**УДК 34.03**

Новиков Илья Игоревич

Уральский государственный юридический университет

Россия, Екатеринбург

[mlgnaticus@gmail.com](mailto:mlgnaticus@gmail.com)

**«ОТВЕТСТВЕННОСТЬ ОРГАНИЗАЦИИ ЗА УТЕЧКУ ПЕРСОНАЛЬНЫХ ДАННЫХ»**

**Аннотация:** Данная статья освящает общие вопросы, касающиеся ответственности организации за утечку персональных данных. В этой работе автор пытается проанализировать различные модели ответственности за похожие правонарушения в правовой системе стран ЕС и Российской Федерации.

**Ключевые слова**: персональные данные, утечка персональных данных, ответственность за утечку персональных данных, кража данных, оператор данных, обработчик данных, организация и данные

We are sharing our personal information every minute. We are getting amazed by the response of unlocking our device using fingerprint. We are using our bank cards to pay for online purchases, and we are adding a real residence address for delivery. Furthermore, our smartphones and smartwatches are tracking every step we take and every calorie we lost. And if in 2001 someone who had stolen our account could only use it for posting some messages, right now, losing your information, could lead to losing a «virtual version» of you. So, data leakage from some service can lead to tragic consequences for a person. And, unfortunately, it is impossible to be sure of the safety of your data. Because every device, every symbol in code is created by person. There is no guarantee, that there will be no mistakes. For example, a well-known telecom operator made a mistake in the code of web-site which had allowed users to find message texts through a search engine[[1]](#endnote-1). Administrator’s account of a forum was hacked, and the database was stolen[[2]](#endnote-2). Popular hotel had leaked data of millions of customers for 4 years[[3]](#endnote-3).

From these examples, we see that data can be lost at any time, regardless of the interests of a person: whether he is a gamer, or he is a traveler, or he just uses messenger on the web site of telecom operator. So, each organization must be ready to take responsibility. In order to discuss liability, we should set some preferences. First, it is necessary to identify the nature of the information that we can consider as personal data the loss of which will lead to irreparable consequences. Russian personal data legislation corresponds to the European standards due to the implementation of principles of European acts like GDPR[[4]](#endnote-4).

There is another question: can the incorporation of principles from European states serve as a guarantee of trust of European countries to Russian personal data legislation? Recent case of CJEU on the Schrems II settles that not only data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses must be afforded a level of protection essentially equivalent to that guaranteed within the EU by the GDPR but also the assessment of that level of protection must consider both the contractual clauses agreed between the data exporter established in the EU and the recipient of the transfer established in the third country concerned, and, as regards any access by the public authorities of that third country to the data transferred, the relevant aspects of the legal system of that third country.[[5]](#endnote-5) So, in this case the court decided that EU – US Privacy shield (standards for cross-border processing of personal data with a commercial intention within Europe and USA) has no legal force.

According to the Article 3 of the Federal Law of the Russian Federation “On the Data Protection”, personal data is any information which is related to the data subject. So, the law has not named the fixed list of data treated as personal data. And the court should decide what should be considered as personal data in different cases. In my opinion, that is not a mistake of the Russian legislator. Because of constant development of technology and society it would be wrong to limit the list of data as, for example, 20 years ago we had no idea that we would use our biometric data to have access to our phones. Therefore, the courts must fulfill their direct function, *i.e.* to consider all the circumstances of the case and resolve the dispute essentially. For example, right now the courts consider combination of surname, first name and patronymic with a phone number or e-mail, banking account, passport biometric data, and etc. as personal data. [[6]](#endnote-6)

Attention should be also paid to the fact that the Federal Law of the Russian Federation “On the Data Protection” aims to protect constitutional human rights such as privacy right and freedom from arbitrary interference with family. So, we can draw a conclusion that personal data should be considered as complex information. Unauthorized access to this information can lead to violation of constitutional rights of human. And if the password of your e-mail could be changed, leaking biometrical information can be a result of losing method of authorization, fingerprint, for example. Every person has its own papillary pattern. It is unique and stays the same for the whole lifetime. It cannot be removed because it regenerates. And if somehow this pattern was lost, you will never be able to use it as a method of authentication.

So, we defined what information can be considered as personal data and how important it is for any person. Also, we assessed the risk of losing the data. Another ground for liability of organization is “guilt”. To understand the sense of GDPR, we need to discover what parties are participating in data processing. Data controller is a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of the processing of personal data, for example, social network or a taxi. Data processor is a natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller, for example, cloud service providers. Data subject (person) is an identifiable natural person, *i.e.* one who can be identified directly or indirectly. Article 32 of GDPR sets obligations for controller and processor. They must depersonalize the information, to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services, possibility to restore personal data in the event of a physical or technical incident; to regulate the process of regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing. GDPT sets a liability for the controller and processor for infringement of the Regulation. Any controller involved in the processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. A controller or processor shall be exempt from liability if they prove that they are in no way responsible for the event giving rise to the damage.

And here I would like to show you a difference between the practice of the courts in Russian Federation and the European courts. In the Russian Federation the organization is also liable if its guilt is proven, and this organization violated the law. The organization can be administratively liable (fine), be a civil defendant (compensation of losses and compensation for moral damage to a citizen), be liable to prosecution (if it is a crime). But there is one more problem of how to expose the organization for violations of legislation on personal data in the Russian Federation. European Regulation GDPT allowed to fine organizations up to 20,000,000 Euros (or up to 4% of global income for the Organization). And the court practice in Europe proves that: «Belgian DPA imposes 20,000 Euros fine on Proximus for several data protection infringements»[[7]](#endnote-7). Russian fines are insignificantly low. Average fine for the data protection violation is 70,000 Rubles (766 Euros) and for large organization it will matter nothing. The most significant fine for repeated violation while dealing with personal data is established for the processing of personal data without using databases located in Russia for recording, systematizing, accumulating, storing, clarifying (updating, changing) or extracting personal data of citizens of the Russian Federation, *i.e.* 18,000,000 Rubles (197,000 Euros). Another problem is civil liability. This issue is very controversial in the Russian practice. Only a few years ago the courts began to compensate non-pecuniary damage in an adequate amount, but only in exceptional cases when the violation resulted in the death or disability of a person (approximately 16,000 Euros and 8,000 Euros, as the case might be). In other cases, the compensation is much smaller. In general, there are no problems with compensation for damages if the plaintiff can prove the damage. In the end, we can see that the liability of organizations in Russia is not as immense as in Europe. Although, if we consider the annual turnover of the leading organizations that are somehow related to the processing of personal data, we could see that such small fines and a sluggish prospect of damages and compensation cannot provide sufficient level of security and protection of the constitutional rights of citizens. By immense the liability for insufficient data protection measures, we can stimulate organizations to develop and improve their security systems as it is more logical to spend money by financing the development than just buying off the consequences that have already come.

List of references.

1. Federal Law of Russian Federation on the data protection: scientific practical commentary/ A.H. Gafurova, E.V. Dorotenko, Y.E. Kontemirov and others.; editor: A.A. Priezzheva. M.: The editorial office of the Russian newspaper, 2015. release 11

FORUM DATABASE LEAK// multiplayer community for Euro Truck Simulator 2 URL: https://truckersmp.com/blog/9 (access date: 20.10.2020).

1. Marriott International faces class action suit over mass data breach // RBC media holding, news URL: https://www.rbc.ru/business/20/08/2020/5f3dc3ca9a794721a8f10076 (access date: 20.10.2020).
2. Federal Law of Russian Federation on the data protection: scientific practical commentary/ A.H. Gafurova, E.V. Dorotenko, Y.E. Kontemirov and others.; editor: A.A. Priezzheva. M.: The editorial office of the Russian newspaper, 2015. release 11

The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield // Court of Justice of the European Union, Press and Information URL: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf (access date: 20.10.2020).

The appellate decision of the Novosibirsk Regional Court under date of 4 july 2017. Case № 33-6394/2017

1. Belgian DPA imposes €20.000 fine on Proximus for several data protection infringements // The European Data Protection Board URL: https://edpb.europa.eu/news/national-news/2020/belgian-dpa-imposes-eu20000-fine-proximus-several-data-protection\_en (access date: 20.10.2020).

Novikov Ilya Igorevich

Ural State Law University

Russia, Yekaterinburg

Mlngaticus@gmail.com

**THE RESPONSIBILITY OF ORGANIZATION FOR DATA LEAKAGE**

**Abstract:** This article focuses on the general issues related to the organization's liability for personal data leakage. In this work, the author tries to analyze various models of responsibility for similar offenses in the legal system of the EU countries and the Russian Federation.

**Key words**: personal data, personal data leakage, liability for personal data leakage, hacked data, Data processor, Data controller, organization and data.

1. The court confirmed 30 000 Rubles fine for "Megafon" due to SMS leak // Russian agency of international information «RIA Novosti» URL: https://ria.ru/20111026/471358290.html (date of the application: 20.10.2020). [↑](#endnote-ref-1)
2. FORUM DATABASE LEAK// multiplayer community for Euro Truck Simulator 2 URL: https://truckersmp.com/blog/9 (access date: 20.10.2020). [↑](#endnote-ref-2)
3. Marriott International faces class action suit over mass data breach // RBC media holding, news URL: https://www.rbc.ru/business/20/08/2020/5f3dc3ca9a794721a8f10076 (access date: 20.10.2020). [↑](#endnote-ref-3)
4. Federal Law of Russian Federation on the data protection: scientific practical commentary/ A.H. Gafurova, E.V. Dorotenko, Y.E. Kontemirov and others.; editor: A.A. Priezzheva. M.: The editorial office of the Russian newspaper, 2015. release 11. [↑](#endnote-ref-4)
5. The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield // Court of Justice of the European Union, Press and Information URL: https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091en.pdf (access date: 20.10.2020). [↑](#endnote-ref-5)
6. The appellate decision of the Novosibirsk Regional Court under date of 4 july 2017. Case № 33-6394/2017 [↑](#endnote-ref-6)
7. Belgian DPA imposes €20.000 fine on Proximus for several data protection infringements // The European Data Protection Board URL: https://edpb.europa.eu/news/national-news/2020/belgian-dpa-imposes-eu20000-fine-proximus-several-data-protection\_en (access date: 20.10.2020). [↑](#endnote-ref-7)