SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2020
ORGANIZATION AND MANAGEMENT SERIES NO. 144

E-COMMERCE AND GDPR CHALLENGES FOR TODAY'S ENTREPRENEUR

Monika SZYMURA

Opole University of Technology; M.Szymura@po.edu.pl, ORCID: 0000-0003-2148-0691

Purpose: On 25.05.2018, Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (GDPR) entered into force. This act established new obligations for controllers and other data processors, and their proper implementation can often be a challenge, especially in light of the system of criminal sanctions in cases of non-compliance. The goal of this article is to discuss challenges and consequences in the e-commerce sector related to the changes in personal data protection laws in the industry.
Design/methodology/approach: The deliberations are based on the related subject literature and an analysis of the legal provisions applicable in the area under discussion.
Findings: The main challenge faced by entrepreneurs is ensuring the safety of personal data at an appropriate level in relation to their potential breaches. This approach is based on technological neutrality and risk, and it results in the requirements to be met by entrepreneurs to become more flexible, and for the implemented protection measures to be relativized.
Practical implications: The simplifications introduced by the GDPR are beneficial for small- and medium-sized entrepreneurs for whom data processing is their main activity. It is not required in small organizations, which generate lower costs.
Originality/value: The publication discusses the issue from the perspective of the e-commerce industry, explaining in particular the new obligations of controllers, the principles of data processing, and the exercising of data subjects' rights.

Keywords: e-commerce, data, controller.

Category of the paper: Viewpoint, literature review.

1. Introduction

On 25 May 2018, the General Data Protection Regulation of 6 April 2016 (the GDPR) entered into force in the entire EU territory. The legal basis of this regulation is Article 16(2) of the Treaty on the Functioning of the European Union. According to Article 16(2) of this Treaty, the European Parliament and the EU Council determine rules relating to the protection

of natural persons with regard to processing of personal data by institutions, authorities, and organizational units of the EU and the Member States in conducting activities within the scope of the applicable EU law, as well as the rules of free movement of such data (OJ C 326/2012). Motive 2 of the GDPR preamble states that "the principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons" (Regulation (EU) 2016/679).

The Supreme Administrative Court, in its decision of 31 January 2012, concluded that the controller of personal data is a data controller who decides about the goals and the means of processing of such data (I OSK 1317/11). While using personal data in business activities, an entrepreneur is most often their controller, and it is the controller who, starting from 25 May 2018, has the obligation to implement the regulation requirements and is later required to maintain and update the data protection system in accordance with the GDPR legal provisions.

The basic challenge faced by the entrepreneurs is to ensure a level of personal data protection that is adequate with respect to its potential breaches. The GDPR introduces in this regard a risk-based approach. The controllers assess each of the data processing tasks independently, in order to select protection appropriate to the risk such processes involve.

The goal of this article is to discuss challenges and consequences in the e-commerce sector related to the changes in personal data protection laws in the industry. The main areas of change are covered, with a particular focus on the new rights of data subjects and the obligations of the controllers and processors of personal data. The deliberations are based on the related subject literature and an analysis of the legal provisions applicable in the area under discussion.

2. E-commerce – a modern form of entrepreneurship

The term *e-commerce* emerged in the 1990s and has been evolving since then (Bartczak, 2016). According to the Organisation for Economic Co-operation and Development (OECD), "an e-commerce transaction is the sale or purchase of goods or services, conducted over computer networks by methods specifically designed for the purpose of receiving or placing of orders. The goods or services are ordered by those methods, but the payment and the ultimate delivery of the goods or services do not have to be conducted online. An e-commerce transaction can be between enterprises, households, individuals, governments, and other public

or private organisations. To be included are orders made over the web, extranet or electronic data interchange" (OECD).

According to the definition adopted by the Federal Networking Council in the USA, the Internet is a global information system that "is logically linked together by a globally unique address space based on the Internet Protocol (IP) or its subsequent extensions/follow-ons; is able to support communications using the Transmission Control Protocol/Internet Protocol (TCP/IP) suite or its subsequent extensions/follow-ons, and/or other IP-compatible protocols; and provides, uses or makes accessible, either publicly or privately, high level services layered on the communications and related infrastructure" (FNC).

Finally, the World Trade Organisation (WTO) defines e-commerce as "production, distribution, marketing, sale or delivery of goods and services by electronic means" (WTO).

In summary, e-commerce encompasses everything related to the purchases and sales of goods and services online (Żukowska, Komańda, 2009). Examples of such are Internet browsers, Internet communicators, streaming, sharing of mobile apps, and electronic mail (Bar, Lamik, 2018). The e-commerce market is characterized by a lack of geographical and time limitations and the ability to deliver any amount of information in various forms to various recipients. An undoubted plus in this regard is the ease of starting an e-commerce business, which involves relatively low initial costs (Yevtushenko, 2017).

The duties of electronic services providers, the exclusion principles of their liability, and the principles of personal data protection for natural persons using electronic services, are regulated in the Polish legal system by the Act of 18 July 2002 on Providing Services by Electronic Means. The act implements the directive on electronic commerce. The provision of services by electronic means should be understood as "performance through a transfer of data upon an individual request of a customer, sent and received via devices for electronic processing, including digital compression, and storing data that is sent, received or transmitted through a telecommunication network within the meaning of the Telecommunications Act of 16 July 2004" (Journal of Laws, Item 123, 2019, Article 1, Item 1). Examples of the above are searching content on the Internet, Internet communicators, streaming, mobile apps sharing, and electronic mail (Bar, Lamik, 2018).

The use of electronic mail or other equivalent means for transferring individual information, for example through natural persons acting outside of their trade, business, or professional activity, including the use in order to conclude an agreement between such persons, is excluded from the provisions of the act (Journal of Laws, Item 123, Article 2, Item 3, 2019). In addition, the following items do not constitute electronic services: statutory audit of accounting books, medical consultation requiring a physical examination of the patient, accessing an electronic catalogue in a shop in the physical presence of the customer, booking of airfares at a travel agency in the physical presence of the customer via a computer network, sharing electronic games in an arcade in the physical presence of the user, and voice telephony (Bar, Lamik, 2018).

3. Data processing

According to Article 4(2) of the GDPR, processing "means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction" (Article 4(2) GDPR). This list is not exhaustive.

There are different preconditions for the processing of personal data in relation to both ordinary personal data and special categories of personal data listed in the regulation. The processing of ordinary data is permitted if it complies with at least one of the preconditions listed in Article 6(1) of the GDPR. The regulation imposes a general ban on the processing of sensitive personal data, with exceptions listed in Article 9(2); e.g., when data are necessary to claim rights in a court proceeding, or when data have been made public by the person they concern. The catalogue of such legal preconditions is exhaustive (Krasuski, 2018).

The basis for the processing of personal data is an act of consent, defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (Article 14(11), GDPR). Granting of consent should be conscious, specific, clear, and voluntary. Most often it is expressed by accepting a consent clause via ticking or checking of a "checkbox", but it can be granted without it (e.g., by subscribing to a newsletter). It is unacceptable to combine consents concerning different purposes.

Order execution gives the right to process a customer's personal data in order to execute the order, in accordance with Article 6(1)(b) of the GDPR. Consent is also not required for processing personal data for marketing purposes (marketing of one's own services and products). An additional precondition is obtaining data legally (Głąb, 2018).

The obligation to register personal data sets has been removed by the GDPR. The data controller is obligated to maintain a register of processing activities. Article 30(5) of the GDPR states that "this obligation shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences" (GDPR, 2018, Article 30(5)).

The register of personal data processing activities is of significance in that it confirms that a given entrepreneur processes personal data in accordance with the law. It is helpful in the implementation of proper security measures. Maintaining this kind of documentation can thus

also prove useful for entities that are not obligated to create a register of data processing activities.

A characteristic of e-commerce activity is a market without borders. The basis of data transfers is the decision of the European Commission determining the suitability of protection in a third country, adequate personal data protection safeguards, and specific situations in relation to which the regulation provides derogations (Lubasz, 2018).

The regulation introduced the *one stop shop* model, whereby the supervision of transnational entrepreneurs is based on a consolidated model. Entities conducting business in more than one Member State (processing transnational data) are under the supervision of the competent ("lead") supervisory authority in the EU, determined based on the location of the company's head office, and the supervisory authorities of the countries in which the business activity is conducted or the processing takes place with support of the lead supervisory authority (Gawroński, 2018).

Doubts may arise as to which types of operations on data are subject to these provisions. A physical transfer of data outside of the EU and their processing via tools located outside this area (cloud-based or hosting) is clearly one of such actions. The qualifying provision of other online services to this group is not so simple. The following decision of the Court of Justice may be helpful: "There is no transfer [of data] to a third country within the meaning of Article 25 of Directive 95/46 where an individual in a Member State loads personal data onto an internet page which is stored with his hosting provider which is established in that State or in another Member State, thereby making those data accessible to anyone who connects to the internet, including people in a third country" (Case C-101/01).

4. Protection of data subject laws

E-commerce entrepreneurs should include in their privacy policy content that is compliant with the provision of law and ensure it is located in an adequate place, as well as give their customers access to their privacy policy. A privacy policy should be written in simple, easily understandable language. Anyone can request the data controller to inform them as to whether their personal data are being processed, and if so, can request a transfer to a different data controller of their own indication.

Action on applications and requests from people to whom data apply should be undertaken immediately, and no later than within a month of the receipt of the request by the controller. If necessary, this deadline can be postponed for two subsequent months due to the complicated nature of the request or to the number of the requests. The interested person should be informed if this is the case (GDPR, 2018, Article 12(3)).

The person to whom data applies has been granted a "right to be forgotten". This means that such a person can request immediate removal of his or her personal data by the controller. Such a request can be made, among other reasons, when data are no longer needed for the purposes for which they were collected or processed, when the data subject withdraws his or her consent for personal data processing, or when the data subject objects to its processing (GDPR, 2018, Article 17(1)). In such cases, the data controller is obligated to immediately remove the relevant personal data.

If the request for removal concerns data already made public, the regulation imposes on the controller an obligation to take additional measures. The controller should inform other controllers processing such data about the request for their removal. This applies also to the removal of links to data, and copies and replications of those data. A request for data removal directed at the controller of a social media portal triggers the need for the portal administrator to notify the browser operators about the need to remove data from search results (Lubasz, 2018).

An entirely new concept introduced in the GDPR is the right to transfer data: "the data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided" (GDPR, 2018, Article 20(1)).

In accordance with Article 21(1) and 21(2), "the data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions" (GDPR, 2018).

The contents of Section 2 of this Article indicate that "where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing" (GDPR, 2018).

The obligation of a data controller who conducts profiling is to give notification of the profiling of the subject who is being profiled. The controller should provide profiling rules, the meaning of the profiling, its foreseeable consequences, and information about the right to object or not to be subject to decisions made as a result of profiling. This obligation is met through the provision of information on the order form or via email (Dębicka, Bordo, et al., 2017).

A breach of personal data protection rules can result in the imposition of a penalty of up to €10 million, or 2% of the total annual turnover of the company (GDPR, 2018, Article 83(4)) and a penalty of up to €20 million or 4% of the total annual turnover (GDPR, 2018, Article 83(5)). The former applies to technological and organizational breaches of data processing rules, including non-implementation of adequate personal data protection measures, liability for applied solutions by the processors, or the failure to report breaches of personal data

security. The latter applies to breaches of the fundamental rules of processing, including the terms of the consent, transferring of the personal data to a recipient in a third country or an international organization, or failure to observe an order on a temporary or final limitation of processing, or suspension of data flow decided by a supervisory authority.

The specified amounts are not absolute. A maximum financial penalty is determined by specifying the upper limit (up to €10 million or €20 million) and the percentage of annual worldwide turnover from the previous financial year (up to 2% or 4%). The upper limit is the higher of these amounts (Bielak-Jomaa, Lubasz, 2018).

5. New obligations of the entrepreneur

The entrepreneur is obligated to implement adequate technical and organizational measures ensuring compliance of their data processing with the provisions of the GDPR. This includes in particular the rules indicated in Articles 5(1) and 5(2), i.e., the rule of conformity with the law, fairness and transparency, purpose limitation, integrity and confidentiality, and the rule of accountability imposing on the controller the responsibility for compliance with the rules of processing and the obligation to ensure a possibility to demonstrate compliance (Bielak-Jomaa, Lubasz, 2018).

The obligation to take data protection into consideration in the design phase necessitates the implementation of adequate technical and organizational measures in order to ensure data safety and protection of privacy from the initial phases of planning data processing (Article 25). Of course, this rule also applies to the phase of execution of data processing. Because an entrepreneur should avoid and be ready to intercept privacy and safety breaches, it is recommended that they conduct periodic reviews of the functioning of the data processing; e.g., by verifying the way in which consents are collected or information obligations are met.

Article 25(2) of the GDPR states that "the controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons" (GDPR, 2018, Article 25(2)).

Default settings that could interfere with the privacy of data subjects are prohibited. The person whose data are subject to protection can make decisions about limiting his or her right to privacy, e.g., by enabling or disabling some functions.

Difficulties can necessitate the implementation of a data protection impact assessment (DPIA) obligation: "where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data" (GDPR, 2018, Article 35(1)).

A DPIA is a process of analysing a company's personal data processing systems and solutions, and an assessment of the risk of breaches in different processing categories.

This is a complicated process, and its implementation has to be approved by the supervisory authority that specifies the types of processing that have to undergo a DPIA. The Personal Data Protection Office specifies nine types of personal data processing operations that require an assessment of the impact on data protection (The President of the Personal Data Protection Office). The list, however, should not be considered as exhaustive.

In accordance with the contents of Article 36(1), "the controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk".

Among the remaining obligations are the following: documenting every processing activity, maintaining the safety of processing and preventing breaches of regulation provisions, and the obligation to notifying a supervisory authority and the data subject about any cases of breaches of data protection.

6. Conclusion

An e-commerce activity entails the processing of personal data. Data protection is characterized by a high level of protection of natural persons, due to the processing of their personal data.

The main challenge faced by entrepreneurs is ensuring the safety of personal data at an appropriate level in relation to their potential breaches. This approach is based on technological neutrality and risk, and it results in the requirements to be met by entrepreneurs to become more flexible, and for the implemented protection measures to be relativized. Because it is the entrepreneurs who perform an independent assessment of the risk of data processing, in order to select adequate security measures in relation to the threats data processing brings, they have to become deeply involved in the implementation of their obligations resulting from the GDPR provisions. Each entrepreneur should perform a detailed analysis of, among others, the owned documentation (internal and external), the scope of the

processed data, and the security measures applied. It should be emphasized that assessment of impact with respect to data protection refers only to risky activities related to data processing.

The simplifications introduced by the GDPR are beneficial for small- and medium-sized entrepreneurs for whom data processing is their main activity. It is not required in small organizations, which generate lower costs.

References

1. Yevtushenko, A. (2017). E-commerce jako innowacyjna forma przedsiębiorczości. In: J. Górski (ed.), *Teraz Polska Promocja i Rozwój – tom 9, e-book.* Warszawa: Fundacja Polskiego Godła Promocyjnego, https://terazpolska.pl/upload/File/Teraz_Polska_Promocja_i_Rozw%C3%B3j_2017_ebook_tom_IX.pdf#page=25, 30.05.2019.
2. Bar, G., Lamik, W. (2018). Świadczenie usług drogą elektroniczną i ochrona konsumenta w sieci. *Radca Prawny. Zeszyty naukowe, 2(15)*, 25-62. http://kirp.pl/publikacja/radca-prawny-zeszyty-naukowe-nr-2-15-2018/ , 3.06.2019.
3. Bartczak, K. (2016). *Bariery rozwojowe handlu elektronicznego.* Wrocław: Exante.
4. Bielak-Jomaa, E., Lubasz, D. (eds.) (2018). *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*. Warszawa: WKP.
5. Case C-101/01 Judgment of the Court, 6 November 2003, Criminal proceedings against Bodil Lindqvist, *European Court Reports 2003 I-12971*, ECLI identifier: ECLI:EU:C:2003:596, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62001CJ0101, 23.05.2019.
6. Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326 (2012).
7. Dębicka, O., Bordo, A., Winiarski, J. (2017). Ochrona danych osobowych w branży e-commerce w Polsce. *Zeszyty Naukowe Uniwersytetu Gdańskiego. Studia i Materiały Instytutu Transportu i Handlu Morskiego, 14*, 145-157, doi: https://doi.org/10.26881/sim.2017.4.08.
8. Fisher, B. (2017). Prywatność informacyjna w usługach audiowizualnych z perspektywy nowych rozporządzeń unijnych (RODO i EPR). *Zeszyty Prasoznawcze*, *229*, 151-171.
9. FNC Resolution: Definition of "Internet" 10/24/95, https://people.ucalgary.ca/~bakardji/Internet/definition.html, 25.05.2019.
10. Gawroński, M. (ed.) (2018). *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*. Warszawa: WKP.
11. Komunikat Prezesa Urzędu Ochrony Danych Osobowych w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony, MP, poz. 827 (2018).

12. Krasuski, A. *Ochrona danych osobowych na podstawie RODO* (2018). Warszawa: WKP.
13. Lubasz, D. (ed.) (2018). *Rodo w e-commerce*. Warszawa: WPK
14. Głąb, P. *Rodo w e-commerce*, https://marketingibiznes.pl/prawo-w-biznesie/rodo-w-e-commerce/, 2.06.2019.
15. Regulation (EU) 2016/679 of the European parliament and of the Council 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, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN, 23.05.2019.
16. Ustawa o świadczeniu usług drogą elektroniczną, Dz.U. poz.123 (2019).
17. WTO, https://www.wto.org/english/thewto_e/minist_e/mc11_e/briefing_notes_e/bfecom_e.htm, 22.05.2019.
18. Wyrok NSA z dnia 31 stycznia 2012 r. (I OSK 1317/11), http://orzeczenia.nsa.gov.pl, 25.05.2019.
19. Żukowska, J., Komańda, M. (2009). E-commerce w ujęciu rynku polskiego. In: J. Rokita, W. Czakon, A. Samborski, *Współczesne i perspektywistyczne kierunki badań w zarządzaniu przedsiębiorstwami* (pp. 551-559). Katowice: Prace Naukowe Akademii Ekonomicznej.