cookies.	4.00	3.89	0.86
I read the terms and privacy policy when using online services.	2.00	2.37	1.06
I regularly delete or block cookies on my computer and other mobile devices.	2.00	2.51	1.10
I turn off the location detection feature of my mobile phone and use it only in certain situations.	4.00	3.43	1.28
I always have an antivirus program installed on my computer and other mobile devices.	4.00	3.80	1.04
I use different passwords to access equipment, devices, and digital services.	4.00	3.74	1.01
I change my passwords regularly.	3.00	2.90	1.12

Further on we were interested in whether respondents know when companies and other organizations can collect their personal data (respondents were able to give more than one answer). We have given only the correct answers to this question. 93.0% of respondents answered that a company and other organizations can collect personal data of individuals when they have given their consent and been informed in advance about the processing of their personal data. Under the second, 1.8% of respondents answered that they have signed a contract for this and when the processing of personal data is in the public interest. From the above, it can be assumed that the respondents do not know all the available legal bases for the processing of personal data and therefore gave the greatest weight to consent, which could be because many companies and other organizations immediately acceded after the General Data Protection Regulation to collect new consents.

We were also interested in whether the respondents know when a company or a person in a company in the private sector is entitled to personal data (respondents gave answers with "Yes" or "No"). We have given various fictional examples. The majority of respondents gave the correct answer to the questions where the disproportion of the purpose of processing such data was clearly visible. However, the least correct answers could be observed in certain more borderline cases, and it would be sensible in further research to find out why the respondents gave the wrong answers.

Table 2: Fictional cases if a company is entitled to personal data

The statement	Correct Answer	% of correct
The butcher requests your State identification number.	No	99.1
You have entered into a copyright agreement with the company. The company requires a tax number or State identification number from you.	Yes	91.2
You took the car to the service station. At the service station, they ask you to find out what brands of cars your family members drive.	No	98.2
When concluding a mobile package for retirees, they ask for information about your age.	Yes	71.1
When taking out life insurance, the insurance company asks you if you are a smoker.	Yes	65.4
Along with the completed crossword puzzle with which you participate in the draw for the colour TV, they require a tax number for the prize before the draw.	No	57.0
The Mountaineering Association requires a copy of your identity document for membership.	No	59.6
You are less than 15 years old. The company requires your consent to process your personal data.	No	58.8

We were interested in how many respondents had bought a product or paid for a service in an online store in the last 12 months. There were 81.1% of them, which indicates a fairly high percentage of individuals who use the online shopping method, which can often save time and

money, as they can make the purchase with a few clicks on their home computer. These respondents then answered three additional questions. The first additional question was how often they shop online. Most respondents shop online several times a year (55.1%), followed by those who shop online several times a month (20.0%). A smaller volume of online shopping may have because the product itself, which the individual intends to buy, cannot be seen live and for security reasons, primarily related to the necessary transmission of personal data online.

Also, these respondents who bought a product in the online store in the last 12 months or paid for a service with a rating from 1 (not true at all) to 5 (absolutely true) answered three additional statements in the field of their online purchase. Table 4 shows that, on average, respondents most agree that they have received the receipt of security SMS messages or other instant notification services for online payments (average = 3.74; SD = 1.29), and the least agree, to check before buying online, whether the company or s. p. entered in the Business Register of Slovenia (average = 2.40; SD = 1.12). It is always recommended that an individual, before making a purchase online, check only the website and that by including an SMS service or other instant notification service, he gains the necessary insight into the transactions made with the help of the card. From the answers received from respondents, it can be assumed that they are aware of the dangers that threaten online shopping, which can be assessed as positive, as each individual first must make their own online business as safe as possible.

Table 3: Agreeing with a general statement in the field of personal data protection

Statement	Median	Average	SD
Before buying online at home, I check whether the company or. s. p. entered in the Business Register of Slovenia.	2,00	2,40	1,12
Before making a purchase, I check that the website is marked "HTTPS" in the address bar of the browser, as this way the website provides a secure connection.	3,00	2,91	1,21
For online payments, I have turned on the receipt of security SMS messages or other instant notification services, as my bank allows me to do so.	4,00	3,74	1,29

When analysing the results, it should be noted that, on average, respondents at least agreed with the statement: “I read the terms and privacy policy when using online services” (average = 2.37; SD = 1.06) and with the statement: "I check before buying online whether the online company is real in the Business Register of Slovenia" (average = 2.40; SD = 1.12). In a more detailed analysis, we found that only 16.2% of respondents agree with the second statement and 3.8% of respondents who bought a product or paid for a service in an online store in the last 12 months completely agree with it.

Therefore, we were further interested in whether these two opinions differ statistically significantly according to the age, education and gender of the respondents. We used the Kolmogorov-Smirnov test to find that the statement "I read the terms and privacy policy when using online services" is not approximately normally distributed (Stat. = 0.251, df = 228, P <0.001) and the statement "Before buying online at home, I check whether the company is really in the Business Register of Slovenia" is not approximately normally distributed (Stat. = 0.244, df = 185, P <0.001). We used the Kruskal-Wallis test (age, education) and the Mann-Whitney test (gender) to determine the differences.

The opinion of respondents, that they read the terms and privacy policy when using online services differs statistically significantly according to age (P = 0.000) and also according to their education (P = 0.032). Respondents over the age of 61 agree most with this statement, while respondents under the age of 20 agree the least. Regarding education, respondents with a college or university degree agree the most with this statement, while respondents with a completed specialization or master's degree agree the least. On the contrary, we found that the

answers of the respondents did not differ statistically significantly according to gender (P = 0.921).

When identifying differences in reading the general terms and conditions and privacy policy online, it can be assumed that the opinion studied differs statistically significantly according to age and education, but not according to the gender of the respondents. By claiming that when using online services, respondents read the terms and privacy policy, those over 61 years of age agree the most, and the younger generations or those up to 20 years of age agree the least. Due to the above, it can be assumed that older respondents are slightly more cautious than younger ones, which could be attributed to the fact that in their youth they were not so involved in online business as opposed to younger generations who know the online environment much better and trust more. It can also be found that individual respondents with a higher level of education give more weight to their online behaviour.

The opinion of respondents that before buying online they check whether the company is really in the Business Register of Slovenia, differs statistically significantly according to age (P = 0.015). Respondents over the age of 61 agree most with this statement, while respondents under the age of 20 agree the least. In the following, we used the Post-hoc test to check where or between which pairs of respondents, according to age, there are statistically significant differences. On contrary, such opinion does not differ statistically significantly according to their education (P = 0.156) and gender of the respondents (P = 0.179).

When determining differences in behaviour before online shopping, it can be assumed that the studied opinion differs statistically significantly according to the age of the respondents, but not according to education and gender. By claiming that respondents check before buying if the company is really in the Business Register of Slovenia, those over 61 years of age agree the most, and those younger than 20 years of age agree the least. Because of the above, it can be assumed that older respondents are more careful when making online purchases, show greater concern for their safety in doing so and are less confident than younger ones. The reasons why younger people are less careful when carrying out certain activities online should be explored in more detail.

Conclusions

In the research, we asked the respondents about their actions when visiting the website, how to use passwords, how to install anti-virus software and other activities related to the protection of personal data. It was found that respondents most often simply confirm the offered cookies to access the desired website, as well as do not read the terms and privacy policy when using a particular online service. It was further found that the older generations read the terms and privacy policy more often than the younger generation. We attribute such behaviours to a lack of will and time in today's fast-paced way of everyday life.

Respondents were also asked about the legal grounds on which companies and other organizations can process the personal data of individuals. From the answers received, it can be concluded that the respondents do not know enough about all available legal bases, as most of them chose the answer that their personal data can be processed if they have given their consent.

In the research, we were also interested in the practices of respondents when using the method of shopping online. From the received answers it can be concluded that many respondents have included the service of immediate notification of the transaction, which can be assessed as positive, but on the other hand, respondents use the least way to verify the credibility of the payee by inspecting the Business Register.

The mentioned research could be carried out periodically in the future and on a possible larger sample, which would enable easier generalization, which the sample used in our research did not allow. This would make it possible to identify differences or deviations based on which it would be possible to make recommendations or improve the existing situation in this area.

Individuals are primarily aware of threats to the protection of personal data, but at the cost of certain benefits or simply out of convenience, they often ignore certain information available to them that could further protect their personal data. Thus, it often happens that individuals do not read the terms and privacy policy when using online services, or simply confirm the cookies offered to access the desired website, as this path is at first glance easier for the individual.

Individuals often see only that attractive and interesting part that is offered to them by the use of certain service (such as shopping from a home armchair or online) or the use of online social networks. In doing so, we suggest that individuals consider whether the use of a particular service or the public disclosure and sharing of certain personal information represents so much added value for them that they are willing to sacrifice part of their privacy for it.

According to the obtained results of the survey questionnaires, the recommendation to individual users of modern information technologies refers mainly to the consistent use of the possibilities and tools they offer for greater protection, as there are still untapped possibilities for data protection.

From the individual's point of view, he must be familiar with the processing of personal data and its purposes for which data are processed by individual companies and other organizations, as well as that he is well acquainted with the legal bases for processing. The individual must be aware that he is protected by the applicable legislation governing the protection of personal data and within which he can demand the protection of his rights.

Individuals are recommended to ensure the security of personal data either by knowing the environment in which they have personal data, to know at all times where it is located, to whom they have entrusted it for further processing, etc. Password policy must be followed, which means that individuals regularly change passwords on their devices to select and use secure passwords (not less than eight characters, etc.), use different passwords to access different applications/devices. It is also important to take care of updating anti-virus programs on devices and, in the event of detected shortcomings, to introduce new measures on their own initiative or to adapt existing measures.

References

Ahtik, Meta, Maja Bogataj Jančič, Maja Brkan, Bojan Bugarič, Matija Damjan, Aleš Galič, Andrej Grah Whatmough, Peter Grilc, Miha Juhart, Boštjan Koritnik, Jerca Kramberger Škerl, Jure Levovnik, Blaž Markelj, Luka Markelj, Špelca Mežnar, Neža Muhič, Neža Pogorelčnik, Jernej Pusser, Lojze Ude, Katarina Zajc in Sabina Zgaga. 2014. *Pravo v informacijski družbi*. Ljubljana: IUS Software, GV Založba.

Ausloos, Jef, Michael Veale in Rene Mahieu. 2019. Getting Data Subject Rights Right. *Journal of Intellectual Property, Information Technology, and Electronic Commerce Law (JIPITEC) 10* (3): 283–309.

Burton, Cedric, Laura De Boel, Christopher Kuner, Anna Pateraki, Sarah Cadiot in Sara Gabriella Hoffman. 2016. The Final European Union General Data Protection Regulation. Privacy and Security Law Report 15: 1–13.

Bernard Korpar, Janja, Sašo Dolenc, Maša Galič, Martin Jančar, Zoran Kanduč, Tina Korošec, Primož Križnar, Liljana Selinšek, Janez Stušek, Helena Uršič, Aleš Završnik in Sabina Zgaga. 2018. *Pravo in nadzor v dobi velikega podatkovja*. Ljubljana: Pravna fakulteta, Inštitut za kriminologijo pri Pravni fakulteti v Ljubljani.

Cerar, Miro, Marijan Pavčnik, Albin Igličar, Erik Kerševan, Vladimir Simič, Mirjam Škrk, Franc Testen in Dragica Wedam Lukić. 2009. *Pravna država*. Ljubljana: GV Založba.

Goddard, Michelle. 2017. The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research 59* (6): 703–705.

Haskins, Jane. 2018. *8 Smart Ways to Protect Your Personal Data*. Https://www.legalzoom.com/articles/8-smart-ways-to-protect-your-personal-data (22. 4. 2020).

Hoofnagle, Chris Jay, Bart van der Sloot in Frederik Zuiderveen Borgesius. 2019. The European Union General Data Protection Regulation: What It Is And What It Means. *Information & Communications Technology Law 28* (1): 65–98.

Information Commissioner. 2015. *Zavarovanje osebnih podatkov*. Https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_o_zavarovanju_OP.pdf (5. 8. 2019).

Information Commissioner. 2019. *Smernice o orodjih za zaščito zasebnosti na internetu: Kaj lahko sami naredimo za zasebnost na internetu?* Https://www.ip-rs.si/publikacije/prirocniki-in-smernice/o-orodjih-za-zascito-zasebnosti-na-internetu/ (22. 4. 2020).

Kovačič, Matej. 2003. *Zasebnost na internetu*. Ljubljana: Mirovni inštitut za sodobne družbene in politične študije.

Kovačič, Matej. 2006. *Nadzor in zasebnost v informacijski družbi*. Ljubljana: Fakulteta za družbene vede.

Kovačič, Matej, David Modic, Marko Rusjan, Liljana Selinšek, Janko Šavnik in Aleš Završnik. 2010. Kriminaliteta in tehnologija: *Kako računalniki spreminjajo nadzor in zasebnost, ter kriminaliteto in kazenski pregon*? Ljubljana: Inštitut za kriminologijo pri Pravni fakulteti.

Makarovič, Boštjan, Damjan Možina, Špela Mežnar, Domen Bizjak, Maja Bogataj in Goran Klemenčič. 2003. *Internet in pravo*. Ljubljana: Pravna fakulteta Univerze v Ljubljani.

Markovič, Zlatka, Maja Brajnik, Tim Pahor, Sandra Pjanić, Eva Langeršek, Benjamin Lesjak, Aljaž Lep in Denis Trinkaus. 2019. *Varstvo osebnih podatkov po uredbi (GDPR)*. Ljubljana: Založba Reforma d. o. o.

Politou, Eugenia, Efthimios Alepis in Constantinos Patsakis. 2018. Forgetting personal data and revoking consent under the GDPR: challenges and proposed solutions. *Journal of Cybersecurity 4* (4): 1–20.

Roszak, Theodore. 1994. *The Cult of Information: A Neo-Luddite Treatise on High-Tech, Artificial Intelligence, and the True Art of Thinking*. Berkeley; Los Angeles: University of California Press.

Tikkinen-Piri, Christina, Anna Rohunen in Jouni Markkula. 2017. EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Compute Law & Security Review 34* (1): 134–153.

Turk, Boštjan Juš in Nika Vogrinčič. 2019. *Internetno pravo z izvlečki najpomembnejših zakonov*. Ljubljana: Inštitut za civilno in gospodarsko pravo.

Voight, Paul. 2017. *The EU General Data Protection Regulation (GDPR).* Cham: Springer International Publishing AG.

Wacks, Raymond. 2018. *Zasebnost: zelo kratek uvod*. Ljubljana: Založba Krtina.

Wagner DeCew, Judith. 1997. *Law, Ethics, and the Rise of Technology*. Ithaca, London: Cornell University Press.

Moti Zwilling, Galit Klien, Dušan Lesjak, Łukasz Wiechetek, Fatih Cetin & Hamdullah Nejat Basim. 2020. Cyber Security Awareness, Knowledge and Behavior: A Comparative Study, *Journal of Computer Information Systems*, DOI: 10.1080/08874417.2020.1712269