

Krešimir Starčević
Atlantic Grupa d.d.
Miramarska 23,
10000 Zagreb, Croatia
krešimir.starcevic@atlanticgrupa.com
Phone: +38512413119

Boris Crnković
Josip Juraj Strossmayer
University of Osijek
Faculty of Economics in Osijek
Trg Ljudevita Gaja 7,
31000 Osijek, Croatia
boris.crnkovic@efos.hr
Phone: +38531224473

Jerko Glavaš
Josip Juraj Strossmayer
University of Osijek
Faculty of Economics in Osijek
Trg Ljudevita Gaja 7,
31000 Osijek, Croatia
jerko.glavas@efos.hr
Phone: +38531224473

UDK: 342.721(497.5)
Preliminary communication

Received: April 9, 2018
Accepted for publishing: May 28, 2018

This work is licensed under a
Creative Commons Attribution-
NonCommercial-NoDerivatives 4.0
International License



IMPLEMENTATION OF THE GENERAL DATA PROTECTION REGULATION IN COMPANIES IN THE REPUBLIC OF CROATIA

Abstract

This paper deals with the current issue of protecting individuals regarding the processing of their personal data and the free movement of such data. As this matter is also regulated by the European Union legislation, the paper describes and analyzes the scope, implications, methods and tools for applying the new EU regulation adopted on 27 April 2016 by the Parliament and the Council of the European Union. The subject matter is the Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. The short title of this Regulation is *General Data Protection Regulation* (GDPR). The term GDPR is thus in common everyday use in companies and among business people, and will also be used in this paper. In addition, the paper analyzes the research conducted on the existing state of affairs and the way in which all collected personal data are processed and used by all stakeholders in the company Atlantic Grupa d.d., Zagreb. In addition, a harmonized project of a structured and methodologically correct procedure for implementation of the provisions of the new Regulation is described for the purpose of achieving the highest degree of compliance of all members of Atlantic Grupa d.d. with the provisions of the GDPR. Finally, the basic objective of the described project is explained, which is to avoid situations that would lead to the extremely high fines for non-compliance with the Regulation.

Keywords: Protection of individuals and their personal data, General Data Protection Regulation (GDPR), Atlantic Grupa d.d.

1. Introduction

1.1 Selected topic

The use of personal data and the question of its protection has always been part of everyday life of all of us, in almost all spheres of activity we are engaged or involved in — from employment to health care, communication with state institutions, participation in prize games, browsing of Internet content etc. Knowingly or unknowingly, we give away our personal information, knowing or not knowing, or not thinking, about the fact that our data is stored somewhere, reviewed, analyzed, and may be transferred to third parties or used for some purpose we may not agree with.

The large amount of personal data accumulated over the years in different places — from public and state authorities to banks, employers, insurers, healthcare systems, businesses — as well as the accelerated development of electronic processing and exchange of personal data, and above all the accelerated and ubiquitous trend of the availability of personal data on the Internet and social networks, has required a normative solution to strengthen and commonly regulate the area of personal data protection.

The 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 (the **Regulation** or **GDPR**) is just such a solution.¹ The Regulation also puts an end to the previous Personal Data Protection Directive (95/46/EC) concerning the processing and free movement of personal data. The Regulation will be in direct implementation in all EU Member States starting on **25 May 2018**, which means that, by its legal force, it becomes the umbrella EU data protection law, which will be directly implemented in the legislation of all EU members without the possibility of interpretation.

1.2 Description of the problem

The EU and the Member States have acted in the area of personal data protection in the normative manner before, in order to achieve a level of protection that would guarantee the right to privacy of a person as a fundamental human right, as expressed in Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms of 1950.

In this respect, and as a result of the accelerated development of electronic processing of data that has been stored and used without control and without

normative arrangements in various sectors, with a great potential for abuse, the very beginning of personal data protection, according to Orešić (2017), dates back to 1981, when the Council of Europe in Strasbourg adopted the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data and the Additional Protocol to the 2001 Convention. For the purpose of raising the public awareness of the protection of personal data, the Council of Europe proclaimed the date of the adoption of the Convention — 28 January — the European Day of Personal Data Protection (known as the *Privacy Day* outside Europe).

According to Protrka (2012), the Convention was the starting point for the development of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The scope of the Directive was considerably broader than the scope of the 1981 Convention. In addition to the automated data processing files, it also included both public and private data files compiled by conventional means.

The Directive sought to achieve a high and uniform level of protection of personal data within the EU, and to balance the ongoing conflict between the individuals' interest in the protection of their privacy and the general interest in the free flow of information, while providing a certain degree of technical and legal protection of personal data as well as removing the obstacles to data exchange.

Despite all the advances in the area of personal data protection achieved by the Directive, it has not achieved a unified approach and scope of protection in Member States' national legislations, while the development of modern technology and the boom of the Internet demanded a solution that would be aligned with the contemporary trends while providing a greater degree of protection and transparency in the use of personal data.

For this reason, a new document has been drafted. After four years of preparation and discussion in the EU bodies, the Regulation was approved by the EU Parliament on 14 April 2016. The Regulation came into force 20 days after its publication in the EU Official Gazette to become directly applicable in all EU Member States two years after that date, i.e. on the date of its full application — **25 May 2018**.

The normative regulation of the protection of personal data in the Republic of Croatia rests on the provisions of the Constitution that guarantee the

right to privacy and expressly guarantee the security and confidentiality of personal data. Bet Radelić (2017) explains that this area of law is regulated by the Personal Data Protection Act, which — as the highest legal standard in the field of personal data protection in the Republic of Croatia — regulates the conditions of personal data processing, and defines the legal basis for the processing, the obligations of the controllers of personal data sets, the powers of the supervisory authorities, and sanctions for non-compliance with the legal provisions. In addition to the Personal Data Protection Act, also in force in the Republic of Croatia are the Convention on the Protection of Individuals with Regard to Automatic Processing of Personal Data and the Additional Protocol to the Convention — ratified in 2005 — and Directive 95/46/EC. Those regulations will be in force until 25 May 2018, whereupon begins the direct application of the Regulation (GDPR) in the Republic of Croatia.

1.3 Need for further monitoring of regulation

Given that the Regulation itself provides for certain areas to be defined, or regulated differently, by national legislation, the Republic of Croatia faces the need to adopt the laws that will be applied in conjunction with the Regulation. It is also necessary to follow the rulings of the European Court of Justice (ECJ) whose rulings are binding on all EU members. Therefore, the need for further monitoring of this topic and the relevant regulation continues. As the date of implementation of the Regulation draws closer, this topic will certainly elicit various interesting discussions in the public at large.

1.4 Topicality of the issue

The Regulation prescribes penalties for controllers or processors who violate the Regulation, which may reach up to 4% of annual global turnover or EUR 20 million, whichever is greater. It is the biggest penalty that can be imposed for the most serious violations, such as breaches of the basic principles, the rights of data subjects and the rules on the transfer of personal data to third countries. A lower penalty of up to 2% of annual global turnover or EUR 10 million, whichever is greater, will be applied for lesser offenses, such as missing regular records, failure to give notice of breach, or failing to carry out impact assessments.

Also provided is the liability of the controller or processor for the damage caused to the data subject by the processing of personal data in a way that is not in conformity with the Regulation. If the controller and processor are involved in the said processing, each is liable for the entire damage to the individual plaintiff.

Because of the above points, the issue is highly topical.

1.5 Purpose and goals of the study

The purpose of the short survey, which was carried out for this study on the example of Atlantic Grupa d.d., Zagreb, Miramarska 23 (hereinafter **Atlantic**), refers to the analysis of the situation regarding the collection, processing and use of personal data in the company with the aim of alignment of the Atlantic system with the provisions of the new Regulation. In accordance with the foregoing, the goals of this paper are: (I) to point out the importance of the new Regulation for all EU member states; (II) to identify the areas within the company, specifically Atlantic, that are subject to change and adaptation to the new Regulation; (III) to present the elaborate plan for the implementation of measures and actions necessary to align the company system, specifically that of Atlantic, to the new Regulation.

2. Theoretical framework

At the beginning of this section, we are trying to define the term *information*, why it is important to collect it, and what is the process of gathering information as conceived here. The shortest, but perhaps the best definition is this: "Information is the data that is managed in a way that can be used" (McKnight, 2014: 34).

If we agree that the definition is appropriate for the topic of this paper, it should be clarified how the process of information gathering or development takes place. Looking for the best description, we offer the definition that says: "The process of information development begins by gathering the facts and the statistical values we call the data. Once collected, the data is usually analyzed." (Certo, Certo, 2008: 534).

Finally, we need to explain why the information gathered is important to managers in the first place. The same authors state: "The information the managers get influences the decision making that determines activities within the organization to a large

extent, which eventually leads to the organization's success or failure." (Certo, Certo, 2008: 534).


If we consider these definitions in the current context and apply them to the topic of this paper, we must once again look at the Regulation itself and its legislative and theoretical scope. It is indisputable that the intention of the adoption of the Regulation was to regulate the area of personal data protection through legislation more effectively. The area was already regulated by the earlier Directive but it failed to achieve a uniform approach and scope of protection in the national legislations of EU members. If we add the accelerated development of modern technology and

the flourishing of the Internet and various social networks, it is obvious that a new solution had become necessary. It had to follow modern trends and provide a greater degree of protection and transparency in the use of personal data.

One has to be aware that the rapid acceleration in the development of modern technology in the area of information gathering and exchange will in a very short time require new regulation to update and modernize this matter yet again.

Before we proceed to elaborate this topic further, Figure 1 below presents a brief overview of the most important areas regulated by the new Regulation.

Figure 1 The most important areas covered by the Regulation (GDPR)

AREAS REQUIRING SPECIAL ATTENTION		
Determine what GDPR areas are the most important and have the biggest impact, and focus on those in planning		
<p>1. Awareness Ensure that the key stakeholders in the organization are informed about the GDPR and novelties it brings</p>	<p>12. Internationalization Establish an oversight body, if your organization is doing business in more than one EU member state (i.e. if you conduct cross-border processing).</p>	<p>11. Data protection controllers If you are under obligation, determine a person who will assume responsibility for compliance with the GDPR, and define the structure and management method.</p>
<p>2. Information in your possession Document what personal data you possess, where it came from, where you are using it and with whom you are sharing it.</p>		<p>10. Data protection by design and data protection impact assessment Verify whether it is necessary and ensure the processes and procedures that enable data protection by design, and based on the data protection impact assessment.</p>
<p>3. Communicating data on privacy Review the current privacy statements and ensure making the necessary changes within the appropriate time frames, using accurate and clear messages.</p>		<p>9. Data theft Ensure the appropriate procedures for discovering, reporting and analysis of personal data theft.</p>
<p>4. Rights of natural persons Implement the processes that will ensure respecting the rights of natural persons (e.g. data deletion, submitting data in the electronic form, etc.)</p>		<p>8. Children Ensure verification and control of the age group of individuals and obtain consent of the parents or legal guardians for any activity in data processing.</p>
<p>5. Requests for access to data Implement the procedures that will satisfy the new additional requests within the new time frames.</p>		<p>6. Legal basis for personal data processing Establish the lawful basis for data processing in GDPR, document and update your privacy statement in order to elaborate it.</p>

Source: UMiUM d.o.o., available at: www.umium.hr (Accessed on: November 20, 2017)

For better understanding of the provisions of the Regulation, here are the definitions of certain key terms as specified therein:

- **personal data** means any information relating to an identified or identifiable natural person ('data subject'); 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;
- **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;
- **controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;
- **processor** means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;
- **consent** of the data subject means 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.

In order to strengthen the area of protection of personal data and make an additional step in the direction of greater protection of citizens, the Regulation has strengthened the rights of citizens as *data subjects* — persons whose personal data are collected and processed — in comparison to the previous reg-

ulations, and introduced additional rights. This is, inter alia, particularly notable in the following areas:

- consent - it should be given actively by the data subject, and with a clear act of confirmation that expresses their voluntary and unambiguous agreement with the processing of their data. Such consent must be given for specific purposes and to the specified controller (express oral or written statement, field marking on the web site...), which means that the silence of a data subject, a pre-selected field with a check mark, or a lack of activity, are not considered to constitute consent;
- right of access (information) - the data subject has the right to know which of their data is being processed, the purpose of processing, to whom the data will be disclosed, the period of data storage etc.;
- right to limit processing / to erasure / to be forgotten - the data subject has the right to demand the termination of use and/or deletion of their data in whole or in the part they no longer agree to be processed, or to exclude the use of that data or its part for any particular purpose;
- right to object - the data subject has the right to address the controller with an objection regarding the manner and purpose of use of their data;
- right to portability of data - means the right of the data subject to obtain all their data in machine-readable format at any time and to easily transfer it to a new controller or processor;
- right to communication of a personal data breach.

Particular attention must be paid to the protection of personal data of children. The Regulation stipulates that consent of parents of children under the age of 16 is required for *online* services, while a member state may determine a lower age limit, but not lower than 13 years. In this respect, a controller must make every reasonable effort to check whether the parent has actually given consent.

Furthermore, the Regulation establishes exclusive conditions under which special categories of personal data may be processed — namely sensitive data (racial or ethnic origin, political opinion, religion or beliefs, trade union membership, health status, sexual life and orientation, genetic and biometric data)

— in which case explicit consent by the data subject is required if processing is necessary for the protection of their interests or for the fulfillment of special obligations or rights of the controller. In such cases, the processing must be specifically marked and protected, and subject to special measures of technical protection. If one or more of the listed conditions are not met, the Regulation expressly prohibits the processing of such personal data.

The question of who is actually bound by the Regulation is also important. The Regulation, in accordance with the defined territorial scope of application referred to in Article 3 is binding for:

- all controllers and processors established in the EU member states, regardless of whether the data processing takes place in or outside the EU, but also for
- controllers and processors not established in the EU if they carry out activities that include collection or processing of personal data of EU citizens (related to the offering of products or services, or to the monitoring of their activities and behavior within the EU).

The defined and strengthened rights of the data subject necessarily impose certain very important obligations on the controller and processor in terms of the use and processing of the subject's personal data.

The controller, as the operator who determines the purpose and method of processing of personal data, must:

- give the data subject full information on the purpose for which their data is collected, in a clear, intelligible and easily accessible form, using clear and plain language;
- be able to prove that the data subject has given consent for processing of their personal data;
- limit the collection of personal data solely to such data as are necessary to achieve the purpose of processing;
- ensure the lawfulness of processing (consent, performance of a contract to which the data subject is party, compliance with the legal obligations of the controller, protection of the key interests of the data subject, issues of public interest or execution of authority of the controller of a data set). Ensuring the lawfulness of processing is particularly important when the processing is carried out

for the purposes of legitimate interests of the controller, in cases where the interests of the data subject are greater, or when the interests of the data subject require the protection of personal data, especially those of children.

In addition to the obligations of the controller, the processor must:

- ensure the exercise of the rights of the data subject (information, limitation of processing / erasure / right to be forgotten, portability, notification of breach, protection of data on children and sensitive data);
- carry out appropriate technical and organizational measures in order to identify the personal data necessary for a specific purpose, define the scope of processing, the storage period, and limit their availability only to a certain necessary circle of persons;
- carry out the appropriate technical and organizational measures to ensure maximum security of personal data - also ensuring that the collected data are not altered and that they are *encrypted* and that an appropriate encryption key management process has been established. Security policies and controls must be introduced which must be able to prove that the data have not been altered, damaged, destroyed, lost, or illegally used;
- perform any such task upon request of the data subject in the shortest possible time, not longer than 30 days, and prove on request that the requested actions have been performed. The proof is a certificate of the work performed issued to the data subject. In the event of doubt and the request of the supervisory authority, the fact that the said actions have actually been carried out must be proved directly.

The Regulation also prescribes the obligation to keep records on personal data processing activities; the records must be kept by:

- controller employing more than 250 employees or
- controller whose processing is a probable risk to the rights and freedoms of the data subject (but only if the processing is not occasional), or
- controller handling special categories of personal data or data on criminal offences or

convictions; they shall, at the request of the supervising body, keep and submit records of the processing activities, which contain all the essential processing elements, such as the identity of the controller with contact information, the purpose of processing, the description of the data subject and the personal data, recipients of the data, data transfers to third countries, storage periods, etc.

The Regulation introduces the obligation to include data protection measures from the beginning of design of a system, rather than being added subsequently. The controller of the data set must follow organizational and technical measures to comply with the requirements of the Regulation and protect the rights and privacy of the data subject (*Privacy by Design*).

Given that the Data Protection Act is based on the consideration of risk, it is the responsibility of the controller to carry out an assessment of the effect of processing in situations where a certain kind of processing is likely to cause high risk for the rights and freedoms of the data subject; the Regulation also determines when such an assessment is mandatory — e.g. in systematic and comprehensive assessment of personal aspects of data subjects based on automated processing (profiling), extensive processing of special categories of personal data, etc. Such an impact assessment should include a description of processing procedures and their purpose, the assessment of necessity and proportionality, the risk assessment, as well as a description of measures taken to reduce the risk of processing. If the assessment of the effect on data protection has demonstrated that the processing would lead to high risk if the controller does not take measures to mitigate it, the controller is obliged to contact the supervisory body and, *inter alia*, provide information on the purpose and methods of processing, measures of protection, the impact assessment conducted, etc.

The Regulation provides an answer to a very important question, especially in Atlantic — the disclosure of personal data outside the EU. Personal data may be transferred from the EU to a third country only in accordance with the provisions of the Regulation. Personal data may be transferred to third countries for which the European Commission has issued a decision on adequacy (transfer based on a decision on adequacy) based on the assessment of the rule of law, respect for human rights, relevant legislation, the existence of an independent super-

visory body and the international obligations of the third country. In the event of the need for transfer of personal data to third countries which do not provide an adequate level of protection, additional protective measures, provided for in the Regulation, shall be adopted to provide a high level of protection of personal data. Instruments that enable personal data to be transferred to such third countries are exhaustively listed in the Regulation, e.g. binding corporate rules, standard contractual clauses, codes of conduct, etc.; also listed are exceptions relating to non-regular data transfer.

The complexity and importance of this issue in almost all companies that are engaged in the collection, processing and use of personal data in their business also implies the need to appoint officers who will deal solely with that matter. Thus, Article 37 of the Regulation lays down the possibility for each controller or processor to designate a personal data protection officer (*Data Protection Officer - DPO*), for these purposes. It also prescribes the mandatory appointment in the following cases:

1. public authorities or public bodies;
2. organizations that are involved in systematic monitoring on a large scale;
3. organizations dealing with extensive processing of personal information of sensitive nature and personal data on criminal cases;
4. cases where legal acts of an EU Member State or EU law impose the obligation to appoint a personal data protection officer.

The Regulation also allows a group of entrepreneurs to appoint a single data protection officer, who must then be easily accessible from each business headquarters. According to the current Croatian legislation, the controller of a personal data set that employs fewer than 20 workers may appoint a personal data protection officer, while a controller with more than 20 employees is required to do so.

Finally, in the event of a personal data breach that is likely to cause a risk to an individual's rights and freedoms, the controller is obliged to notify the supervisory authority (in the Republic of Croatia it is the Croatian Personal Data Protection Agency - AZOP)²

within 72 hours of the discovery of the breach, and notify the data subjects themselves without delay.

The processor is obliged to inform the controller about the incident without unnecessary delay.

3. Methodology of work

This paper covers theoretical considerations and a shortened form of secondary research, i.e. it uses the data from an analysis carried out at Atlantic. Therefore, the scientific methods used in this paper are defined by the characteristic of the individual parts of the research. In the preparation of the paper, the following scientific methods have been used in the appropriate combinations: methods of analysis and synthesis, the classification method, the description method and the compilation method. The latter was used carefully, with care taken over the faithful quoting and citing of the sources.

The previously defined problems and the set of research goals have yielded the following hypothesis, tested by the short research and analysis given in this paper:

HYPOTHESIS (H):

It is possible to avoid the burden of extremely high fines for non-compliance with the provisions of the Regulation by applying a structured and methodologically sound procedure, which will maximize the degree of compliance of all members of Atlantic Grupa d.d. with the legal provisions of the Regulation (GDPR).

4. Description of research and research results

4.1 The aim of research

The study used as secondary research in this paper was carried out on the example of Atlantic Grupa d.d., Zagreb. The competent authorities in the company have made the decision to establish the procedure of alignment with the provisions of the Regulation through a project approach.

This approach seemed necessary for many reasons. Primarily, the company involved is a business system with a large number of separate legal entities, with establishments and activities in several countries within and outside EU, conjoined by synergies and organizational processes.

Furthermore, companies within Atlantic carry out business activities in different fields, from the production of various types of food products (coffee,

soft drinks and bottled water, biscuits and chocolates, vitamin drinks...), food supplements, food intended for athletes, over the group's own chain of pharmacies and specialized stores, to the distribution of a wide range of own and principal brands. Finally, within Atlantic, a whole range of personal data sets is kept by individual companies (video surveillance, employee and working time records, members of *loyalty* clubs, participants of prize games, buyers ...).

The following information is a good illustration of the volume of personal information kept by companies within Atlantic:

- companies within the group employ 5,500 people;
- employee record of each employed person includes approx. 40 items of personal data, which means nearly 220,000 personal data items on employees alone;
- companies operating in the Atlantic system are collecting and have collected personal information on other natural persons through activities like prize games, *loyalty* programs, job offers, health clubs, convenience programs and discounts, etc. ... which amounts to the records containing ca. 700,000 additional personal data items.

As a conclusion, the fact is that Atlantic business system keeps almost 1,000,000 personal data items on natural persons.

4.2 Study findings

Before a structured approach to harmonization with the provisions of the Regulation was initiated, areas in which the existing situation needed to be established had been identified, and further steps and necessary measures defined.

Within Atlantic, four key areas have been identified: (I) **personal information** and all the ways in which it is collected, (II) **roles and responsibilities** in data management within the business system, (III) analysis of existing **policies and procedures**, and (IV) levels of **technical control**. In Figure 2 below, the project approach of alignment with the Regulation is being systematized and described.

Figure 2 Graphic presentation of the project approach of alignment with the Regulation

Technical controls	<ul style="list-style-type: none"> * Do our IT systems support the GDPR requirements? * What to do with them?
Policies and procedures	<ul style="list-style-type: none"> * Is personal data management integrated into the business processes? * Do we have procedures in place regarding the treatment of personal data?
Roles and responsibilities	<ul style="list-style-type: none"> * Who is responsible for personal data? * Do we have the appropriate roles and responsibilities?
Personal data	<ul style="list-style-type: none"> * What kind of data do we have? * How do we use it? * Where is it?

Source: Created by the authors

At the same time, when defining the project approach, the goals that need to be achieved through the individual phases of the project were identified:

- recording/mapping of personal data and databases;
- identifying and, if necessary, defining the legal basis for data collection and processing;
- development of Rules of Organization at the level of the Atlantic business system as the umbrella solution for all companies within the group;
- preparation of the basis for risk assessment and its implementation;
- defining the organizational and technical measures to ensure adequate measures of personal data protection;
- appointment of personal data protection officers;
- appointment of persons responsible for the protection of personal data for each process;
- developing a culture of personal data protection at all levels, and
- conducting the education of employees.

The project itself is defined through the implementation of certain phases. The implementation phases have been summarized and further described in Figure 3 below.

Figure 3 The graphic presentation of phases in the project of alignment with the Regulation

PROCESS OF ALIGNMENT WITH THE GDPR

<p>1. DEFINING THE AREA OF DATA PROCESSING</p> <p>Identify and understand where, why and how personal data is processed.</p>	<p>2. RISK ASSESSMENT</p> <ul style="list-style-type: none"> * Identify potential threats; * Determine the remaining risk; * Identify areas that are key to DPIA 	<p>3. DATA PROTECTION IMPACT ASSESSMENT</p> <ul style="list-style-type: none"> * Determine specific threats related to new technologies; * Analyze high-risk areas.
<p>4. GAP ANALYSIS</p> <ul style="list-style-type: none"> * Identify technical measures; * Identify organizational measures; * Asses efficiency of the measures in order to reduce the risks; * Determine the remaining risk – Is it acceptable or not? 	<p>5. ACTION PLAN</p> <ul style="list-style-type: none"> * Identify new or potential organizational and technical measures in order to reduce the risk to an acceptable level; * Define priorities and an action plan in order for the measures to be implemented. 	
<p>6. ALIGNED PRIVACY PROGRAM</p> <ul style="list-style-type: none"> * Define privacy, policies and procedures; * Implementation of technical measures; * Informing and training the staff involved in data processing area. 	<p>7. MONITORING PRIVACY ALIGNMENT</p> <ul style="list-style-type: none"> * Set up the alarms and warning systems; * Examine efficiency of the implemented measures; * Define mechanisms for identifying new risks in the privacy area. 	

Source: UMiUM d.o.o., available at: www.umium.hr (Accessed on: November 20, 2017)

The research included business areas in Atlantic where personal data processing in a significant volume had been identified:

1. Human Resources
2. IT
3. Sales
4. Pharmaceuticals
5. Marketing
6. Legal Affairs
7. Safety at work.

All personal data sets were identified in all of the above organizational units and the following data was processed within the risk assessment:

- the name of the personal data set;

- the type of data collected within the set (name, last name, year of birth, email address etc.);
- the legal basis for collection of personal data (consent, legal basis);
- the data storage method (in the IT system as a database, written documents, etc.);
- identification of the IT platform where data is stored, or the physical locations where documentation is kept;
- data on the person responsible for the personal data set.

Furthermore, a transparent methodology for risk assessment regarding the collected and identified (mapped) data was established as well as for determining the need for further activities, with the aim of their elimination or mitigation. An overview of the risk assessment regarding the collected data is given in Table 1 below.

Table 1 Risk assessment based on collected data

Impact	High	4	8	12	16
	Medium high	3	6	9	12
	Medium low	2	4	6	8
	Low	1	2	3	4
		Low	Medium low	Medium high	High
	Probability				

Source: Created by the authors

Applying the methodology defined in this way, a risk rating for each individual set of personal data was established, together with the measures, deadlines and persons responsible for corrections. Based

on that rating, a comprehensive structural risk map with the measures, deadlines and responsible persons is being created. The example of such structural risk map is given in Table 2 below.

Table 2 Example of a structural risk map

Business area	Name of the risk	Description of the risk	Threat	Impact	Probability	Total Risk	Responsibility	Treating the risk	Treating the risk & action plan (description of controls implemented)	Established deadline	
Contact center	Limiting access to Sharepoint site for contact center, donations, and prize games	Access to the Sharepoint site is enabled for all employees who have an active AD account, which is not in compliance with the "need to know" principle	Leakage of personal data, penalty from the regulator	R,F	4	3	12	N.N.	Risk reduction	Restrict access rights to Sharepoint in accordance with the "need to know" principle	01/31/2018
Pharmacia	Unauthorized access to the Loyalty Web application	Unauthorized hacker break-in into Dietpharm and Pharmacy Loyalty Web Applications	Hacker attack	O,R,F	4	3	12	N.N.	Risk reduction	Conducting detailed penetration testing (involves the implementation of measures to reduce the observed defects during the test itself) at least once a year	02/28/2018

Source: Created by the authors

To summarize, the main risks to the protection of personal data in the Atlantic business system and, in parallel, measures for their removal/mitigation, have been identified as:

- limitation of access to the *Sharepoint* site by the contact center, donations and prize games;
- more detailed recording of activities of IT systems that contain personal user information;
- unauthorized access to the *Loyalty* web application;
- management of user consent;
- more advanced control of access to *Success Factors* and *Digital Ninja*;
- identifying real needs and limiting the access rights to data sets;
- data on users of personal computers;
- agreement at the level of Atlantic on processing of personal data within the entire group;
- education program on personal data protection for Atlantic employees;
- rules for protection of personal data.

Finally, it should be noted that, prior to the implementation of the project of alignment with the Regulation, and based on the explained methodology for risk assessment regarding the collected and identified (mapped) data, the final risk assessment in both identified areas has been set on the level of 12. The expected outcome of the risk assessment after the full implementation of the project of alignment with the Regulation is targeted to end at the level of 4. The risk estimated at the level of 4 would be a result of the medium low probability (2) and medium low impact (2). It is therefore self-explanatory that the implementation of the structured and in-house designed project of alignment with the Regulation should be considered as successful, workable and sustainable.

5. Discussion

As outlined in the previous sections of this paper, the new Regulation provides very clear and precise guidelines for accessing, recording, using, and managing the collected personal data. All controllers and processors must adapt to the guidelines and

rules and organize their processes and systems in the direction of maximum protection and transparency in the use and processing of personal data.

Systems and processes must be set up and organized so as to minimize the possibility of abuse of personal data, or breach by third parties into IT and other databases containing personal data. Furthermore, the structure of accountability, the right of access to and use of personal data must be clearly set and defined within each business entity. Quality education of all persons within the business entity who have access to, and use of, personal data of the data subjects, is very important, so that they are familiar with, and can act within, the legal provisions and the internal rules in a consistent manner.

It is also important to define the relationship with the contractual partners (processors) to whom the controller provides the collected personal data for processing, with a special emphasis on the definition of the obligations regarding the protection of the data and the way the data is used by the processors.

Also, it is sound policy to control any system from time to time, either through periodic internal control, or occasionally by external experts.

It is also very important to have an open and earnest relationship with the supervisory body and the data subjects themselves, to act on their requests within the legal deadlines, and to fulfill the obligation to notify the supervisory body, but also the data subject, in the event of a breach of the data subject's personal data.

Although the structured and in-house designed project of alignment with the Regulation would lower the risk assessment level from 12 to 4, and despite all the measures taken and the maximum of transparency in the system, the possibility of a breach or misuse in this area is always possible. With that in mind, the fact that an appropriate personal data protection and management system is in place within the business entity, and that its consistent application can be proved, will certainly be a good mitigating circumstance for the business entity involved. This is an investment that every business entity needs to make — to at least reduce the threat of penalty, if not to eliminate it altogether.

6. Conclusion

The Regulation represents a very significant advance in the area of personal data protection - from its modernization and upgrading, providing all EU citizens with a uniform right to protect their personal data, to the enabling of much greater control over the processing of such data, in particular in today's digital environment abundant with new technologies.

It introduces an additional dimension to the area of personal data protection, which was standardized to a notable degree even before the adoption of this Regulation — one aimed at raising the awareness of the necessity of respect and implementation of the prescribed measures. Namely, the penalties for the perpetrators of breaches of security are quite severe. For serious violations they amount to up to EUR 20 million, or 4% of the total annual (global) turnover. Such significant penalties will certainly provide additional motivation for all controllers and processors to achieve the maximum possible compliance with the provisions of the Regulation, and its consistent implementation.

Another important aspect is the great media attention raised by the novelty of the Regulation. It will certainly help increase the awareness of the data subjects themselves of their rights and of the pos-

sibility of control over the management of their personal data.

Based on everything stated in this paper, and in particular on the basis of:

- a very detailed theoretical elaboration of the issue of protection of individuals with regard to the processing of personal data and the free movement of such data,
- a transparent presentation of the current state of affairs in this area on the example of Atlantic, together with the targeted lowering of the risk assessment level from 12 to 4 and
- a description of a pragmatic, operational and feasible project plan that defines the areas, activities, risks, deadlines and persons responsible for the implementation of a comprehensive alignment of the Atlantic's rules with the provisions of the Regulation.

It can be concluded that **it is possible to avoid the burden of extremely high fines for non-compliance with the provisions of the Regulation by applying a structured and methodologically sound procedure that will maximize the degree of compliance of all members of Atlantic Grupa d.d. with the legal provisions of the Regulation (GDPR).**

REFERENCES

1. Bet Radelić, B. (2017). "Zaštita osobnih podataka u radnim odnosima", in Bet Radelić, B. et al. (Eds.), *Zaštita osobnih podataka i granice zaštite privatnosti radnika*, Radno pravo, Zagreb, pp. 7-8.
2. Certo, S. C., Certo, S. T. (2008). *Moderni menadžment*. Zagreb: MATE.
3. McKnight, W. (2014). *Information Management: Strategies for Gaining a Competitive Advantage with Data*. Waltham: Elsevier, Inc.
4. Orešić, H. (2017). "Konvencija 108 za zaštitu osoba glede automatizirane obrade osobnih podataka", in Bet Radelić, B. et al. (Eds.), *Zaštita osobnih podataka i granice zaštite privatnosti radnika*, Radno pravo, Zagreb, pp. 27-28.
5. Protrka, N., (2013). "Normativna uređenost zaštite podataka u Republici Hrvatskoj", *Policajska sigurnost*, Zagreb, Vol. 22, No. 4, pp. 509-510.

LIST OF ABBREVIATIONS

RH	-	Republic of Croatia
EU	-	European Union
GDPR	-	General Data Protection Regulation
AZOP	-	Personal Data Protection Agency
d.d.	-	Joint stock company

(ENDNOTES)

- 1 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), available at: <http://eur-lex.europa.eu/legal-content/HR/TXT/PDF/?uri=CELEX:32016R0679&from=EN> (Accessed on: March 1, 2018)
- 2 Personal Data Protection Agency — AZOP (2017), "Guide to the General Data Protection Regulation", available at: <http://azop.hr/> (Accessed on: March 8, 2018)

Krešimir Starčević
Boris Crnković
Jerko Glavaš

IMPLEMENTACIJA OPĆE UREDBE O ZAŠTITI PODATAKA U TRGOVAČKIM DRUŠTVIMA U REPUBLICI HRVATSKOJ

SAŽETAK

U ovom radu obrađuje se aktualna tema zaštite pojedinaca u vezi s obradom njihovih osobnih podataka i slobodnom kretanju takvih podataka. Kako ovu materiju uređuje i zakonodavstvo Europske unije, u radu se opisuje i analizira doseg, implikacije te metode i alati za primjenu nove uredbe Europske unije usvojene 27. travnja 2016. u Parlamentu Vijeća Europske unije. Radi se o Općoj uredbi o zaštiti podataka, odnosno preciznije o Uredbi o zaštiti pojedinaca u vezi s obradom osobnih podataka i slobodnom kretanju takvih podataka (2016/679). Izvorni naziv ove uredbe na engleskom jeziku je *General Data Protection Regulation* (GDPR) pa se u svakodnevnom rječniku među poduzećima i gospodarstvenicima, ali i u ovom radu koristi još i naziv GDPR. Nadalje, u radu se analizira provedeno istraživanje o zatečenom stanju i načinu na koji se obrađuju i koriste svi prikupljeni osobni podatci svih dionika toga procesa u sustavu trgovačkoga društva Atlantic Grupa d.d., Zagreb. Osim toga, opisuje se usuglašeni projekt strukturiranog i metodološki ispravnog postupka primjene odredaba nove Uredbe, a u svrhu najvišeg mogućeg stupnja usklađenja obveza svih članica Atlantic Grupe d. d. s pravnom regulativom Uredbe (GDPR). Na kraju, obrazlaže se osnovni cilj opisanog projekta, izbjegavanje situacija koje bi dovele do naplate izrazito visokih propisanih novčanih kazni za nepoštivanje odredaba Uredbe.

Ključne riječi: zaštita pojedinaca i njihovih osobnih podataka, Opća uredba o zaštiti podataka (GDPR), Atlantic Grupa d. d.