

Ana Tokhadze*

The Interdisciplinary Analysis of Institutional Role of Data Protection Officer in the System of Corporate Governance

The reinforcement of legal regulation of personal data protection was conditioned by the increasing tendency towards systemic and large-scale processing of personal data by large companies, especially in terms of protecting the rights and interests of data subjects. The institute of data protection officer, which has not yet been reflected in the Georgian law, represents a kind of mechanism ensuring the proportionality between the legality of data processing, corporation and interests of data subject. The paper is focused on the interdisciplinary insight of this institute in the perspective of corporate law, on the one hand, and on the other hand, the law on personal data protection, so as to determine its institutional function in the organizational structure of the legal entity of private law.

Keywords: Corporative governance, data protection, data protection officer (DPO), General Data Protection Regulation (GDPR).

1. Introduction

The positive legal provisions continue their self-reliant existence overtime through the power of law-making transformation. The rationale of discussing the harmonization between Georgian and European law probably should begin with seeking the answer to the following question: Does law transform society, or conversely, will it be transformed by society? Law, as a system evolving, creates the general welfare of society by defining the binding provisions for behavior¹. However, evidently, the emergence of free market economy was accompanied by the self-regulation of industries and economic actors, and after de-codification it was further followed by the arbitrary

* Ph.D. student and the Teaching Assistant in the field of Private Law of the Faculty of Law at Ivane Javakhishvili Tbilisi State University; Head of the International Relations, Analytics and Strategic Development Department of the Personal Data Protection Service of Georgia.

¹ Bentham J., Of Laws in General, Hart H. L. A. (ed.), 1970, 31-33.

regulation of social-economic relations², which was implemented more spontaneously due to the “principle of demand and supply” to maintain competitiveness, on the one hand, and by the pressure of social responsibility, on the other hand³. This is how the voluntary accountability of corporations to civil society was formed.

Giving considerations to current trends, in terms of the scale and impact of economic activities of mega-corporations the attention of a legislator is focused on the legal status of “interested parties” (“stakeholders”)⁴, including consumers, and most importantly, based on the interest of presented study, on the legal status of data subjects. The rigor of legal regulation is evaluated and shaped by the degree of impact made by the entrepreneurial activities of corporations upon the interests of “stakeholders”. Thus, it is clear, why the corporate law, on the one hand and the law on personal data protection, on the other hand, establish certain organizational-legal obligations through imperative regulation. The integration of the institute of data protection officer into the system of corporative governance belongs exactly to such requirements.

The data protection officer, in its corporative-legal sense, represents the integral element of intra-organizational structure, and in terms of the law on personal data protection it is deemed to be a kind of guarantor for the lawful processing of data and protecting the rights of data subject. The present study aims to establish the truth of the following thesis: the data protection officer ensures the reasonable proportionality between the interests and rights of corporations – as a legal entity and data subject.

The interdisciplinary nature of the study is the outcome of a kind of attempt to interrelate the corporate law with that of personal data protection. And as “[...] all the cognition is explanation”⁵, this paper is descriptive in nature, so as to convey the conceptual categories of the issue and field to be studied; the analytical-synthetic method is applied to formulate the intermediate results in the unified system and highlight their logical relationship with the objective of research.

² *Magnier V.*, Comparative Corporate Governance, Legal Perspectives, 2017, 1-4. This purpose is expressed by the “Soft regulation” of corporate governance, which was submitted to European Commission by Prof. Paul Davis in 1997 with the idea that, the commission should define the standard of supranational corporate governance, and each member state should be guided by the principle “comply or explain” within the national law, see: *Johnson A.*, Soft Law, in: EC Regulation of Corporate Governance, UK, 2009, 343-347.

³ *Picciotto S.*, Regulating Global Corporate Capitalism, 2011, 61-65, 193-200.

⁴ In the scientific literature the terminological definition of “Stakeholder” allows to imply a data subject too in it, as it includes any such person whose interest can be influenced by the activity of corporation. See *Makharoblishvili G.*, General Analysis of Corporate Governance, 2015, 313-317 [in Georgian].

⁵ *Jasper K.*, Introduction to Philosophy, *Gorgisheli V.* (trans.), 2019, 73 [in Georgian].

2. Focus on the Personal Data Protection as a Modern Model of Corporate Governance

According to the position expressed in literature, the era of emergence of intangible economy conditioned the existence of capitalism without capital⁶. Personal data represents exactly such intangible capital of modern type. The obligation of lawful data processing requires the corporation to take the proper technical and organizational measures, shape the appropriate internal organizational structure as well as to introduce the management system. The corporate governance in its essence is the kind of system of separation and management of property (*share capital invested in entrepreneurial society*) and control (*organizational body authorized to manage the aggregate capital*), which envisages the legal interests of shareholders and the interested parties.⁷ The specified governance system can be implemented according to the one-tier and two-tier model/scheme from the organizational viewpoint.⁸

The system of corporate governance proposes several types of models expressing its main reference point (e.g., there exists a managerial model, the model focused on maximization of the shareholders' wealth, also, the model focused on the interests of employees and the interested parties)⁹. In the narrow sense, the difference between the models is conditioned by the management policy and strategy of a corporation, and, more generally, - by the environmental economic and legal factors within which the corporation operates.¹⁰ Accordingly, the management model of each corporation varies in the area of entrepreneurial activities and managerial policy. The implementation of governance with the focus on personal data protection can be assessed as one of the varieties of above models. Such model is especially noteworthy for the economic actors processing a large volume of personal data as well as whose entrepreneurial activities considerably effects the interests of data subjects.

One of the fundamental principles¹¹ of corporate governance represents openness and transparency which envisage the timely disclosure of information relating to financial status, managerial structure, governance and management of the corporation. It is worth noting, that one of the principles of data processing ensures the transparency, which obligates the controller

⁶ See, *Haskel J., Westlake S., Capitalism without Capital: The Rise of the Intangible Economy*, 2018, 3-10.

⁷ *Burduli I., Makharoblishvili G., Tokhadze A., Zubitashvili N., Aladashvili G., Maghradze G., Egnatashvili D., Corporate Law*, 2022, 634-638 [in Georgian].

⁸ The mentioned is based on Charter autonomy in some cases and in some cases – legislative requirement, see Arts. 124 and 182, Law of Georgia on "Entrepreneurs", 875-VRS-XMP, 02/08/2021.

⁹ *Tokhadze A., Enhancement of Corporate Social Responsibility – An Analysis from the Perspective of Economic and Sectoral Cooperation under the Three Association Agreements*, in: *Legal Aspects of the EU Association Agreements with Georgia, Moldova and Ukraine in the Context of the EU Eastern Partnership Initiative*, *Trunk A., Panych N., Rieckhof S. (eds.)*, 2017, 104-106.

¹⁰ *Makharoblishvili G., general analysis of Corporate Governance*, 2015, 161, 162-163 [in Georgian].

¹¹ *G20/OECD, Principles of Corporate Governance*, 2015.

to provide the data subjects with the straightforward access to any of the information relating to data processing.¹² It should be noted that the legislation of the European Union¹³ establishes the duty of accountability and additional obligations for a data controller and processor, so as to ensure effective protection of personal data.¹⁴ One of the forms of such measures is deemed to be the institute of data protection officer.¹⁵

Thus, the data protection-oriented model of corporate governance is shaped by the sphere of entrepreneurial activities of business entity and the intensity and volume of personal data processing therein. On the other hand, the legitimate interests of data subject as a “stakeholder” is taken into account exactly in the entrails of such a model of corporate governance. Correspondingly, the purpose of data protection-oriented model of corporate governance is: a) the full compliance of the corporation, as a data controller or processor, with the legislative regulation of data protection; b) the protection of the rights of a data subject as a “stakeholder”.

3. Data Protection Officer as the Element of Model for Personal Data Protection-oriented Corporate Governance

The institute of Data Protection Officer represents one of, but not a single, elements of data protection-oriented model of corporate governance. The evaluation of the risks of impact of data protection (“Data Protection Impact Assessment”) and the existence of its internal policy is a kind of expression of accountability. Occasioned by the format of this work, it is impossible to review all the legal aspects of the institute of officer, so, this chapter is focused on the specific key features characterizing the institute.

3.1. Functional Separation of Data Protection Officer and Corporate Compliance Officer

The Data Protection Officer is a qualified expert of data protection whose function is to hold consultations with the corporate management on ensuring the compliance with data protection

¹² Preamble, §39, 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), OJ L 119, 4/5/2016, 1–88. Art. 4, para. 1, sub-para. “a”, Law of Georgia on “Personal Data Protection”, Art. 15, 5669-rs, 28/12/2011.

¹³ §84, Article 10, *Council of Europe*, Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+; CM/Inf(2018)15-final), 18/05/2018.

¹⁴ *Council of Europe*, Explanatory Report, Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+; CM/Inf(2018)15-final), 18/05/2018, Art. 10.

¹⁵ *Ibid*, § 87.

regulations.¹⁶ Unlike the corporate executives, a Data Protection Officer does not represent the fiduciary¹⁷ of the business entity (*in other words, a representative implementing the best interests of corporation*). He/she is not a corporate compliance officer, either. However, with the aim of drawing a parallel, the general comparison of functions of the two institutions can be made.

Corporate compliance is the “firstborn” of the Anglo-American legal family. It combines a number of measures, through which the activities of corporate insiders (managers, employees) are conducted in accordance with the legal norms.¹⁸ Exactly the corporate compliance officer is delegated to determine the legal or economic challenges and objectives. At first glance, their functions seem to overlap, however, the institutional role of the compliance officer and the Data Protection Officer should not be confused. In this respect, the interest is evinced in the fact that due to the conflict of interest Belgian data protection authority penalized the controller €50,000, because the person appointed as a Data Protection Officer at the same time held the position of the head of corporate compliance service, money laundering reporting officer.¹⁹

In addition, it is essential that the Data Protection Officer has the appropriate qualification, the expertise in data protection and the ability to independently carry out the duties assigned to him/her.²⁰ Therefore, the principle of competence applies to him/her. The Data Protection Officer reports directly to the top-management of data controller or processor²¹ that implies even the submission of periodic reports as a practical expression of the principle of accountability. In order to ensure the independence of the officer, no instructions or tasks may be given to him/her by the data controller or processor.²² Conversely, the function of corporate compliance officer can be implemented in any organizational unit of a corporation. Moreover, as opposed to the corporate compliance officer, the Data Protection Officer has an active relationship with external actors as well (e.g., data subject, data protection supervisory

¹⁶ *The European Union Agency for Fundamental Rights and the Council of Europe*, Handbook on European Data Protection Law, 2018, 198.

¹⁷ Fiduciary duty is imposed on the management members of the corporation, who take entrepreneurial decisions on the basis of the best interests of society. *Schneeman A.*, Law of Corporations and Other Business Organizations, 2010, 39.

¹⁸ *Ibid.*, 363.

¹⁹ Autorité de protection des données, Dossiernummer: DOS-2019-04309, 2020, <<https://cedpo.eu/dpo-case-law/>> [20.01.2023].

²⁰ *Voigt P., Bussche A.*, The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 56-57.

²¹ Art. 38(3), 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), OJ L 119, 4/5/2016, 1–88.

²² *Voigt P., Bussche A.*, The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 59.

authority). Accordingly, it is necessary to disclose his/her contact information and inform the data protection supervisory authority of the appointment of data protection officer.²³

The function of Data Protection Officer encompasses three segments: information, cooperation and supervisory obligations²⁴. The first implies holding the proper consultations with data controller/processor on data processing; the second intends the active communication and cooperation with the data protection supervisory authority; and the third one means the supervision of compliance with the legislation regulating data protection.²⁵ In order to perform these functions properly, the officer is authorized to carry out inspections, have access to personal data, familiarize himself/herself with the statements of data subjects and for this purpose independently take any actions within the standard of ethics.²⁶

3.2. Prerequisites for the Appointment of a Data Protection Officer

The EU General Data Protection Regulation envisages the obligation to appoint a Data Protection Officer in three separate cases.²⁷ The existence of officer's institute in the business entity operating in the private sector is linked to that type of core activities of the processor or controller, when the operations implemented in its scopes intend the extensive regular, systematic monitoring of the subject's data or when their main activity is connected to the large-scale processing²⁸ of special categories of data. In the said definition, the "principal activity" of the controller or processor and the "qualitative" and "quantitative" indicators of the operations carried out within it are noteworthy. Since, in a corporate law sense, the main entrepreneurial and ancillary economic activities performed within the scopes of general legal capacity of private legal entities are different concepts²⁹, the salient point to appoint the officer is that the personal data should be processed for the purpose of gaining profit in an organized, reasonable, repeated manner³⁰ and as part of its core activities performed independently by the entrepreneurial

²³ *Article 29 Data Protection Working Group*, Guidelines on Data Protection Officers (DPOs), 16/EN, WP 243 rev.01, 2016, 10.

²⁴ *Voigt P., Bussche A.*, The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 60.

²⁵ *Ibid.*

²⁶ *Data Protection Officer*, Professional Standards for Data Protection Officers of the EU Institutions and Bodies Working under Regulation (EC) 45/2011, 2010, 12-13.

²⁷ Art.37, 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), OJ L 119, 4/5/2016, 1–88.

²⁸ *Ibid.*, Art. 37(1).

²⁹ *Burduli I., Makharoblishvili G., Tokhadze A., Zubitashvili N., Aladashvili G., Maghradze G., Egnatashvili D.*, Corporate Law, 2022, 634-638 [in Georgian].

³⁰ Art.2, para.2, The Law of Georgia on "Entrepreneur", №875-Vrs-Xmp, 02/08/2021.

entities. There should be also assessed the scale of personal data processing, which is determined according to the following criteria: a) the number of data subjects; b) the volume of processed data; c) the length of processing; d) the geographical coverage of processing.³¹ The national legislation may envisage other grounds of appointment of Data Protection Officer, for example, according to Federal Data Protection Act of Germany, in the private company, where at least 20 employees relating to the automated data protection are employed, the data protection officer must be appointed.³² The presence of an officer is also necessary if data processing is subject to the study of Data Protection Impact Assessment or if personal data are processed with the aim of commercial transmission, anonymous transmission or market or public opinion research.³³

As regards the classification of Data Protection Officer, the distinction is made between the internal and external officer institutions.³⁴ An internal officer is a person employed by the corporation and the other is a person associated with the corporation by the legal agreement (contract). It is also possible to separate the compulsory from voluntary Officer's institute. As it was highlighted in the previous paragraph, the definition of an officer is mandatory³⁵ in the cases in question, however, the mentioned does not exclude the appointment of the officer voluntarily within the framework of self-regulation and statutory autonomy. Obviously, it indicates the high culture of corporate governance and standard of accountability. The General Data Protection Regulation (Article 37(2)) stipulates the general officer's institute as well, when several controllers and processor have one officer. The mentioned is particularly useful for corporate consortiums, group of organizations and holding companies.

As mentioned-above, the appropriate professional qualification is one of the conditions for appointment to the post. According to the commentary literature, this relates to the officer's certification, the knowledge of general rules of business management.³⁶

³¹ *Kuner Ch., Bygrave L., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford, 2020, 693.*

³² § 38, Bundesdatenschutzgesetz, (BDSG), 30/06/2017.

³³ *Ibid.*

³⁴ *Voigt P., Bussche A., The EU General Data Protection Regulation (GDPR), A Practical Guide, 2017, 57.*

³⁵ Occasioned by the goals of the paper, the case of mandatory appointment of data protection officer in public agency is not reviewed, see Art. 37(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), OJ L 119, 4/5/2016, 1–88.

³⁶ *Kuner Ch., Bygrave L., Docksey Ch., The EU General Data Protection Regulation (GDPR), A Commentary, Oxford, 2020, 695.*

3.3. DPO's Independence and the Prohibition of Conflicts of Interest

A Data Protection Officer should be equipped with appropriate resources to ensure that he/she can carry out his/her own duties in an independent, timely and competent manner.³⁷ Any influence or pressure on DPO is prohibited. At the same time, nor may he hold the position in the corporation that would allow him to determine the purpose and means of data processing³⁸. Consequently, he/she must not be a data controller or processor. In addition, it is worth noting, that a Data Protection Officer may also combine other functions, provided this does not lead to a conflict of interests.³⁹ A conflict of interests constitutes when the officer simultaneously performs the function that is in direct conflict to that of protection of personal data within his/her institution.⁴⁰ In this case, any similar conflict of interest on the part of the DPO must be declared and disclosed. From the perspective of the corporate law, there is no conflict of interest when a certain group of organizations has the common officer. However, as mentioned above, the Data Protection Officer must be able to perform his/her duty perfectly.

The interest should be evinced in the practice of supervisory authorities of data protection: the Slovenian Data Protection Supervisory Authority considered the appointment of the company Chief Executive Officer CEO or the member of board of directors as a DPO to be the conflict of interest and deemed it inadmissible⁴¹. In 2019, the Spanish Data Protection Supervisory Authority penalized the corporation €25,000 because it imposed the function of a DPO on so called "Internal Data Protection Board" - a body set up within the internal corporate structure, which, according to the controller, had assumed the same function as the Data Protection Officer.⁴²

In accordance with the recommendation of *European Data Protection Supervisor* the Data Protection Officer must not be employed by the corporation on the fixed-term or short-term contract; He/she should be able to manage its own funds independently and should be accountable only to the top management of the corporation.⁴³

³⁷ Voigt P., Bussche A., *The EU General Data Protection Regulation (GDPR), A Practical Guide*, 2017, 58-59.

³⁸ *Article 29 Data Protection Working Group*, Guidelines on Data Protection Officers (DPOs), 16/EN, WP 243 rev.01, 2016, 24.

³⁹ Voigt P., Bussche A., *The EU General Data Protection Regulation (GDPR), A Practical Guide*, 2017, 60.

⁴⁰ *Data Protection Officer*, Professional Standards for Data Protection Officers of the EU Institutions and Bodies Working under Regulation (EC) 45/2011, 2010, 15.

⁴¹ *Informacijski pooblaščenec*, Advisory Opinion, N07121-1/2021/577, 2021, <[https://gdprhub.eu/index.php?title=IP - 07121-1/2021/577#Facts](https://gdprhub.eu/index.php?title=IP_-_07121-1/2021/577#Facts)> [22.01.2023].

⁴² *Agencia Española Protección Datos*, Resolución de procedimiento sancionador, Procedimiento Nº: PS/00417/2019, <<https://cedpo.eu/dpo-case-law/>> [22.01.2023].

⁴³ *European Data Protection Supervisor*, Data Protection Officer (DPO), <https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en> [20.01.2023].

Accordingly, the principle of independence and the requirement to prohibit conflicts of interest also apply to the Data Protection Officer, along with the other principles mentioned above. A logical extension of the principle of independence and impartiality is the rule of appropriate remuneration, which is also attached some importance in corporate law⁴⁴ in terms of ensuring the independence of management board.

3.4. The Issue of DPO's Liability

The EU General Data Protection Regulation does not include a separate provision regulating the responsibility of the Data Protection Officer. The Data Protection Officer is not personally liable for the failure to comply with the data protection legislation. However, it is worth noting, that he carries the duty of loyalty⁴⁵ to the very organization to which he has been assigned. The officer acts on the basis of internal professional beliefs that are linked to the principle of care. He is therefore obliged to consider each case carefully and without delay⁴⁶.

The duty of confidentiality⁴⁷ is also applicable to the Data Protection Officer. In corporate governance the concept of the duty of silence imposed on the members of management and supervisory board serves the purpose of protecting insider information.⁴⁸ It must not be relaxed or excluded.⁴⁹

The failure to fulfil obligations duly and in good faith is the direct liability of the Data Protection Officer. From this point of view, the scientific literature refers to the contractual liability of the external officer and in terms of the data subject - to his/her tort liability.⁵⁰ As far as the internal officer is concerned, his/her liability is grounded on the labour law.⁵¹

⁴⁴ About the remuneration of management. See *Schneeman A.*, Law of Corporations and Other Business Organizations, 2010, 348-349.

⁴⁵ *Data Protection Officer*, Professional Standards for Data Protection Officers of the EU Institutions and Bodies Working under Regulation (EC) 45/2011, 2010, 14-15.

⁴⁶ *Ibid*, 15.

⁴⁷ Art. 38(5), 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), OJ L 119, 4/5/2016, 1–88.

⁴⁸ *Chanturia L.*, Corporate Governance and Liability of Management Members in the Corporate Law, 2006, 360-361 [in Georgian].

⁴⁹ *Ibid*, 362.

⁵⁰ *Paal P. B., Pauly D. A.*, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, Kommentar, 3. Aufl., 2021, Art. 39, para. 11, 12.

⁵¹ *Ibid*.

3.5. The Dismissal of a DPO

The EU General Data Protection Regulation does not regulate the issue relating to the dismissal of the officer and the termination of legal relationship with him/her. Accordingly, the mentioned represents the issue to be regulated by the national legislation of the EU member country. Pursuant to Article 38(3) of the GDPR, an officer may not be dismissed or penalized in connection with the performance of duties imposed on him/her by a data controller or processor. The officer cannot be dismissed for the sole reason that the data controller or processor does not agree with the data processing guidelines proposed by him/her.⁵² Such regulation of the issue creates a high standard to protect a DPO against the pressure from the data controller/processor. This naturally creates the positive impact on DPO's independence. On the other hand, the mentioned does not deal with the gross negligence or cases of wrongdoings on the part of officers.

The Court of Justice of the European Union (CJEU) in its judgment of 22 June 2022 in the case of "Leistriz AG v. LH" noted that the above-mentioned requirement of the Regulation (under Article 38(3) of the GDPR) applies to both internal and external officer. The national law of a member state may envisage the possibility of terminating the contract with the officer only on the fairgrounds, even if the termination is not related to the performance of the officer's duties, as long as this does not hinder the achievement of the objective laid down in the general provisions.⁵³ The mentioned represents the additional safeguard for the independence of a DPO, which in turn ensures the homogeneous and consistent implementation of the rules regulating the rights related to data processing throughout the European Union.⁵⁴ Moreover, the national legislation may consider far stronger mechanism to protect the officer from dismissal than it is established by the GDPR.⁵⁵

4. Conclusion

The standards of personal data protection are recognized at the international level have been reflected in the strategy of corporate governance. The aforementioned conditions the establishment of the new model of corporate governance, which is focused on protecting the interests and rights of data subjects. In this paper such a management policy is referred to as the personal data protection-oriented model of corporate governance. Its introduction in the

⁵² *Article 29 Data Protection Working Group, Guidelines on Data Protection Officers (DPOs)*, 16/EN, WP 243 rev.01, 2016, 15.

⁵³ CJEU, C-534/20, *Leistriz AG v. LH* [2022], para. 23-24, 36.

⁵⁴ *Ibid*, para. 26.

⁵⁵ *Ibid*, para. 33-36.

governance system will ensure the compliance of the corporation with the legislation regulating the data protection, as well as, take into consideration the interests of the data subject – “a stakeholder” in the system of corporate governance. One of the elements of such model represents the Data Protection Officer, who ensures the proportionality between the legal and economic interests of the entrepreneurial entity, on the one hand and a data subject on the other. In order to achieve the mentioned goal, the officer is equipped with the appropriate legal leverage. In particular, he is bound by the principles of independence, confidentiality, competency and accountability. In addition, he is protected from the direct or indirect influence of corporate insiders (implying the executives and supervisory board members of the corporation). In its turn, the principles of competence and care applicable to the officer as well as the prohibition of conflicts of interests serve the effective implementation of protection of data subjects’ rights and the compliance of the corporation with the acts regulating the data protection.

Based on the economic-legal analysis⁵⁶ of institute of Data Protection Officer, it may be inferred that it ensures the reduction of those additional expenses relating to the corporate compliance, which the entrepreneurial entity may incur (e.g., in the form of penalty charged) due to the incompliance with the acts regulating data protection. The voluntary appointment of a DPO intends the decrease exactly in this economic expenditure and, as it is evaluated in this paper, indicates the high culture of corporate governance and personal data protection.

Nowadays, the institute of the Data Protection Officer is not familiar to the Georgian legislative regulation. However, the draft law on “Personal Data Protection”⁵⁷ envisages its institutional regulation that will have the positive effect on raising the awareness of entrepreneurial entities regarding the personal data protection and putting the modern model of corporate governance into practice.

Bibliography:

1. Bundesdatenschutzgesetz, (BDSG), 30/06/2017.
2. *Council of Europe*, Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+; CM/Inf(2018)15-final), 18/05/2018.

⁵⁶ Implying the economic analysis of law as the method established in the law science. *Posner R.*, Economic Analysis of Law, 2011, 1-3.

⁵⁷ Art. 33, Draft Law of Georgia on “Personal Data Protection № 07-3/353/9, 22/05/2019, <www.parliament.ge> [23.01.2023].

3. *Council of Europe*, Explanatory Report, Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+; CM/Inf(2018)15-final), 18/05/2018.
4. Draft Law of Georgia Personal Data Protection, №07-3/353/9, 22/05/2019, <www.parliament.ge> [23.01.2023].
5. The Law of Georgia on “Entrepreneurs”, 875-VRS-XMP, 02/08/2021.
6. The Law of Georgia on Personal data protection, 5669-RS, 28/12/2011.
7. 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), OJ L 119, 4/5/2016, 1–88.
8. *OECD*, Principles of Corporate Governance, 2015.
9. *Article 29 Data Protection Working Group*, Guidelines on Data Protection Officers (DPOs), 16/EN, WP 243 rev.01, 2016, 10, 15, 24.
10. *Bentham J.*, Of Laws in General, *Hart H. L. A. (ed.)*, 1970, 31-33.
11. *Burduli I., Makharoblishvili G., Tokhadze A., Zubitashvili N., Aladashvili G., Maghradze G., Egnatashvili D.*, Corporate Law, 2022, 60-63, 634-638 [in Georgian].
12. *Chanturia L.*, Corporate Governance and Liability of Management Members in the Corporate Law, 2006, 360-36, 362 [in Georgian].
13. *Data Protection Officer*, Professional Standards for Data Protection Officers of the EU Institutions and Bodies Working under Regulation (EC) 45/2011, 2010, 12-13, 14-15.
14. *European Data Protection Supervisor*, Data Protection Officer (DPO), <https://edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en> [20.01.2023].
15. *European Union Agency for Fundamental Rights and the Council of Europe*, Handbook on European Data Protection Law, 2018, 198.
16. *Jasper K.*, Introduction to Philosophy, *Gorgisheli V. (trans.)*, 2019, 73 [in Georgian].
17. *Johnson A.*, Soft Law, in: EC Regulation of Corporate Governance, UK, 2009, 343-347.
18. *Haskel J., Westlake S.*, Capitalism without Capital: The Rise of the Intangible Economy, Princeton, 2018, 3-10.
19. *Kuner Ch., Bygrave L., Docksey Ch.*, The EU General Data Protection Regulation (GDPR), A Commentary, Oxford, 2020, 693, 695.
20. *Makharoblishvili G.*, General Analysis of Corporate Governance, 2015, 161, 162-163, 313-317 [in Georgian].
21. *Magnier V.*, Comparative Corporate Governance, Legal Perspectives, 2017, 1-4.
22. *Paal P. B., Pauly D. A.*, Datenschutz-Grundverordnung Bundesdatenschutzgesetz, Kommentar, 3. Aufl., 2021, Art. 39, para. 11, 12.
23. *Picciotto S.*, Regulating Global Corporate Capitalism, 2011, 61-65, 193-200.

24. *Posner R.*, *Economic Analysis of Law*, 2011, 1-3.
25. *Schneeman A.*, *Law of Corporations and Other Business Organizations*, 2010, 39, 348-349, 363.
26. *Tokhadze A.*, *Enhancement of Corporate Social Responsibility – An Analysis from the Perspective of Economic and Sectoral Cooperation under the Three Association Agreements*, in: *Legal Aspects of the EU Association Agreements with Georgia, Moldova and Ukraine in the Context of the EU Eastern Partnership Initiative*, *Trunk A., Panych N., Rieckhof S. (eds.)*, 2017, 104-106.
27. *Voigt P., Bussche A.*, *The EU General Data Protection Regulation (GDPR), A Practical Guide*, 2017, 56-60.
28. *Autorité de protection des données*, Dossiernummer: DOS-2019-04309, 2020, <<https://cedpo.eu/dpo-case-law/>> [20.01.2023].
29. *Agencia Española Protección Datos*, Resolución de procedimiento sancionador, Procedimiento Nº: PS/00417/2019, <<https://cedpo.eu/dpo-case-law/>> [22.01.2023].
30. *Informacijski pooblaščenec*, Advisory Opinion, N07121-1/2021/577, 2021, <https://gdprhub.eu/index.php?title=IP_-_07121-1/2021/577#Facts> [22.01.2023].
31. CJEU, C-534/20, *Leistriz AG v. LH* [2022].