PERSONAL DATA
PROTECTION SERVICE

JOURNAL OF PERSONAL DATA PROTECTION LAW

N1, 2024

Journal of Personal Data Protection Law

№1, 2024

The third edition of the Journal of Personal Data Protection Law is dedicated to the enactment of the new law of Georgia “On Personal Data Protection"

P-ISSN 2720-8745
E-ISSN 2720-8761

Table of Contents

From the Editor-in-Chief

Dear Reader,

We are pleased to present the third edition of the Journal of Personal Data Protection Law, dedicated to the enactment of new law of Georgia “On Personal Data Protection."

To strengthen the fundamental constitutional rights of personal data protection and privacy, align existing data protection legislation with European standards, fulfill Georgia’s international obligations, and establish globally recognized principles and best practices, data protection supervisory bodies play a critical role. The national data protection supervisory authority’s activities are essential for enforcing legislation effectively and implementing supervisory responsibilities and powers. International cooperation between data protection supervisory authorities is also key to integrating best practices worldwide. In this regard, our collaboration with the European Data Protection Board (EDPB), the European Data Protection Supervisor (EDPS), and other data protection authorities across Europe is particularly valuable. This cooperation facilitates the exchange of best practices, which is instrumental as we work towards implementing the new personal data protection law.

This scientific publication also serves as a platform for collaboration between Georgian and international scholars and practitioners in privacy and data protection law. It offers readers a selection of insightful research on current issues in the field and emerging international legal trends. The primary mission of the journal is to foster comparative legal discourse on information protection, leveraging rigorous research to support the development of the national supervisory body and enhance public awareness.

The current issue of the journal explores key trends and pressing topics in personal data protection, including international data transfer, synthetic data and concept of anonymization, notary electronic registry and data security standards, the protection of minors’ data, among others. Each article represents a valuable scholarly contribution to defining legal institutions under the new law “On Personal Data Protection”. I would like to extend my gratitude to each author for their contributions to this issue and for sharing such insightful research.

I would like to express special gratitude for the contribution of Prof. Dr. Norbert Bernsdorff, Retired Judge at the Federal Social Court of Germany, Professor at Philipps University of Marburg, and member of the editorial board of the Journal of Personal Data Protection Law, for his invaluable scientific support of the journal.

I would also like to express my gratitude to privacy researcher Dr. Alexander Boudewijn and University of Bologna researcher Andrea F. Ferraris for presenting an innovative and timely scientific paper.

Considering the rapid pace of technological progress, I believe this issue of the journal will attract a wide audience, with its published works appealing not only to legal scholars but also to professionals in related fields of privacy and personal data protection law.

Assoc. Prof. Dr. Dr. Lela Janashvili

President of the Personal Data Protection Service of Georgia
Associate Professor at Ivane Javakhishvili Tbilisi State University
Associate Professor at the Autonomous University of Barcelona

Norbert Bernsdorff*

Transfer of Personal Data to Third Countries - "Safe Harbour", "EU-US Privacy Shield" and "Trans-Atlantic Data Privacy Framework"

The new „Trans-Atlantic Data Privacy Shield Framework“-Agreement is the successor of the „EU-US Privacy Shield“-Agreement. The European Commission’s adequacy decision, which was based on the latter, was declared invalid bei the Court of Justice of the European Union in July 2020 in the sensational „Schrems II“ judgement. Prior to this, the judges in Luxembourg had already criticised the adequacy decision, which was based on the predecessor agreement known as „Safe Harbour“-Agreement. The reason in both cases was the far-reaching surveillance and intervention powers of the US security authorities with regard to the personal data of citizens of the European Union. These two judgements meant that, according to the Court of Justice, the level of data protection in the USA was not equivalent to that in the European Union.

Keywords: *Data privacy, data protection, transfer to third countries, „Safe Harbour“-Agreement, „EU-US Privacy Shield“-Agreement, „Trans-Atlantic Data Privacy Shield Framework“-Agreement, Facebook, Court of Justice of the European Union, case law, General Data Protection Regulation.*

1. Introduction

Personal data may only be transferred to third countries if the level of protection guaranteed by the General Data Protection Regulation (GDPR)[1] is not "undermined". Third countries are countries in which the GDPR does not apply. As the GDPR is only binding for the member states of the European Union (EU), third countries are therefore all countries that are not members of the EU. This means that the countries of the European Economic Area, Iceland, Liechtenstein and Norway, also belong to the group of third countries as long as they have not decided to apply the GDPR. A particular transmission problem exists in relation to the United States of America (USA). These do not have a level of data protection equivalent to that in Europe.

* Doctor of Law, Professor at the Philipps University of Marburg; Retired Judge of the German Federal Court of Social Affairs; Former Data Protection Commissioner of the Lower Saxony Judiciary. The Author is a Member of the Editorial Board of the “Journal of Personal Data Protection Law“.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, OJ 2016 L 119, 1.

Since the "*Edward Snowden*" case and his surveillance by the US secret service, trust in American data protection has been lost. EU citizens can also be monitored in the USA, for example when they send messages via the US network Facebook (Meta).

Following the failure of the "Safe Harbour" and "EU-US Privacy Shield" data protection agreements between the European Union (EU) and the USA before the Court of Justice of the European Union, the EU and the USA have now attempted for the third time to find a compromise between the high standard of protection provided by European data protection law and the mass surveillance that continues to be politically desirable in the USA with the "Trans-Atlantic Data Privacy Shield Framework"-Agreement.

2. History and Significance

The former Data Protection Directive (95/46/EC; DPD)[2] correctly recognised the cross-border movement of personal data as a necessity for the development of international trade. The cross-border flow of data and thus also the cross-border transfer of personal data is a matter of course in a digitally networked world and not least due to the possibilities of using the Internet. However, an equal level of data protection or even just an equal concept of data protection does not exist globally.[3]

The DPD had two effects: On the one hand, it created an EU-wide framework for national data protection laws and thus harmonised the level of data protection in the EU. In doing so, it created the framework conditions for a fundamentally unhindered transfer of personal data within the EU. On the other hand, it demarcated the EU from other countries in terms of data protection law. This is because it stipulated the conditions under which data could be transferred to countries other than EU member states.

The GDPR continued this approach in Articles 44 to 50. However, the depth of its provisions goes beyond the depth of the provisions of the former DPD. The GDPR thus takes account of developments in the reality of life since 1995. The following should be pointed out: EU data protection law should not be a "brake block" for economic development.[4] Cross-border data traffic with third countries is essential for business and trade; however, it is risky for data protection.

3. The System of the General Data Protection Regulation

The transfer of personal data to third countries is regulated in Articles 44 to 50 of the GDPR. The GDPR thus creates a standardised level of data protection within the EU; at the same time, it distinguishes the EU from other countries by setting limits on the processing of personal data in third countries.

Article 44 GDPR sets out the general principles for the transfer of personal data to third countries. Articles 45 to 49 regulate various instruments for justifying the transfer of personal

[2] 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, OJ 1995 L 281, 31.

[3] See: *Wuermeling U.*, Handelshemmnis Datenschutz - Die Drittländerregelung der Europäischen Datenschutzrichtlinie, Berlin, 2000.

[4] For more information see: *Rüpke G.*, *von Lewinski K.*, *Eckardt J. (eds.)*, Datenschutzrecht - Grundlagen und europarechtliche Umgestaltung, Munich 2018, § 18. On the requirements of a "European internal data market" *Brink St.*, *Oetjen St.*, *Schwartmann R.*, *Voss K.*, So war die DSGVO nicht gemeint, Frankfurter Allgemeine Zeitung (FAZ) v. 17 July 2022.

data to a third country. Article 50 GDPR standardises international cooperation for the protection of personal data. The admissibility criteria in Articles 45 to 49 GDPR are not legally related to each other. According to Article 45, the adequacy of the level of data protection is recognised for a specific third country. With the mechanisms of Articles 46 and 47 GDPR, an adequate level of data protection is created for certain companies in third countries with regard to certain data processing. Individual specific transfers of personal data are permitted on the basis of Articles 48 and 49 GDPR.

The assessment of the permissibility of a transfer of personal data to a third country requires a two-stage examination.[5] Article 44 GDPR expressly clarifies that, in addition to Articles 44 et seq. GDPR, the other provisions of the GDPR must also be complied with. These are the provisions in Articles 6, 9 and 10 GDPR.[6] At the first stage, in accordance with the general prohibition with the reservation of permission anchored in Articles 6, 9 and 10 GDPR, it must be checked whether there is a legal basis for the transfer of the data to the recipient. In the second stage, it must be checked whether the requirements of Articles 44 et seq. GDPR are met. This is because only then is the transfer of personal data to the third country permitted.

This two-tier structure also results from the purpose and system of the GDPR. It creates a standardised data protection legal framework in the EU. Therefore, cross-border processing as such does not pose a risk to the data subject. The risk therefore only arises from a transfer from one data controller to another data controller. Articles 6, 9 and 10 GDPR take this risk into account.[7] A data transfer outside the area of the harmonised legal framework poses an additional risk.

Onward transfer by the recipient in the third country to another third country is also only permitted if Articles 44 et seq. GDPR and the other provisions of the GDPR are complied with.

4. The Case Law of the Court of Justice of the European Union

The transfer of personal data to the USA has already been criticised twice by the Court of Justice under data protection law. Firstly, it declared the "Safe Harbour"-Agreement negotiated by the EU and the USA invalid, and then the "EU-US Privacy Shield"-Agreement, including the respective adequacy decisions of the European Commission (EU Commission).

a. Judgement of the Court of Justice in Case C-362/14, Maximillian Schrems/Data Protection Commissioner, Digital Rights Ireland Ltd, 6 October 2015 ("Schrems I")[8]

The decision of the Court of Justice of 6 October 2015 on the EU Commission's „Safe Harbour“ Principles was of crucial importance for the transfer of personal data to third countries and in particular for data transfers to the USA. In this judgement, the Court of Justice laid down fundamental cornerstones for the former DPD. The decision had an influence on the design of Articles 44 to 50 of the later GDPR.

[5] Likewise: *Albrecht J. Ph.*, *Jotzo Fl.*, Das neue Datenschutzrecht der Europäischen Union, Baden-Baden, 2017, Part 6.
[6] *Schantz P.*, *Wolff H. A.*, Das neue Datenschutzrecht, Berlin, 2017, 239.
[7] See *Rüpke G.*, *von Lewinski K.*, *Eckardt J. (eds.)*, Datenschutzrecht- Grundlagen und europarechtliche Umgestaltung, Munich, 2018, § 18, 266.
[8] ECLI:EU:C:2015:650.

Facts of the case: *Schrems*, an Austrian citizen, lodged a complaint with the Irish data protection supervisory authority with the aim of preventing Facebook Ireland from transferring his personal data to Facebook Inc. in the USA. At that time, all persons resident in the Union territory who wished to use Facebook had to sign a contract with Facebook Ireland, a subsidiary of Facebook Inc. based in the USA, when they registered. The personal data of Facebook users resident in the Union territory were transferred in whole or in part to Facebook Inc. servers located in the USA and processed there. The Irish data protection supervisory authority rejected the complaint as unfounded. Among other things, it stated that all issues relating to the adequacy of the protection of personal data in the USA had to be clarified in accordance with the EU Commission's adequacy decision 2000/520/EC[9] and that the Commission had found in this decision that the USA guaranteed an adequate level of protection if the requirements of this decision were met („Safe Harbour" Principles). The Irish data protection supervisory authority considered itself to be bound by the adequacy decision of the EU Commission without its own review competence. The complainant *Schrems* then took legal action. The Irish High Court made clear its concerns about the admissibility of the data transfer to the USA. It ultimately referred the question to the Court of Justice for a preliminary ruling as to whether the Irish data protection supervisory authority was bound by the finding made by the EU Commission in its decision that the USA guaranteed an adequate level of protection or whether Art. 8 of the European Charter of Fundamental Rights[10] would have authorised it to override such a finding if necessary.

The question of the legality of the EU Commission's Decision 2000/520/EC on the "Safe Harbour" Principles was not the subject of the Irish High Court's referral. Nevertheless, the Court of Justice also ruled on it. It pointed out that the complainant *Schrems* was de facto questioning this legality with his complaint. The Court of Justice thus extended the subject matter of its decision.

With regard to the question referred by the Irish High Court, the Court of Justice comes to the conclusion that the national data protection supervisory authorities are not limited in their review competence by a decision of the EU Commission under the DPD; there is an independent review competence of the national supervisory authorities. However, the authority to declare a decision of the EU Commission invalid lies solely with it; the Court of Justice has a monopoly on rejection. The national data protection supervisory authorities would therefore have to take legal action before it after exercising their review competence.

The Court of Justice considered that where a claim is lodged with national supervisory authorities, they can examine whether the transfer a person's data to a third country complies with the requirement of the EU legislation on the protection of the data, even in those cases which the EU Commission adopted decision finding a third country affords an adequate level of protection of personal data and even considered that the Court of Justice alone has jurisdiction to declare an EU act invalid.

On the merits, the Court of Justice stated word-by-word:

„In particular, legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by Article 7 of the Charter (see, to this effect, judgment in Digital Rights Ireland and Others, C-293/12 and C-594/12, ECLI:EU:C:2014:238, paragraph 39).

[9] Decision 2000/520/EC of the European Commission of 26 July 2000.
[10] Charter of Fundamental Rights of the European Union, OJ 2010 L 83, 389.

Likewise, legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him , or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection, as enshrined in Article 47 of the Charter. The first paragraph of Article 47 of the Charter requires everyone whose rights and freedoms guaranteed by the law of the European Union are violated to have the right to an effective remedy before a tribunal in compliance with the conditions laid down in that article. The very existence of effective judicial review designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law (…).“

With its ruling, the Court of Justice not only established the invalidity of the "Safe Harbour"-Agreement between the EU and the USA. With its judgement, it also laid down criteria for assessing the adequacy of the level of data protection.[11] This also had an impact on the successor agreement - the "EU-US Privacy Shield"-Agreement - which came under increased scrutiny in terms of data protection law and data protection policy.

b. Judgement of the Court of Justice in Case C-311/18, Data Protection Commissioner/Facebook Ireland Ltd, Maximillian Schrems, 16 July 2020 ("Schrems II")[12]

In order to once again take into account the importance of data traffic to the USA, the "EU-US Privacy Shield"-Agreement on data exchange with the USA was implemented on 12 July 2016 as a successor agreement to the "Safe Harbour"-Agreement on the basis of the EU Commission's adequacy decision 2016/1250[13]. The content of this adequacy decision by the EU Commission was that companies that made a voluntary commitment in accordance with the „EU-US Privacy Shield“ Mechanism had an adequate level of data protection.

The "EU-US Privacy Shield" Mechanism was therefore comparable to the "Safe Harbour" Mechanism. US companies made a voluntary commitment to the US Department of Commerce to process data transferred to them from the EU only in accordance with certain "principles"; there was a voluntary commitment to maintain the level of data protection in the EU. The Federal Trade Commission and the US Department of Transportation monitored compliance with this voluntary commitment. The "EU-US Privacy Shield" Mechanism was therefore only open to companies that were subject to the supervision of these authorities. The Department of Commerce was primarily responsible for monitoring compliance with the voluntary commitment. Penalties could be imposed by the Federal Trade Commission in the event of violations. From the outset, there were considerable doubts about the effectiveness of data protection supervision by US authorities.

Facts of the case: The complainant in the "Safe Harbour" proceedings, *Schrems*, complained to the Irish data protection supervisory authority that Facebook Ireland was forwarding his data to the parent company in the USA. In further proceedings, an Irish court turned to the Court of Justice to decide whether the standard contractual clauses and the „EU-US Privacy Shield“ are compatible with the European level of data protection. The Luxembourg judges declared the „EU-US Privacy Shield“ Mechanism invalid. In view of the US authorities' access options, the data protection requirements are still not guaranteed. In

[11] Likewise *Kühling J.*, *Heberlein J.*, EuGH "reloaded": "unsafe harbour" USA vs. "Datenfestung" EU, Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2016, 7,9.
[12] ECLI:EU:C:2020:559.
[13] Decision (EU) 2016/1250 of the European Commission of 12 July 2016.

addition, the legal protection for data subjects - the right to an effective legal remedy - is still inadequate.

A particular problem after all of this was the US authorities' authorisation to access data transferred from the EU and the question of legal remedies against this access. This was a key aspect of the Court of Justice's decision to declare the "Safe Harbour" Mechanism invalid.

The Court of Justice word-by-word formulated:

„In those circumstances, the limitations on the protection of personal data arising from the domestic law of the United States on the access and use by US public authorities of such data transferred from the European Union to the United States, which the Commission assessed in the Privacy Shield Decision, are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required, under EU law, by the second sentence of Article 52 (1) of the Charter.

Therefore, the ombudsperson mechanism to which the Privacy Shield Decision refers does not provide any cause of action before a body which offers the persons whose data is transferred to the United States guarantees essentially equivalent to those required by Article 47 of the Charter.

It follows, that Article 1 of the Privacy Shield Decision is incompatible with Article 45 (1) of the GDPR, read in the light of Articles 7, 8 and 47 of the Charter, and is therefore invalid.“

What is the role of the EU Commission and what is the role of the national data protection supervisory authorities when data is transferred to third countries?

The EU Commission is not obliged to review the level of data protection in third countries when adopting standard contractual clauses. Rather, the Court of Justice emphasises the responsibility of the data exporter to check the level of protection in the third country for each data transfer and to provide suitable guarantees for the protection of the data transferred to a third country. It may be necessary to provide additional safeguards over and above the standard contractual clauses by means of additional measures.

The data exporter is obliged to suspend or terminate the data transfer if the protection of the transferred data cannot be adequately ensured even by additional measures.

The national data protection supervisory authorities have a very important role to play in the application of appropriate safeguards such as the standard contractual clauses. They are obliged to review the application of the appropriate safeguards, in particular if a complaint is lodged against a data transfer on the basis of an appropriate safeguard that casts doubt on the effectiveness of an adequacy decision by the EU Commission.

According to Art. 58 GDPR, the national supervisory authorities must prohibit the data transfer or order its suspension if there is no valid adequacy decision by the EU Commission, neither the appropriate guarantee nor additional measures sufficiently ensure the protection of the data transferred to a third country and the data exporter does not suspend or terminate the data transfer itself.

In their assessment of the level of protection existing in the third country, the supervisory authorities are ultimately bound by adequacy decisions of the EU Commission if these are valid.

5. The New "Trans-Atlantic Data Privacy Framework"-Agreement

A few years after the Court of Justice ruling of 16 July 2020 ("Schrems II"), the EU Commission and the USA have made a new attempt at a data protection agreement. A new

adequacy decision by the EU Commission should finally put the transfer of personal data to US companies on a legally secure footing.

a. Preparations

On 25 March 2022, US President *Biden* and EU Commission President *von der Leyen* announced their agreement in principle on a "Trans-Atlantic Data Privacy Shield Framework" Mechanism. The content of this agreement is set out in a press release from the US government, among other things.[14]

This results in the following:[15]

Instead of the ombudsperson of the previous "EU-US Privacy Shield"-Agreement, the "Trans-Atlantic Data Privacy Shield Framwork"-Agreement is to create a quasi-judicial, two-tiered body that will decide on complaints from data subjects in the EU. The body would be authorised to investigate comprehensively and order binding remedies. Although it should not be part of the judiciary, it should be as independent as possible. In particular, it should be composed of persons who are not members of the US government.

Furthermore, new measures are being established at the US security authorities in order to reduce surveillance to a proportionate level and enforce constitutional standards. It remains unclear what these measures will be. The USA will not implement these changes by means of a parliamentary act, but only by means of a new administrative regulation (so-called Executive Order) issued by the US President.

The "Trans-Atlantic Data Privacy Shield Framework"-Agreement is intended to build on the previous "EU-US Privacy Shield" Mechanism. The requirements for US companies will remain the same and previous certifications will continue to apply. Accordingly, even the term "Privacy Shield" will continue to be used for the certification. The US government had continued the "Privacy Shield" certification unchanged even after the ruling of the Court of Justice on 16 July 2020.[16]

The "Trans-Atlantic Data Privacy Shield Framework"-Agreement contains certain principles for the self-certification of US companies that are based on European data protection law. They appear to be a kind of GDPR "light".[17] Self-certification is carried out by registering a US company on a Department of Commerce website in return for a registration fee. The corresponding website has been available since 17 July 2023.[18] From this date, the approximately 2,600 "Privacy Shield"-certified US companies will also be considered "Trans-

[14] For more information see: <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states and european commission-announce-trans-atlantic-data-privacy-shield framework.pdf> [10.05.2024]. Also *Glocker F.*, Politische Lösung für Datentransfers in die USA zeichnet sich ab <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/trans-atlantic-data-privacy-shield-framework.html> [10.05.2024].

[15] *Glocker F.,* EU-US Data Privacy Framework: Beschluss der EU-Kommission, <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eu-us-data-privacy-framework-beschluss-der-eu-kommission.html> [10.05.2024] Also: *Glocker F.,* Politische Lösung für Datentransfer in die USA zeichnet sich ab <https://www.cmshs-bloggt.de/datenschutzrecht/trans-atlantic-data-privacy-shield-framework.html> [10.05.2024].

[16] For more information see: <https://www.privacyshield.gov/article?id=EU-US-Privacy-Shield-Programm.html> [10.05.2024].

[17] Thus expressly *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eu-us-data-privacy-framework-beschluss-der-eu-kommission.html> [10.05.2024].

[18] The website can be found at <https://www.dataprivacyframework.gov/s.html> [10.05.2024].

Atlantic Data Privacy Framework"-certified. These include all major US cloud providers, SaaS providers and IT service providers.

b. So-called. Executive Order and Adequacy Decision of the EU Commission

On 10 July 2023, the EU Commission adopted the "Trans-Atlantic Data Privacy Shield Framework"-Agreement and announced the corresponding adequacy decision in the Official Journal.[19] The US government has also published the US President's so-called Executive Order. Due to the improvements in the law of the US security authorities, the EU Commission now considers the US level of data protection to be equivalent to that of the EU if US companies have self-certified under the new mechanism.[20]

6. Conclusions - "Schrems III"?

The "Trans-Atlantic Data Privacy Shield Framework"-Agreement has a decisive advantage: it offers legal certainty! The EU Commission's new adequacy decision binds national data protection supervisory authorities. They may not prohibit data transfers to self-certified US companies, but must treat them as authorised. This eliminates the great uncertainty surrounding standard contractual clauses, which the data protection supervisory authorities previously regarded as insufficient protection for data subjects in some cases.

The transfer to non-self-certified US companies is also effectively facilitated. It is true that data controllers must continue to conclude standard contractual clauses with non-self-certified companies. In such cases, national data protection supervisory authorities would actually be obliged to examine the law of the third country for compatibility with European data protection law (so-called transfer impact assessment). Instead of carrying out their own so-called transfer impact assessment, the parties can therefore now refer to the existing assessment of US law by the EU Commission in the adequacy decision.[21]

It is doubtful whether the "Trans-Atlantic Data Privacy Shield Framework" - Agreement and the EU Commission's adequacy decision really fulfil the requirements of the Court of Justice. Resistance to this is already very strong:

The establishment of an independent, quasi-judicial body to examine complaints is indeed skilful and could possibly meet the Court of Justice's requirements for a judicial remedy. However, it remains unclear whether the very generally formulated so-called Executive Order of the US President, on which the extensive surveillance activities of the US security authorities are based, will fulfil the requirements of the Court of Justice for clear and precise rules on the scope and application of the measures in question. Furthermore, it is not clear from the published documents how the surveillance by US security authorities can be limited to what is "absolutely necessary" as required by the Court of Justice.

The fate of the "Trans-Atlantic Data Privacy Shield Framework"-Agreement could once again be decided before the Court of Justice. Civil rights organisations such as the *NOYB*[22] -

[19] Decision (EU) 2023/4745 of the European Commission of 10 July 2023.

[20] On this in detail *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission <https://www.cmshs-bloggt.de/datenschutzrecht/eu-us-data-privacy-framework-beschluss-der-eu-kommission.html> [10.05.2024].

[21] *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eu-us-data-privacy-framework-beschluss-dereu-kommission.html> [10.05.2024].

[22] „None Of Your Business".

European Center for Digital Rights, which is led by the complainant *Schrems,* have already announced their intention to bring an action against the EU Commission's new adequacy decision. French member of the European Parliament *Latombe* has also expressed this intention. However, the Court of Justice is not expected to rule on this quickly.[23]

Note: For the transfer of personal data to other third countries for which - unlike the USA - there is no adequacy decision by the EU Commission, the ruling of the Court of Justice of 16 July 2020 remains relevant.[24]

Bibliography:

1. Charter of Fundamental Rights of the European Union, OJ 2010 L 83, 389.
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC, OJ 2016 L 119, 1.
3. 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, OJ 1995 L 281, 31.
4. Decision 2000/520/EC of the European Commission of 26 July 2000.
5. Decision (EU) 2016/1250 of the European Commission of 12 July 2016.
6. Decision (EU) 2023/4745 of the European Commission of 10 July 2023.
7. *Albrecht J. Ph.*, *Jotzo Fl.*, Das neue Datenschutzrecht der Europäischen Union, Baden-Baden, 2017.
8. *Bernsdorff N.*, „EU-US Data Privacy Shield Framework“ und der EuGH, Zeitschrift für den europäischen Datenschutz (ZED) 2023, 210.
9. *Eichenhofer E.*, „e-Privacy“ im europäischen Grundrechtsschutz: Das „Schrems“-Urteil des EuGH, Europarecht (EuR) 2016, 76.
10. *Glocker F.*, Politische Lösung für Datentransfers in die USA zeichnet sich ab <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/trans-atlantic-data-privacy-shield-framework.html> [10.05.2024].
11. *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eu-us-data-privacy-framework-beschluss-der-eu-kommission.html> [10.05.2024].
12. *Kühling J.*, *Heberlein J.*, EuGH „reloaded“: „unsafe harbor“ USA vs. „Datenfestung“ EU, Neue Zeitschrift für Verwaltungsrecht (NVwZ) 2016, 7.
13. *von Lewinski K.*, Privacy Shield – Notdeich nach dem Pearl Harbor für den transatlantischen Datenverkehr, Europarecht (EuR) 2016, 405.
14. *Rüpke G.*, *von Lewinski K.*, *Eckhardt J. (eds.)*, Datenschutzrecht – Grundlagen und europarechtliche Umgestaltung, Munich, 2018.
15. *Schantz P.*, *Wolff H. A.*, Das neue Datenschutzrecht, Berlin, 2017.

[23] See *Bernsdorff N.*, "EU-US Data Privacy Shield Framework" und der EuGH, Zeitschrift für den europäischen Datenschutz (ZED) 2023, 210, 213.

[24] *Bernsdorff N.*, "EU-US Data Privacy Shield Framework" und der EuGH, Zeitschrift für den europäischen Datenschutz (ZED) 2023, 210,214; *Glocker F.*, Politische Lösung für Datentransfers in die USA zeichnet sich ab <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/trans-atlantic-data-privacy-shield-framework.html> [10.05.2024]; also *Glocker F.*, EU-US Data Privacy Framework: Beschluss der EU-Kommission <https://www.cmshs-bloggt.de/tmc/datenschutzrecht/eu-us-data-privacy-framework-beschluss-der-eu-kommission.html> [10.05.2024].

16. *Schreiber G.*, *Kohm W.*, Rechtssicherer Datenschutz unter dem EU-US Privacy Shield? – Der transatlantische Datenverkehr in der Unternehmenspraxis, Zeitschrift für Datenschutz (ZD) 2016, 255.
17. *Schwartmann R.*, Datentransfer in die Vereinigten Staaten ohne Rechtsgrundlage, Europäische Zeitschrift für Wirtschaftsrecht (EuZW) 2016, 864.
18. *Weichert Th.*, EU-US Privacy Shield – Ist der transatlantische Datenverkehr nun grundrechtskonform?, Zeitschrift für Datenschutz (ZD) 2016, 209.
19. *Wuermeling U.*, Handelshemmnis Datenschutz – Die Drittländerregelung der Europäischen Datenschutzrichtlinie, Berlin, 2000.
20. CJEU, Case C-362/14, *Maximillian Schrems/Data Protection Commissioner, Digital Rights Ireland Ltd.* („Schrems I"; 2015).
21. CJEU, Case C-311/18, *Data Protection Commissioner/Facebook Ireland Ltd., Maximillian Schrems* („Schrems II"; 2020).

Alexander Boudewijn*
Andrea F. Ferraris**

Legal and Regulatory Perspectives on Synthetic Data as an Anonymization Strategy

In an increasingly digital world, the protection of personal data is paramount for individuals, organizations, and regulators. As data collection technologies evolve, so must methods for ensuring data privacy. This paper explores synthetic data as a promising privacy-enhancing technology (PET) for anonymization, focusing on legal, theoretical, and practical perspectives. Synthetic data, generated algorithmically, do not pertain to real individuals, making them valuable for data science and AI development while preserving privacy. We examine the regulatory context, particularly under the GDPR, and identify privacy risks and attacks that anonymization must defend against. We argue that synthetic data, when properly generated, can meet anonymization standards and provide deployment recommendations to mitigate privacy risks. Our findings contribute to a standardized framework for synthetic data privacy assurance, aligning with current and future data protection regulations.

Keywords: *Synthetic data, anonymization, privacy-enhancing technology, GDPR.*

1. Introduction

In an increasingly digital world, the protection of personal data has become a critical concern for individuals, organizations, and regulators. As data collection and processing technologies evolve, so too must the methods for ensuring that personal information remains secure. One such method is anonymization, which aims to transform data in such a way that individuals are no longer identifiable. This process is essential for complying with privacy regulations like the General Data Protection Regulation (GDPR) and for protecting individuals' privacy against misuse. This paper explores synthetic data as an emerging privacy enhancing technology (PET)[1] and more specifically, anonymization technology from a legal and theoretical viewpoint.

Synthetic data are not collected empirically, but generated through algorithms. As such, they do not pertain to real individuals, but can be useful in data science activities and artificial

* PhD, Data Privacy Researcher at Aindo SpA, Trieste, Italy.
** Research Specialist / PhD Candidate in Law, Science and Technology, Data Valley Consulting srl, Milan, Italy & University of Bologna.
[1] OECD, "Emerging Privacy Enhancing Technologies: Current Regulatory and Policy Approaches," OECD Digital Economy Papers (OECD, 2023).

intelligence (AI) development. The introduced perspectives and interpretations on the technology and the concept of privacy contribute to a standardized and sound framework for synthetic data privacy assurance.

The remainder of this paper is structured as follows: in section 2, we provide an overview of the regulatory definition of anonymization, focusing on the GDPR. In particular, we provide an analysis of personal data, anonymous data, and the requirements on anonymization processes, including possible types of attacks they should protect against. In section 3, we use the developed legal theory to show that synthetic data generation from real data through generative artificial intelligence can serve as an anonymization technology if carried out correctly. In particular, we consider both scientific and regulatory evidence. In Section 4, we use the developed concepts to provide recommendations for proper deployment of synthetic data based on potential privacy hazards and open research topics.

2. The Concept of Anonymization

In this section, we provide an introduction to the concept of anonymization as also outlined in previous work.[2] Anonymization is the process of transforming personal data to ensure that individuals are no longer identifiable, either directly or indirectly, within a dataset. This technique is essential for safeguarding privacy in our increasingly data-centric world, aligning with regulations like the GDPR. By effectively removing or altering identifiable elements, anonymization protects against unauthorized access and misuse of personal information while still allowing for meaningful data analysis and utilization. Before exploring the various approaches to achieve anonymization, it is crucial to first understand the elements of personal data as defined by the GDPR.

2.1. Personal Data

The General Data Protection Regulation (GDPR)[3] defines personal data as "***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*".

This definition includes four key elements, as analyzed by López & Elbi[4]:

1. "**any information**": This term is comprehensive, encompassing all types of information about a person, regardless of its nature (objective or subjective) or the context in which the person acts (e.g., as a consumer, patient, employee). It covers a wide spectrum, from sensitive data to general information about private, family, or professional life.

[2] *Panfilo D., Boudewijn A. T., Ferraris A. F., Cocca V., Zinutti S., De Schepper K., & Chauvenet C. R.,* Measuring Privacy Protection in Structured Synthetic Datasets: A Survey, in: *Hideyuki Matsumi, Paul De Hert et al. (ed)*, Privacy and Data Protection: Ideas that Drive Our Digital World, 2024.

[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) (Text with EEA relevance), (GDPR) art. 4.1.

[4] *López C.A.F., Elbi A*., On The Legal Nature of Synthetic Data, NeurIPS 2022 Workshop on Synthetic Data for Empowering ML Research, 2022.

2. "**relating to**": Information relates to a person in three ways: through its content (specific data about an individual, like medical records), purpose (if it's used to evaluate or affect an individual's status or behavior), and result (if its use impacts the individual's rights and interests). These forms of relation contribute to an understanding at a population level rather than providing precise individualized information.
3. "**an identified or identifiable**": This focuses on the ability to distinguish a person within a group through identifiers, which may be direct (like a name) or indirect (like a unique combination of information). The protection extends to personal data regardless of the identification method.
4. "**natural person**": The protections cover all human beings, emphasizing the universal aspect of a "natural person" in alignment with human rights principles. It applies to living individuals who are identifiable or can be identified.

These components collectively ensure a consistent and comprehensive approach to data protection, balancing the broad scope of personal data with the need for identifiable linkage to an individual.

2.2. Anonymization and Anonymized Data

Anonymized data refers to information devoid of personally identifiable markers, ensuring no individual can be discerned either directly or through auxiliary data accessible to third parties. Properly anonymized data is exempt from data protection regulations like the GDPR since it ceases to be personal data. Such anonymization safeguards individual privacy against unlawful or unethical use.[5] Recital 26 of the GDPR delves deeper into personal data, further elucidating the concept of anonymization. It posits that anonymized data is "*information that does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a way that the data subject is not or no longer identifiable*."

The possibility of re-identification, or the process of transforming anonymized data back into personal data, is assessed based on its likelihood within a given dataset[6]. This might occur via data matching techniques or other similar methods. Recital 26 elucidates that to determine whether a person can be identified, one should take into account all the methods likely to be utilized, such as singling out, either by the controller or by another person.

"To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly."

The notion of "*reasonableness*" is crucial in this context, referring to the means used to identify the person, which may involve significant costs, time, and operations. The assessment should take into account the state of existing and available technologies at the time of data processing, as well as possible future developments.[6]

[5] *Foglia C.*, Il Dilemma (ancora aperto) dell'Anonimizzazione e il Ruolo della Pseudonimizzazione nel GDPR, in Circolazione e Protezione dei Dati Personali, tra Libertà e Regole del Mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al Novellato d.lgs. n. 196/2003 (Codice Privacy), 2019. *Stalla-Bourdillon S., Knight A.,* Anonymous Data v. Personal Data-False Debate: an EU Perspective on Anonymization, Pseudonymization and Personal Data, Wisconsin International Law Journal, 2017.

[6] *Tempestini L., D'Acquisto G.,* Il dato personale oggi tra le sfide dell'anonimizzazione e le tutele rafforzate dei dati sensibili,in Le nuove frontiere della privacy nelle tecnologie digitali, Aracne, 2016.

The principle of data protection does not apply to anonymized data if it is only possible to identify a person through unreasonably extensive means. Hence, the challenge in identifying an individual from anonymized data lies in the minimal presence of potentially identifiable elements.[7]

The Article 29 Working Party (WP29), in Opinion 4/2007, delved into the concept of personal data, concentrating on the "identified or identifiable" aspect of the definition[8]. The robustness of the anonymization process is measured by the ``means reasonably to be used'' test.

"To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."

The need for feasibility is particularly relevant in the context of statistical data. If even aggregated data, due to a small sample size or availability of other identifying information, potentially leads to identification, it underscores the inadequacy of the anonymization process.[9]

An effective anonymization strategy prevents any entity from isolating an individual in a dataset or linking two records within a dataset. Simply removing direct identifiers is insufficient to ensure anonymity.[11] It often necessitates additional measures, the nature of which depends on the context and purpose of the data processing. It is crucial to weigh the effort and cost of anonymization against the increasing technical capacity to identify individuals, the availability of public datasets, and instances of incomplete anonymization.[10][11]

The term "identifiable" extends to any entity in control of the data, not just the original data controller. If the controller retains the identifiable raw data and shares a modified version, it remains classified as personal data. Conversely, if the controller renders the data unidentifiable at an aggregate level and only shares these aggregate statistics, it is deemed anonymous data. When applying anonymization techniques, data controllers need to evaluate the level of guarantee provided by the selected method in relation to the current technological state.

2.3. Types of Privacy Leaks and Attacks

Three keycategories of attacksidentified by WP29 act as a benchmarkfor a proper anonymization, namely: Singling Out, Linkability, and Inference, as defined below.[12]

- **Singling Out**: Singling Out refers to the capability to isolate some or all records which identify an individual in a dataset. It suggests the ability to distinguish an individual in a group, even without precisely knowing who the individual is. It pertains to the distinctiveness of an individual's record, which might lead to identification.

[7] *D'Acquisto G., Naldi M.*, Big Data e Privacy by Design, Anonimizzazione, Pseudonimizzazione, Sicurezza, Giappichelli, 2017.
[8] *Article 29 Data Protection Working Party (WP29)*, Opinion 4/2007 on the Concept of Personal Data, 2007.
[9] *Information Commissioner's Office (ICO)*, Anonymisation: Managing Data Protection Risk Code of Practice, 2012.
[10] *Agencia Española de Protección de Datos (AEDP) and European Data Protection Supervisor (EDPS)*.
[11] Misunderstandingrelated to Anonymization, 2021, <https://www.edps.europa.eu/data-protection/our-work/publications/papers/aepd-edps-joint-paper-10-misunderstandings-related_en>[31.07.2024].
[12] Article 29 Data Protection Working Party (WP29). "Opinion 05/2014 on Anonymisation Techniques", 2014.

The singling out phenomenon was strikingly highlighted in the 1990s when an MIT student, Latanya Sweeney, successfully re-identified the supposedly anonymized health records of Massachusetts Governor William Weld.[13] She cross-referenced these records with public voter registration data, underscoring that ZIP code, birth date, and gender alone could uniquely identify a vast majority of the US population.

- **Linkability**: Linkability pertains to the ability to link at least two records concerning the same data subject or a group of data subjects from the same data set or two different data sets. This means that if different pieces of information, collected separately, can be linked together to possibly identify an individual, they are not effectively anonymized.

  Linkability surfaced prominently during the 2006 Netflix data breach. Anonymized customer data was intricately linked with public data from the Internet Movie Database (IMDb) by researchers Narayanan and Shmatikov. They managed to reverse the anonymity for users who had posted movie ratings under their names on IMDb, bringing to light how seemingly unrelated pieces of information could jeopardize data anonymization.
- **Attribute inference**: attribute inference refers to the ability to deduce, with significant probability, the value of an attribute from the values of a set of other attributes. In a legal context, it relates to the possibility of deducing unknown information about an individual from known information. Inference attacks can take advantage of statistical dependencies in the data to deduce sensitive information from non-sensitive information.

  It is interesting in this sense a 2014 case concerning the New York City Taxi and Limousine Commission's dataset as it illuminates the issue of inference.[14] The anonymized dataset contained extensive details of every taxi ride in the city. However, researchers could infer not only specific drivers' activities and earnings but also pinpoint individuals, including celebrities, demonstrating that even supposedly anonymized data could be vulnerable to inference attacks.

A robust anonymization procedure, thus, safeguards against the possibility of isolating individuals (singling out), associating records within or amongst datasets (linkability), and deducing information on specific individuals contained in the dataset (inference).[15] Simply eliminating overtly identifiable elements is inadequate; often, the processing context and purpose necessitate additional steps. Data protection laws apply as long as the identification or attribution remains possible, irrespective of the data controller or recipient's intentions.

Recent views of privacy classify attacks into two categories: identity disclosure and attribute inference.[16] These correspond roughly to singling out attacks and attribute inference attacks under the WP29 definition, respectively. The underlying intuition here is that upon successfully conducting an attack, the attacker must either have correctly identified an individual in a dataset (identity disclosure), or must have gained some information about a specific individual (parameter inference). In this light, linkability is a means to achieve one of these outcomes, but not a distinct attack category. Due to the abundance of information

[13] *Barth-Jones D.*, The 'Re-Identification' of Governor William Weld's Medical Information: A Critical Re-Examination of Health Data Identification Risks and Privacy Protections, Then and Now, 2012. *Narayanan A., Shmatikov V.*, How to Break Anonymity of the Netflix Prize Dataset (arXiv preprint cs/0610105), 2006.
[14] *Hern A.,* New York Taxi Details Can Be Extracted from Anonymised Data, Researchers Say, The Guardian, 2014.
[15] Article 29 Data Protection Working Party (WP29), "Opinion 05/2014 on Anonymisation Techniques", 2014.
[16] *Hu J., Bowen C.M.*, Advancing Microdata Privacy Protection: A Review of Synthetic Data, 2023.

available in the current digital world and the limited means needed to relate it to individuals[17] are at times raised as arguments supporting this perspective.[18]

3. Synthetic Data Generation as an Anonymization Technology

Following Jordon et al., we define the concept of synthetic data as follows:[19] *"Synthetic data (SD) is data that has been generated using a purpose-built mathematical model or algorithm (generator), with the aim of solving a (set of) data science task(s)."*

In the remainder, we restrict our analysis to *synthetic data generated through machine learning algorithms from original real-world data* (hereafter "synthetic data" or "SD"). This form of synthetic data has become the most discussed in application domains and the legal community.

In the remainder of this section, we outline why SD generation classifies as an anonymization technique as defined in Section 2. To this end, we first discuss computer scientific perspectives on the matter. We then discuss the dynamic and evolving legal landscape surrounding the technology. Finally, we discuss proper deployment conditions by considering potential risk factors and providing concrete deployment recommendations. Combined, these viewpoints not only show that SD can serve as an anonymization tool.

3.1. Scientific Perspectives

Anonymization and privacy protection are widely considered a core application of SD.[20] SD technology lends itself particularly well to this use case because it breaks the direct correspondence between data and real individuals. Legacy anonymization technologies rely on obscuring real data, for instance through randomization and generalization.[21] By contrast, SD generation proceeds by inferring a stochastic model of a given real dataset. This model captures the patterns of the real data in a probabilistic manner. Subsequently, this model can be sampled to generate new, entirely artificial records. Combined, a set of such artificial records exhibits the same patterns as the real dataset, since the underlying distribution is the same.

This process is best illustrated by a thought experiment.[22] Suppose one wants to create an artificial dataset that accurately represents the properties of some real population. Through research, the individual has knowledge of some properties of this population. For example, they know that the female to male ratio of the population is 1:1. Furthermore, they know that roughly one in six people have blue eyes, while the others have brown eyes. To create the data of an artificial person, they now do the following experiment: first, they flip a coin. If it lands on heads

(a chance of 1/2), they mark down "female". If it lands on tails, they mark down "male". Next, they roll a die. If it lands on the face with six eyes (a chance of 1/6), they mark down

[17] See, e.g., *De Montjoye Y. A., Hidalgo C. A., Verleysen M., & Blondel V. D.*, Unique in the Crowd: The Privacy Bounds of Human Mobility, Scientific Reports, 3(1), 2013, 1-5.
[18] *Beduschi A.*, Synthetic Data Protection: Towards a Paradigm Change in Data Regulation? *Big Data & Society*, 11(1), 2024.
[19] *Jordon J., Szpruch L., Houssiau F., Bottarelli M., Cherubin G., Maple C., Weller A.*, Synthetic Data-What, Why and How? 2022.
[20] Ibid.
[21] Article 29 Data Protection Working Party (WP29), "Opinion 05/2014 on Anonymisation Techniques", 2014.
[22] Thisthoughtexperiment was previously described in a blogpost, <https://aindo.com/blog/is-synthetic-good/> [30.07.2024].

"blue eyes". If it lands on any other face (1, 2, 3, 4 or 5, a chance of 5/6), they mark down "brown eyes". By repeating this experiment many times, the individual obtains an entirely synthetic population that has all the statistical and mathematical properties of the real population.[23] Yet, the records are generated by a series of probabilistic experiments, not by reference to real individuals.

Generative AI-based SD generation works in an analogous, but automated and more sophisticated manner. The thought experiment requires prior knowledge about the population (the distribution of male to female and of eye colors). When using generative AI, this is not a requirement: all relevant patterns are extracted directly from the data. Furthermore, generative AI-based generators accurately replicate correlations between attributes. In the thought experiment, for example, the overall proportion of blue-eyed individuals may be 1/6, but perhaps blue eyes are more common among females than males. A generative model could automatically infer and replicate this correlation. We refer the reader to Finocchiaro et al.[24] for an accessible overview of machine learning-based SD generation techniques.

The degrees of both privacy protection and realism of properly generated SD are widely recognized. The United States of America's National Institute for Standards and Technology (NIST) compared a multitude of de-identification algorithms.[25] Their results table[26] shows that SD generators excel at combining data utility with privacy protection. This empirical evidence for SD as a reliable anonymization tool is corroborated by the NeurIPS 2020 Hide-and-Seek Privacy challenge.[27][28] Submissions to the challenge demonstrated a privacy protecting SD algorithm (hiders), or a re-identification algorithm based on membership inference attacks (seekers). The challenge showed that only for a single (likely improperly synthesized) hider could any method re-identify significantly more than random guesses would.

3.2. Policy and Regulatory Perspectives

Like in the scientific community, SD generation as an anonymization process is gaining recognition in the legal scholarly community. In a seminal paper, Bellovin et al. state that:[29] *"Synthetic data offers progress. Though not a silver bullet, the method allows us to put an end to the de-identification–re-identification arms race and focus on what matters: useful, private data. To this extent, we recommend the privacy community accept synthetic data as a valid, next step to the database privacy problem."*

[23] By a theorem called "The Law of Large Numbers", see any introductory text on probability theory.

[24] *Finocchiaro G., Landi A., Polifronei G., Ruffo D., Torlontano F.*, Il Futuro Regolatorio Dei Dati Sintetici. La Sintetizzazione dei Dati Come Risorsa per Ricerca Scientifica, Innovazione e Politiche Pubbliche nel Panorama Giuridico Europeo, 2024.

[25] See: *Task C., Bhagat K., Howarth G.,* SDNist v2: DeidentifiedDataReport Tool, 2023, <https://data.nist.gov/od/id/mds2-2943> [30.07.2024].

[26] See NIST Collective Research Cycle (CRC), <https://pages.nist.gov/privacy_collaborative_research_cycle/pages/archive.html> [30.07.2024].

[27] *Jordon J., Jarrett D., Saveliev E., Yoon J., Elbers P., Thoral P., van der Schaar M.*, Hide-and-Seek Privacy Challenge: Synthetic Data Generation vs. Patient Re-Identification.

[28] Competition and Demonstration Track, 2021.

[29] *Bellovin Steven M., Dutta, Preetam K., Reitinger N.*, Privacy and Synthetic Datasets. *S*tanford Technology Law Review, Vol. 22, 2018.

This view is echoed in a more recent legal analysis by Finocchiaro et al., concluding that SD, if properly generated, constitute "*an advanced anonymisation technique that complies with current and future data protection regulatory requirements.*"[30]

Outside of the scholarly community, SD generation is gaining recognition as an anonymization process among policy-makers and even independent authorities. The Spanish Data Protection Agency (AEDP) explicitly recognizes that SD can be, at least under certain conditions, equated to anonymized data, suitable for personal data de-identification.[31] The Data Governance Act[32]and the Artificial Intelligence Act (AIA)[33] recognize SD generation as a privacy-preserving data processing method, equating it with anonymous or non-personal data. The European Union's *Joint Research Centre* (JRC) extends this acknowledgment, perceiving properly designed synthetic data not only as free of privacy-related risks but also as a strategic enabler in the domain of Artificial Intelligence.[34]

Lastly, interesting in France a law called the "Loi pour une République numérique" empowers the CNIL (Data Protection Authority in France) to validate and certify anonymization techniques. In 2020, the CNIL did use such power and certified a methodology for generating SD, affirming its anonymous nature based on criteria like individualization, linkability, and inference, thus acknowledging SD as (at least potentially equiparable to) anonymous data[35]. The CNIL even made a step further expressing interest in the development of a framework for empirically evaluating the degree to which specific synthetic datasets protect privacy[36] so as to be able to rely on quantitative and more objective analysis in validating different SD generation techniques.

4. Recommendations for Proper Deployment of Synthetic Data

In Section 3, we provided scientific and regulatory perspectives on SD generation as an anonymization technology. Throughout, we noted that SD generation serves as a strong tool in achieving anonymity, *provided that it is generated properly*. In this section, we analyze the notion of "proper generation" by studying sources of potential privacy risks, as well as some theoretical implications of SD generation. Throughout, we provide concrete recommendations to minimize risks. This fosters proper use of the technology, allowing resulting SD methods to achieve anonymization status.

[30] *Finocchiaro G., Landi A., Polifronei G., Ruffo D., Torlontano F.*, Il Futuro Regolatorio Dei Dati Sintetici. La Sintetizzazione dei Dati Come Risorsa per Ricerca Scientifica, Innovazione e Politiche Pubbliche nel Panorama Giuridico Europeo, 2024.

[31] Agencia Española de Protección de Datos (AEDP), "Approach To Data Spaces From GDPR Perspective", 2023.

[32] See Recital 7 of the Regulation (EU) 2022/868.

[33] See art. 10.5.a and art. 59.1.b of the Regulation (EU) 2024/1689.

[34] See *Hradec J., Craglia M., Di Leo M., De Nigris S., Ostlaender N., Nicholson N.,* Multipurpose Synthetic Population for Policy Applications, JRC Technical Report, 2022, 58-60.

[35] See Octopize's communication on the CNIL evaluation in the following presentation: <https://documentation-snds.health-data-hub.fr/files/presentations/meetup-snds7/20210318_Octopize_Deck-OctopizeHdhCom_MLP-2.0.pdf> [30.07.2024].

[36] SeeCNIL's Letterto Statice GmbH on Anonymeter, <https://www.anonos.com/hubfs/Documents/Reports/CNIL_Anonymeter.pdf> [30.07.2024].

4.1. Synthetic Data Risk Factors

Core risk factors are identified in our previous work,[37] namely: 1) the quality of the generator; 2) the approach to synthesis; 3) properties of the real dataset (presence of outliers, sparsity, etc.); 4) the information available to the attacker (threat model). These factors align closely to the caveats for SD technology identified by the European Data Protection Supervisor (EDPS)[38]. These risks can be evaluated and typically mitigated in practice by adopting a proactive and quantitative approach to privacy assessment. Worryingly, a recent literature study in the medical field found that while 85% (78/92) of papers include synthetic data for privacy use cases, only 42% of papers (39/92) use a privacy quantification method.[39] This shows that synthetic data privacy protection is not always quantified. Instead, it is presumed to offer sufficient protection by default, providing a false sense of security.

Recommendation: practitioners working with synthetic data should be aware of potential privacy risks. Moreover, they should use quantitative and objective methods to assess, evaluate and mitigate privacy risks. Our recent survey on privacy quantification[40] provides an in-depth discussion of such methods and their merits. In the remainder, we also present additional practical recommendations for the optimal use of these tools. We further recommend the use of fidelity and utility metrics to make sure that a good balance between privacy and utility is achieved.

4.2. SD-based and Generator-based Privacy

A fundamental question in SD technology is whether privacy protection is a property of SD (here after: "SD-based") or of the generator that produces the SD (hereafter: "generator-based"). These viewpoints affect how privacy is quantified in practice. To illustrate the different perspectives, consider the so-called "infinite monkey theorem".[41] This theorem roughly states that, given an infinite amount of time, a monkey randomly hitting keys on a typewriter will type the works of Shakespeare at some point. Similarly, it is easy to imagine a generator that, due to its stochasticity, produces a record (nearly) identical to a real individual's, without that real individual having been in its training set.[42] The question then arises: is this individual's privacy breached? Under SD-based privacy, the answer is "yes", as the synthetic dataset exposes the individual. Under generator-based privacy, the answer is

[37] *Panfilo D., Boudewijn A. T., Ferraris A. F., Cocca V., Zinutti S., De Schepper K., Chauvenet C.R.*, Measuring Privacy Protection in Structured Synthetic Datasets: A Survey, in: Hideyuki Matsumi, Paul De Hert et al. (ed) Privacy and Data Protection: Ideas that Drive Our Digital World, 2024.

[38] *Wiewiórowski W.*, Synthetic Data: What Use Cases as Privacy Enhancing Technology? IPEN Webinar on Synthetic Data, European Data Protection Supervisor.

[39] *Kaabachi B., Despraz J., Meurers T., Otte K., Halilovic M., Prasser F., Raisaro J. L.*, Can We Trust Synthetic Data in Medicine? A Scoping Review of Privacy and Utility Metrics, 2023.

[40] *Boudewijn A. T. P., Ferraris A. F., Panfilo D., Cocca V., Zinutti S., De Schepper K., Chauvenet C. R.*, Privacy Measurements in Tabular Synthetic Data: State of the Qrt and Future Research Directions, NeurIPS 2023 Workshop on Synthetic Data Generation with Generative AI, 2023.

[41] See most introductory texts on probability theory.

[42] Unlike the monkeys and Shakespeare, the generator will not *almost surely* generate the record of any given individual. This is because a generator models a specific distribution very accurately, unlike the uniform distribution over keys hit in the theorem. Thus, a generator does not necessarily generate all combinations of all possible attribute values given an infinite amount of time. Still, the scenario where a generator, due to stochasticity, produces a record overly similar to a real individual whose data was not in the training set is well within the realm of possibilities.

"no", since the production of the individual's data was not a consequence of the model's lack of protection of records in its training set.

The SD-based privacy viewpoint is more common in practice: a recent literature review on quantification of both utility and privacy in SD in medical contexts found that 81.2% of papers (18 out of 22) on SD using a privacy quantification approach are SD-based; only 9.1% (2 out of 22) are generator-based. The remaining 9.1% use a combination of both.[43] This popularity of SD-based privacy is likely due to two reasons. Firstly, the comparison with the infinite monkey theorem exposes a shortcoming of model-based privacy. Secondly, data-based privacy can be measured through metrics with clear real-world interpretations. In particular, these metrics typically quantify the likelihood that produced records are memorized from real ones; hazardous similarities between synthetic and real records; or the success rates of deliberately conducted attacks.[44]

Like SD-based privacy, generator-based privacy has several merits. Firstly, it is typically added to the generation process in an a priori, user-controlled manner. The most widespread examples are generalization control through early stopping and differential privacy,[45] with the user specifying a so-called *privacy budget*. Secondly, a number of *composition theorems* apply to differentially private systems, roughly stating that no further mathematical manipulation of a differentially private generator can remove its differentially private status. Recall that possible future developments should be taken into consideration when determining whether anonymization was successful. This makes the composition property particularly appealing. Shortcomings include that privacy budgets have no clear real-world interpretation and are hard to choose in practice.[46][47] Furthermore, the composition theorems apply to mathematical manipulation, not the use of compounding auxiliary information.

Recommendation: In light of the above discussion, we recommended employing a combination of data-based and generator-based methods. Data-based methods focus on the synthetic datasets produced, utilizing empirical privacy evaluations and similarity assessments to ensure that no identifiable information remains. Conversely, model-based techniques provide strong theoretical guarantees by embedding privacy mechanisms directly into the data generation process. These methods ensure that the generative models themselves do not expose individual data points. A combined approach maximizes the robustness of privacy protection, addressing both the model and the data perspectives.

4.3. "Relating to in Content" and Synthetic Data

López & Elbi argue that only access to information relating to an individual "in content" should be considered a breach.[48] This theoretical viewpoint seems evident in an applied setting, as aggregate statistics, such as those released by public institutions, can already relate

[43] *Kaabachi B., Despraz J., Meurers T., Otte K., Halilovic M., Prasser F., Raisaro J. L.*, Can We Trust Synthetic Data in Medicine? A Scoping Review of Privacy and Utility Metrics, 2023.

[44] For a thorough survey on both SD-based and generator-based quantification of privacy, see: *Boudewijn A. T. P., Ferraris A. F., Panfilo D., Cocca V., Zinutti S., De Schepper K., Chauvenet C. R.*, Privacy Measurements in Tabular Synthetic Data: State of the Qrt and Future Research Directions, NeurIPS 2023 Workshop on Synthetic Data Generation with Generative AI, 2023.

[45] *Dwork C., Roth A.,* The Algorithmic Foundations of Differential Privacy, Foundations and Trends in Theoretical Computer Science, 9(3-4), 2014, 211-407.

[46] *Lee J., Clifton C.*, How Much is Enough? Choosing for Differential Privacy.

[47] International Conference, ISC 2011, Proceedings 14, Springer Berlin Heidelberg, 2011, 325-340.

[48] *López C.A.F., Elbi A.*, On The Legal Nature of Synthetic Data, NeurIPS 2022 Workshop on Synthetic Data for Empowering ML Research, 2022.

to specific individuals "in purpose" and "in result". For instance, an overview of average incomes per region can lead to prejudice about individuals residing in a particular region.

Applying this viewpoint to SD, the question becomes whether access to SD allows attackers to infer knowledge pertaining to a specific individual. SD (and/or its generator) poses a privacy risk if its access leads to *specific information about* (i.e. relates to in content) a specific individual that could not have been inferred from mere general information. This is particularly relevant in the context of attribute inference attacks, as they deal with information attributable to an individual.

The Anonymeter framework by Giomi et al.[49] includes an implementation of an attribute inference attack that models the described notion of specificity and genericity. In particular, they compare the success rates of attribute inference attacks informed by SD to those of attribute inference attacks informed by a control group. The control group consists of real data that was not used for training the generator. If these success rates are comparable, then the information gained by SD access was generic in nature. If, on the other hand, significantly more can be deduced about a specific individual through SD than through the control set, this information relates to a specific individual in content and constitutes a privacy risk. A comparable approach to the use of control groups is also advocated in using distance-based privacy indicators.[50]

Recommendation: To refine the assessment of privacy (and risk of attribute inference attacks in particular), we recommend systematically including control groups of real data not used in the training of the generator. By doing so, researchers can more accurately determine whether the information derived from synthetic data is genuinely generic or if it improperly reveals specific individual details, posing a privacy risk.

4.4. Generator Training as a Form of Data Processing

While properly generated synthetic data (SD) is considered anonymous, the process of obtaining it involves training a generator using real data, classified under data protection laws as personal data processing. The United Kingdom's Information Commissioner's Office (ICO)[51]explicitly characterizes this training as such, emphasizing the need for stringent adherence to the legal framework.

In particular, SD generator needs to bear in mind from a regulatory perspective the following aspects:

- Legal Basis and Purpose: Data controllers must establish a clear and lawful basis for processing personal data, particularly when it involves sensitive categories such as health data (GDPR Article 6 and Article 9). The purpose of this processing should be explicitly defined and documented, aligning with the principle of purpose limitation.
- Data Protection Impact Assessment (DPIA): A DPIA is crucial when processing is likely to result in high risks to the rights and freedoms of natural persons (GDPR Article 35). This assessment should detail the data flows, evaluate the risks

[49] *Giomi M., Boenisch F., Wehmeyer C., Tasnádi B.*, A Unified Framework for Quantifying Privacy Risk in Synthetic Data, 2022.
[50] *Platzer M., Reutterer T.*, Holdout-Based Empirical Assessment of Mixed-Type Synthetic Data, Frontiers in Big Data, 2021.
[51] *Information Commissioner's Office (ICO)*, Anonymisation: Managing Data Protection Risk Code of Practice, 2012.

associated with the synthesis process, and describe measures to mitigate these risks. It should be noted that the DPIA is not a one-time requirement but should be revisited and updated to reflect changes in the processing activities or to address any data breaches or security issues that may have arisen.

- Technical and Organizational Measures: To ensure the integrity and confidentiality of personal data, GDPR Article 32 requires controllers to implement appropriate technical and organizational measures. This includes secure data handling practices, data minimization, and pseudonymization techniques during the training phase of the SD generator.
- Documentation and Compliance: Documentation should be kept to demonstrate compliance with GDPR requirements[52]. This includes maintaining records of processing activities under GDPR Article 30, detailing the purpose of processing, categories of data subjects and personal data, and the recipients of the data.
- Certifications and Standards Compliance: Adhering to recognized standards such as ISO/IEC 27001 and obtaining certifications like Europrivacy™/® can further evidence compliance with GDPR and enhance the trustworthiness of the anonymization processes. Europrivacy™/®[53] assesses compliance with GDPR and is managed by the European Centre for Certification and Privacy (ECCP), aligned with ISO/IEC 17065 and Article 42 of the GDPR.
- Ethical Considerations: Beyond legal compliance, ethical considerations should guide the synthesis of personal data. This involves ensuring that the synthetic data generation does not reproduce or exacerbate biases present in the original data sets, thereby upholding ethical standards and promoting fairness in data usage.
- Transparency and Accountability: GDPR emphasizes transparency and accountability. Data controllers should be transparent with data subjects about the use of their data for synthesizing SD and the measures in place to protect their privacy. This includes clear communication through privacy notices and public disclosures of DPIA summaries where appropriate.

Recommendation: Practitioners involved in synthetic data (SD) generation should establish a legal basis and define a clear purpose for anonymization, adhering to GDPR requirements. It is advisable to perform regular audits and continuous monitoring, along with updates to the Data Protection Impact Assessment (DPIA) to keep pace with technological and regulatory changes. The DPIA, mandatory under GDPR Article 35, should assess risks and outline mitigation strategies.

Furthermore, aligning SD practices with international standards such as ISO/IEC 27001 and obtaining certifications like Europrivacy™/® can enhance compliance credibility. Europrivacy™/®, recognized across EU and EEA Member States, evaluates GDPR compliance and is managed by the European Centre for Certification and Privacy (ECCP), adhering to ISO/IEC 17065 and Article 42 of the GDPR.

This approach promotes legal and ethical synthetic data use, supporting ongoing research and development while maintaining public trust.

[52] As provided by the Accountability principle ex art. 5.2 GDPR.

[53] See Aindo's entry in the Europrivacy/registry: <https://repository.europrivacy.org/en/certifications/edit/d9064da7-603a-4377-b596-b654824e365f> [30.07.2024].

5. Conclusion

As we navigate an era marked by exponential growth in data and escalating privacy concerns, synthetic data generation presents itself as a promising anonymization strategy. This paper has thoroughly evaluated synthetic data from multiple dimensions—legal, theoretical, and practical—highlighting its effectiveness as a privacy-enhancing technology (PET). Our analysis confirms that when produced correctly, synthetic data meets the strict anonymization criteria set forth by the General Data Protection Regulation (GDPR) and other related frameworks.

The need for transformation of data to a state where individuals are indistinguishable is critical, as traditional anonymization techniques increasingly fail to withstand sophisticated re-identification techniques. Synthetic data offers a contemporary solution by creating artificial datasets that reflect the statistical patterns of real data without any direct links to individual identities. This not only maintains privacy but also ensures the usability of data, proving essential for advancements in data science and artificial intelligence.

Regulatory recognition of synthetic data as a viable anonymization method is gaining momentum. Esteemed bodies such as the Spanish Data Protection Agency, the European Union's Joint Research Centre, and France's CNIL have endorsed the capability of synthetic data to fulfill anonymization standards. The endorsement is further strengthened by certifications like Europrivacy™/®, which attest to the adherence of synthetic data processes to GDPR and other regulatory stipulations.

However, the implementation of synthetic data generation demands careful consideration. It is crucial to rigorously assess factors like the quality of the generator, the methodology of synthesis, the characteristics of the source data, and the prevailing threat model. Employing quantitative methods to evaluate privacy and adopting a comprehensive approach that melds data-based and generator-based privacy strategies are vital to mitigate potential risks effectively. Additionally, the inclusion of control groups in empirical privacy assessments and adherence to data protection laws during the training of generators are imperative to uphold stringent compliance standards.

Looking forward, the field of data anonymization is set to evolve with advanced technological methods, rigorous legal regulations, and detailed empirical risk evaluations. This paper emphasizes the significant potential of synthetic data to adeptly address the complexities of data privacy in our digitally evolving landscape, contingent upon its strategic and cautious deployment.

Bibliography:

1. European Commission, "Regulation of the European Parliament and of the Council: on European Data Governance (Data Governance Act)".
2. European Commission, "Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (ARTIFICIAL INTELLIGENCE ACT) and Amending Certain Union Legislative Acts".
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) (Text with EEA relevance).
4. *Agencia Española de Protección de Datos (AEDP),* "Approach to Data Spaces from GDPR Perspective", 2023.
5. *Agencia Española de Protección de Datos (AEDP) and European Data Protection Supervisor (EDPS)*, 10 Misunderstanding related to Anonymization, 2021.
6. *Barth-Jones D.*, The 'Re-Identification' of Governor William Weld's Medical Information: A Critical Re-Examination of Health Data Identification Risks and Privacy Protections, Then and Now, 2012.
7. *Beduschi A.*, Synthetic Data Protection: Towards a Paradigm Change in Data Regulation? *Big Data & Society*, 11(1), 2024.
8. *Bellovin Steven M., Dutta, Preetam K., Reitinger N.*, Privacy and Synthetic Datasets, Stanford Technology Law Review, Vol. 22, 2018.
9. *D'Acquisto G., Naldi M.*, Big Data e Privacy by Design, Anonimizzazione, Pseudonimizzazione, Sicurezza, Giappichelli, 2017.
10. *De Montjoye Y. A., Hidalgo C. A., Verleysen M., Blondel V. D.*, Unique in the Crowd: The Privacy Bounds of Human Mobility, Scientific Reports, 3(1), 2013, 1-5.
11. *Dwork C., Roth A.,* The Algorithmic Foundations of Differential Privacy, Foundations and Trends in Theoretical Computer Science, 9(3–4), 2014, 211-407.
12. *Finocchiaro G., Landi A., Polifronei G., Ruffo D., Torlontano F.*, Il Futuro Regolatorio Dei Dati Sintetici. La Sintetizzazione dei Dati Come Risorsa per Ricerca Scientifica, Innovazione e Politiche Pubbliche nel Panorama Giuridico Europeo, 2024.
13. *Foglia C.*, Il Dilemma (ancora aperto) dell'Anonimizzazione e il Ruolo della Pseudonimizzazione nel GDPR, in Circolazione e Protezione dei Dati Personali, tra Libertà e Regole del Mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al Novellato d.lgs. n. 196/2003 (Codice Privacy), 2019.
14. *Giomi M., Boenisch F., Wehmeyer C., Tasnádi B.*, A Unified Framework for Quantifying Privacy Risk in Synthetic Data, 2022.
15. *Hern A.,* New York Taxi Details Can Be Extracted from Anonymised Data, Researchers Say, The Guardian, 2014.
16. *Hradec J., Craglia M., Di Leo M., De Nigris S., Ostlaender N., Nicholson N.*, Multipurpose Synthetic Population for Policy Applications, JRC Technical Report, 2022.
17. *Hu J., Bowen C.M.*, Advancing Microdata Privacy Protection: A Review of Synthetic Data, 2023.
18. *Information Commissioner's Office (ICO),* "Anonymisation: Managing Data Protection Risk Code of Practice", 2012.

19. *Jordon J., Jarrett D., Saveliev E., Yoon J., Elbers P., Thoral P., van der Schaar M.*, Hide-and-Seek Privacy Challenge: Synthetic Data Generation vs. Patient Re-Identification, In NeurIPS 2020 Competition and Demonstration Track, 2021.
20. *Jordon J., Szpruch L., Houssiau F., Bottarelli M., Cherubin G., Maple C., Weller A.*, Synthetic Data-What, Why and How? 2022.
21. *Kaabachi B., Despraz J., Meurers T., Otte K., Halilovic M., Prasser F., Raisaro J. L.*, Can We Trust Synthetic Data in Medicine? A Scoping Review of Privacy and Utility Metrics, 2023.
22. *Lee J., Clifton C.*, How Much is Enough? Choosing ε for Differential Privacy, In Information Security: 14th International Conference, ISC 2011, Proceedings 14, Springer Berlin Heidelberg, 2011, 325-340.
23. *López C.A.F., Elbi A.*, On The Legal Nature of Synthetic Data, NeurIPS 2022 Workshop on Synthetic Data for Empowering ML Research, 2022.
24. *Narayanan A., Shmatikov V.*, How to Break Anonymity of the Netflix Prize Dataset, 2006.
25. *OECD*, "Emerging Privacy Enhancing Technologies: Current Regulatory and Policy Approaches," OECD Digital Economy Papers (OECD, 2023).
26. *Panfilo D., Boudewijn A. T., Ferraris A. F., Cocca V., Zinutti S., De Schepper K., Chauvenet C. R.*, Measuring Privacy Protection in Structured Synthetic Datasets: A Survey, in: Hideyuki Matsumi, Paul De Hert et al. (ed) Privacy and Data Protection: Ideas that Drive Our Digital World, 2024.
27. *Platzer M., Reutterer T.*, Holdout-Based Empirical Assessment of Mixed-Type Synthetic Data, Frontiers in Big Data, 4, 2021.
28. *Stalla-Bourdillon S., Knight A.,* Anonymous Data v. Personal Data-False Debate: an EU Perspective on Anonymization, Pseudonymization and Personal Data, Wisconsin International Law Journal, 2017.
29. *Task C., Bhagat K., Howarth G.,* SDNist v2: Deidentified Data Report Tool, 2023, <https://data.nist.gov/od/id/mds2-2943> [30.07.2024].
30. *Tempestini L., D'Acquisto G.,* Il dato personale oggi tra le sfide dell'anonimizzazione e le tutele rafforzate dei dati sensibili, in Le nuove frontiere della privacy nelle tecnologie digitali, Aracne, 2016.
31. *Wiewiórowski W.*, Synthetic Data: What Use Cases as Privacy Enhancing Technology? IPEN Webinar on synthetic data, European Data Protection Supervisor.

Ekaterine Shengelia*
Irakli Leonidze**

Notary Electronic Registry and Data Security

Starting from March 1, 2024, with the implementation of the Law of Georgia "On Personal Data Protection," the updated regulations governing database management and security have gained particular significance. Legislative and institutional developments emphasize the necessity of examining the operation of the notary electronic registry to determine the obligations of notaries in relation to personal data processing, as well as the potential legal consequences of breaches in data security.

Keywords: *Personal Data Protection Service, notary electronic registry, Notary Chamber of Georgia, notary, data security.*

1. Introduction

The new Law of Georgia "On Personal Data Protection" has established a significant legal framework for data protection in Georgia, aligning with the European Union's General Data Protection Regulation (GDPR). This framework ensures the protection of fundamental human rights and freedoms, including the rights to privacy, personal space, and communication, during the processing of personal data.[1]

As a public law entity, the Notary Chamber of Georgia —an association of notaries operating on the principle of self-governance and based on mandatory notary membership[2]—has assumed a central role in these legal innovations. Given that the notary electronic registry enables the Notary Chamber and individual notaries to process personal data for specific purposes, it is considered an integral component of notarial services and must adhere to data security requirements.

The purpose of this study is to assess the conditions under which the personal data of individuals are processed within the notary electronic registry, evaluate its compliance with the provisions of the Law of Georgia "On Personal Data Protection," and examine the innovations implemented in notary registries by member states of the Council of Notaries of the European Union.

---

* Associate Professor of the Law Faculty of Ivane Javakhishvili Tbilisi State University, Doctor of Law, Director of the Scientific Research Institute of Notary Law, Notary of Georgia.

** PhD student of Ivane Javakhishvili Tbilisi State University Faculty of Law, Researcher-analyst of the International Relations, Analytics and Strategic Development Department of the Personal Data Protection Service.

[1] Law of Georgia "On Personal Data Protection", 14/06/2023, Article 1. Also, see Bernstorff N., European Union "Data Protection Law", Journal of Personal Data Protection Law, No. 2, 2023, 14-15.

[2] Law of Georgia on Notaries 04/12/2009, Article 4.

2. Types of Notary Electronic Registry

A notary is required to maintain a notarial registry, in which all notarial acts performed are recorded.[3] This registry serves as a database of the personal data of individuals receiving notarial services and includes both open and closed internal systems[4]. In the course of their professional duties, a notary processes personal data in accordance with the principles and legal grounds of data processing, including the handling of special categories of data and personal data of minors.

The function of the open internal system allows notaries to access data related to entities involved in notarial activities. All notaries have access to the notarial acts registered therein, regardless of which notary performed the act, including:

- The registry of inheritance matters;
- The registry of wills;
- Information on the enforcement sheets from the general register.

The openness of the registry of inheritance matters is necessary to prevent two different notaries from issuing inheritance certificates of similar content for the same estate. A notary cannot open the estate to legal heirs if the will of the heir is already held by another notary. Additionally, multiple writs of identical content cannot be issued for real estate, among other things.

Conversely, access to the closed internal system is restricted solely to the notary who performed the act recorded in the register. This system includes:

- The general registry, which records all notarial acts, except for those mentioned above;
- The registry of objections to promissory notes and checks;
- The registry of money and securities;
- The registry of resolutions.

A key issue under discussion is in which form the data stored in the open internal system should be made available to other notaries and public institutions beyond the scope of notarial activities, such as the public registry. On the one hand, the notary is bound by a duty of professional secrecy; on the other hand, certain actions and results of the notary's work are accessible to fellow notaries and individuals connected with the registry. For instance, a notary public, another person who authenticated the will, a witness, or individuals who signed the will on behalf of the testator are prohibited from disclosing information related to the will's content, its preparation, modification, or revocation before the opening of the estate[5]. However, this information/personal data may be stored electronically. Registration in the notary registry can reveal the existence and content of a will and potentially expose it to other individuals.

Article 27 of the Law of Georgia "On Personal Data Protection" sets forth data security requirements. These requirements are conditional in nature and underscore the importance of data protection. However, the enforcement of these conditions and the legal

[3] Compere: European Commission for the Efficiency of Justice, Working Group on the Evaluation of Judicial Systems, Specific Study of the CEPEJ on the Legal Professions: Notaries – 2018, Notaries of Europe (CNUE),

[4] Order of the Minister of Justice of Georgia "On approval of the instruction on the procedure for performing notarial acts", 31/03/2010, Article 33.

[5] Civil Code of Georgia, 26/06/1997, Article 1363.

consequences of data insecurity during notarial activities are marked by certain distinct characteristics. Notably, the updated regulations on data security highlight the mechanisms for responding to data breaches and the obligation to appoint a data protection officer.[6]

Under the new law, the data controller and the data processor are required to ensure that all actions performed on data are recorded in electronic form. This includes information on incidents, data collection, modification, access, disclosure (transfer), connection, and deletion. When data is processed in non-electronic form, the controller and processor must record all actions related to the disclosure and/or alteration of data, including incidents.[7] In the context of the notary registry, this requirement pertains both to the overall responsibility for the systematic operation of the register and specifically to the performance of notarial activities.[8]

When recording a notarial act in the notary registry, it is mandatory to provide the following data:

- The date and registration number of the notarial act;
- The name, surname, place of residence, and personal identification number of the participant in the notarial act. For a minor without an identity document, the name, surname, and date of birth are recorded. For a legal entity, the name, legal address, and identification code (for resident legal entities) must be included. For other organizational formations, the name and location are required.
- The content of the notarial act;
- The notary fee.

In inheritance proceedings, the heir's name, date of death, and identification data are also required. For the registration of a protocol regarding the publication of a will, the content of the testamentary decree, identification data of the heir or alternate heir, the name and surname of the executor named in the will, their place of residence, other identification data, as well as the name and surname of the person entrusted with appointing the executor, and information on the legatee (if applicable) are to be provided.

As observed, the indication of personal data is essential for registering an action in the notary register, yet a different standard of notarial responsibility applies to public and private deeds. This raises the question of whether a similar regulatory approach can be applied to data protection requirements. On one hand, there are legal consequences related to the breach of notarial professional secrecy or violations of notarial law, while on the other, there are legal consequences arising from violations of data security.

It is possible that a data security breach may result from the actions of data subjects, their representatives, other notaries, or employees of public institutions outside the notarial sphere. Alternatively, such breaches could fall within the scope of the notary's professional responsibility. For example, if details of a notarial act are disclosed to another public institution, data security is compromised. In this case, the notary follows notarial legislation, thereby linking data security issues to notarial activities, particularly with respect to the

[6] Regarding the development of databases, see: 2022 report on the activities of the Personal Data Protection Service, 96; 2023 report on the activities of the Personal Data Protection Service, 52-53.

[7] Law of Georgia "On Personal Data Protection", 14/06/2023, Article 27, Paragraph 4. Also, incl. *Wudarski A., Sirdadze L.,* Registry jungle in the 21st century, Georgian-German Journal of Comparative Law, No. 6, 2020, 22

[8] See Recommendations of the Personal Data Protection Service for Public Institutions on Issuing/Updating Interdepartmental Legal Acts for Compatibility with the Law of Georgia "On Personal Data Protection", 2023, 1-2.

handling of public and private deeds.[9] This underscores the need for establishing a uniform standard for data security.

Regardless of whether a public or private deed is involved, the notary must adhere to the general rule of ensuring data security. However, if the notary register does not allow for the application of a common standard to both public and private deeds, how should the notary proceed in such instances?

The notary is not liable for the non-compliance of a private deed with the law or for failing to adequately reflect the will of the signatory in a private deed.[10] A notary (or substitute) commits a serious disciplinary offense if they breach the obligation of professional secrecy, except for cases provided under subsection "b" of Article 7[11] of the Disciplinary Statute. This statute stipulates that a violation of professional secrecy that results in serious consequences is considered a particularly serious disciplinary offense. Consequently, a violation of data security rules by a notary may not necessarily result in professional liability, which is a natural outcome of the legal framework.

It is also important to note that public institutions were directed to align the terms related to data processing in their sub-legal normative acts and individual legal acts with the new Law of Georgia "On Personal Data Protection" by the time of its implementation[12]. From June 1, 2024, the law came into full effect.

3. Production of Notary Electronic Registry and Data Security

A notarial act that is not registered in the notary registry is deemed invalid, except in certain exceptional cases provided by law[13]. Each notarial act is assigned a unique number and is registered after the notary has signed and sealed the document[14]. The entry in the notary registry is made by the notary or an employee of the notary bureau acting on their behalf, who is contractually bound to maintain the confidentiality of the notarial act. This obligation also applies to a substitute notary public.[15]

When a notarial act is registered in the notary registry, it must be accompanied by an electronic copy of the notarial deed.[16]

The administration and technical supervision of the notary electronic registry is overseen by the Notary Chamber of Georgia. In accordance with the agreement signed with the Chamber, those responsible for the administration and technical supervision of the notary

[9] Order of the Minister of Justice of Georgia "On approval of the instruction on the procedure for performing notarial actions", 31/03/2010, Article 15.

[10] Order of the Minister of Justice of Georgia "On approval of the instruction on the procedure for performing notarial actions", 31/03/2010, Article 15.

[11] see Order No. 69 of the Minister of Justice of Georgia "On the approval of the regulation "On Disciplinary Responsibility of Notaries", 31/03/2010

[12] Guidelines of the Personal Data Protection Service, recommendations for public institutions on issuing/updating intra-departmental legal acts for compatibility with the Law of Georgia "On Personal Data Protection", 2023, 2.

[13] See *Kharitonashvili N.,* Conference "Digitalization of German and Georgian Notary", Georgian-German Journal of Comparative Law, No. 4, 2023, 88-89.

[14] Compere: European Judicial Systems Efficiency and Quality of Justice, Specific Study of the CEPEJ, Council of Europe, №26, 2018, 220.

[15] Law of Georgia on Notaries, 04/12/2009, Article 24.

[16] Compere: *Kharitonashvili N.,* Digitization of the Georgian Notary, Georgian-German Journal of Comparative Law, No. 6, 2023, 149.

registry are obligated to maintain the confidentiality of any information obtained during the data processing. Therefore, they are accountable for any breaches of notarial secrecy.[17]

In comparison, the Belgian Data Protection Supervisory Authority, in a specific case, emphasized that a notary, as the data controller, mistakenly sending personal data to the email address of unintended recipients and then attempting to recall the messages, constitutes a data security breach. This was considered a violation of data security rather than a technical flaw in data processing.[18]

A notary or a substitute notary must apply to the Notary Chamber of Georgia for authorization to access the notary register. The Notary Chamber of Georgia is responsible for issuing, suspending, or terminating the authorization for access to the notary register when a notary's authority is suspended or terminated. The Chamber ensures the security and protection of the data in the notary register, including the training of notaries (and their substitutes) as well as their hired employees on the proper use of the notary register. It also approves the technical instructions for the operation of the notary register[19]. While this is a legal requirement, in practice, its implementation may vary. The Notary Chamber of Georgia and notaries, in cooperation with one another and depending on specific cases, can be considered as joint controllers[20], data controllers, or data processors, depending on how the purposes and grounds of data processing are determined by these entities or individuals. It is also important to note that, generally, a notary is the data controller. However, in smaller cases, the notary may assume the status of a data processor in relation to the Notary Chamber of Georgia or another public institution. For instance, under the agreement between a notary and the National Public Registry Agency, the notary is assigned the role of data processor, while the public registry serves as the data controller. In such cases, the notary, as a data processor, is responsible for processing personal data only within the limits prescribed by the agreement and the law.

As for the notary register, the notary manages it under their own name and independently processes the personal data of individuals within the register. Therefore, in relation to the notary register, the notary is the data controller.

Substitute notaries, notaries employed under an employment contract, and notary assistants are in an employment relationship with the notary and thus are not considered data processors, as the data processor should not be in an employment relationship with the data controller[21]. These individuals are not data controllers themselves but play a crucial role in ensuring the continuity of notarial activities and form part of the staff of the notarial office[22]. In this context, the notary holds the leading status within the notarial bureau.

For comparison, the Polish Data Protection Supervisory Authority has clarified that a notary may act as a data processor when performing notarial duties if they have signed an

[17] See: Recommendation of the Personal Data Protection Service "On the Principles of Personal Data Processing", 2024, 29; Recommendation of the Personal Data Protection Service "On the implementation of measures related to the incident", 2024, 5-6.

[18] Case of the Data Protection Authority (Belgium) №52, 03/04/2024.

[19] Compere: *Asvanua N.,* Personal data protection mechanisms, Tb., 2023, 39-40.

[20] Compere: *Kuner C., Bygrave L. A., Docksey C.,* the EU General Data Protection Regulation (GDPR) – a Commentary, Oxford University Press, Oxford, 2020, 25-27.

[21] Law of Georgia "On Personal Data Protection", 14/06/2023, Article 3.

[22] Compere: European Commission for the Efficiency of Justice, Study on the Functioning of Judicial Systems in the EU Member States, Specific Study on the Facts and Figures from the CEPEJ Questionnaires 2012 to 2020, Strasbourg, 2022, 899-900.

agreement with the data controller in accordance with Article 28 of the EU General Data Protection Regulation (GDPR).[23]

Under the new Law of Georgia "On Personal Data Protection," the Notary Chamber of Georgia, as a public institution, is obliged to appoint a data protection officer[24]. According to Article 27(a) of the General Administrative Code of Georgia, an administrative body is defined as a public institution, which includes any legal entity of private law that is financed by state or municipal budget funds. In the context of this provision, an administrative body also refers to any state or municipal institution, legal entity under public law (excluding political or religious organizations), or any other entity exercising public legal powers based on Georgian legislation. Consequently, the Notary Chamber of Georgia, as a legal entity under public law, is considered a public institution, and there is no ambiguity regarding its obligation to appoint a data protection officer. In contrast, a notary, under a literal interpretation of these provisions, cannot be considered a public institution, although they exercise state authority.

It should be noted that under the Law of Georgia "On Personal Data Protection," a data controller or data processor who processes the data of a large number of individuals or systematically and extensively monitors their behavior is obligated to appoint a data protection officer. This obligation, however, does not apply if the entity processes the personal data of no more than 3 percent of the population of Georgia, based on the most recent national census. Given the general statistical data, an individual notary is unlikely to process the personal data of more than 3 percent of Georgia's population within a reporting year. Therefore, under this condition, a notary is not required to appoint a data protection officer. However, this does not exclude the possibility that, depending on changes in the quantitative criteria or legal norms, the requirement for a notary to appoint a data protection officer may arise in the future.

From the perspective of data security, the data controller is required to implement appropriate technical and organizational measures to ensure that data processing complies with the law, and must be able to demonstrate the legality of such processing[25]. Therefore, as previously mentioned, there is currently no requirement for a notary office to have a designated data protection officer, as it is feasible for the general administration of this matter to be handled within the organizational framework of the Notary Chamber of Georgia.

The following entities are involved with the notary electronic registry:

- The Notary Chamber of Georgia;
- Individuals contracted by the Chamber for the management of the register;
- The Chamber's personal data protection officer;
- Notaries;
- Substitutes for notaries;
- Notaries employed under employment contracts;
- Notary assistants.

It is essential to define the status and obligations of each of these parties in every specific case, in accordance with the Law of Georgia "On Personal Data Protection,"

[23] Case of the Data Protection Authority (Poland) №DKN.5131.31.2021, 07.02.2023.

[24] See Guidelines of the Personal Data Protection Service, recommendations for public institutions on issuing/updating intra-departmental legal acts in order to be compatible with the Law of Georgia "On Personal Data Protection", 2023, 14.

[25] Law of Georgia "On Personal Data Protection", 14/06/2023, first paragraph.

specifically determining who may be classified as a data controller, data processor, or joint controller.[26]

For comparison, the Spanish Data Protection Supervisory Authority found in a particular case that a notary had failed to inform an individual about the purpose of processing identification data and the data security measures applied during the execution of the notarial act. The notary argued that notarial legislation did not impose such an obligation. However, the supervisory authority cautioned the notary on the necessity of providing this information to the data subject when collecting data directly, irrespective of whether notarial legislation mandates such disclosure.[27]

Notarial legislation governs the professional conduct of notaries, but the issue of data security is regulated externally and influences notarial activity. This introduces new roles or statuses for notaries in the realm of data processing.[28]

Any employee of the data controller, as well as the processor, who participates in data processing or has access to data, is obliged to adhere strictly to the scope of authority granted to them and to protect the secrecy and confidentiality of the data[29]. This obligation extends even after the termination of their official authority. Controllers and processors are mandated to define the scope of access to their data in accordance with the employees' powers. They must implement adequate measures to prevent, detect, and address instances of illegal data processing by employees. This includes ensuring that employees are informed about data security protection issues.[30] It is also pertinent to highlight the technical instructions that may impose obligations on specific individuals or grant them authority regarding the management of the registry. Despite the fact that notaries perform state activities independently within their own notary bureaus, the data related to their actions, as well as the personal data of citizens, are collected in the notary electronic registry. Therefore, irrespective of how diligently an individual notary complies with data protection legislation, this alone will not suffice to guarantee data security.

In a comparative analysis, in one case involving a data security breach, the Italian Data Protection Supervisory Authority was approached by the Italian Chamber of Notaries. They requested an examination of the status, obligations, and responsibilities of commercial banks and notaries concerning the processing of data related to the credit obligations of individuals within the electronic register. The supervisory authority determined that the provider of the electronic registry (data controller) was liable for the data security violation, having arbitrarily notified and processed the data contained in the aforementioned registry without proper notification to the controller.[31]

The notary is obligated to protect the data related to access to the notary register[32]. All individuals who have been granted the right to enter the notary register for various legal

[26] Compere: *Elizbarashvili S.,* Protection of human rights in the era of technological development: the beginning of regulation of artificial intelligence, collection of articles - Protection of human rights: European experience and national challenges, Tb., 2023, 80-81.

[27] Case of the Data Protection Authority (Spain) №PS/00044, 23/10/2020.

[28] See: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), 28/01/1981; General Data Protection Regulation (GDPR), 27/04/2016; Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108+), 18/06/2018.

[29] Law of Georgia "On Personal Data Protection", 14/06/2023, Article 27, Paragraph 5.

[30] Law of Georgia "On Personal Data Protection", 14/06/2023, Article 27, Paragraph 6.

[31] Case of the Data Protection Authority (Italy) №9993548, 11/01/2024.

[32] Compere: *Khubua G., Sirdadze L.,* Law technologies (legaltech) in Georgia, their use in private companies and public agencies, Georgian-German Journal of Comparative Law, No. 7, 2022, 10.

reasons are required to maintain the confidentiality of information regarding notarial activities[33]. This obligation remains in effect even after these individuals lose their right to access the notary register.[34]

The data controller, along with data processor, is required to implement organizational and technical measures that correspond to the potential and associated threats of data processing. These measures must ensure data protection against loss, illegal processing, and include destruction, deletion, modification, disclosure, or unauthorized use[35]. To preserve the informational integrity of the notary electronic registry, it is essential to systematize its management and functions.

In a comparative case, the Belgian Data Protection Supervisory Authority observed that personal data processed during notarial activities and stored in the notary registry cannot be transferred to the registering authority (another public institution) unless such transfer is based on the wishes of the data subject[36]. Otherwise, the notary would not only be in violation of data protection legislation but would also breach ethical obligations.

When determining the necessary organizational and technical measures to ensure data security, the controller and processor are obliged to consider the categories of data, volume, and purpose of data processing, form, means, and potential threats to the rights of the data subject. They must also periodically evaluate the effectiveness of the technical and organizational measures taken to ensure data security and, if necessary, implement adequate measures to safeguard data security and/or update existing measures.[37]

It can be stated that the current system of the notary electronic registry does not adequately account for advancements in modern information technologies, including automated individual decision-making and profiling[38]. Despite its electronic nature, the system cannot fully facilitate the drafting of a notarial deed without the active participation of a notary public in the process. Therefore, it is crucial to develop the necessary functions for automatic processing within the notary electronic registry to ensure the legality and correctness of citizens' data processing when obtaining notarial services.

4. Updates on Notary Electronic Registry in Member States of the Council of Notaries of the European Union

The Council of Notaries of the European Union is comprised of representatives from the Notary Chamber of Georgia of 22 member countries. In 2024, the Notary Chamber of Georgia joined the Council of Notaries of the European Union as an observer. Among the primary objectives of the member states of the Council of Notaries of the European Union is the enhancement of notarial databases for automatic data processing and the integration of updated information technologies and artificial intelligence.[39]

[33] Compere*: Peterfalvi A., Esther D.,* When Our Machines Learn Us: European Union Efforts to Regulate AI-Based Decision-Making and Profiling, Journal of Personal Data Protection Law, No. 1, 2023, 72-74.

[34] According to the opinion of the Advocate General of the Court of Justice of the European Union, the supervisory authority is obliged to act immediately upon discovering the fact (incident) of a breach of personal data security, the case "TR v Land Hessen", <https://pdps.ge/ka/content/1068/-Datanewsroom> [14.05.2024].

[35] Law of Georgia "On Personal Data Protection", 14/06/2023, Article 27, Paragraph 2.

[36] Case of the Data Protection Authority (Belgium) №48, 08/04/2021.

[37] Law of Georgia "On Personal Data Protection", 14/06/2023, Article 27, Paragraph 3.

[38] Recommendation of the Personal Data Protection Service "On rights and profiling related to automated individual decision-making", 2024, 4-6.

[39] European Commission for the Efficiency of Justice, Working Group on the Evaluation of Judicial Systems, Specific Study of the CEPEJ on the Legal Professions: Notaries – 2018, Notaries of Europe (CNUE), 7-10.

In Italy, an electronic model of the notarial deed has been in place since 2013, eliminating the need for a printed counterpart. Users input their personal data into the notary electronic registry template, which then generates an electronic document of the notarial deed. This document is reviewed by the on-duty notary, who is selected by the user from within the system. The service is noted for its speed and reliability.[40]

The Czech notary registry is integrated with the court register, allowing notaries public access to both the notarial and judicial stages of the review process for user applications and their accompanying documents. This shared access is facilitated by the delegation of certain functions to notaries. In the context of probate proceedings, both notarial and judicial actions are conducted electronically, with only the final outcome being printed. Through this delegation of authority, the notary is granted access to data stored in the court database and is permitted to process it based on predetermined criteria.[41]

In Austria, since 2000, there has been an electronic working document that is integrated with the notary registry system and includes an archiving function. The notary can execute any notarial act within this document, and once the notarial act is completed, the notarial deed is automatically recorded in the performed actions field. The system is characterized by its high capacity, security, and flexible sharing functionality, enabling the notary to efficiently manage both current and archived notarial acts.[42]

Since 2014, Romania has implemented an electronic platform that combines various types of notary registers. The management of these registers is overseen by the Center for the Management of Notary registries. This application-based system allows for the real-time generation of documents, requiring the input of the user's personal data, the content, and the notary involved.[43]

The Belgian Notary has developed an electronic platform for public real estate auctions, allowing users to participate in auctions from their homes. Through this system, the notary reviews the auction results and prepares a notarial deed, which enables the auction winner to request property registration. Furthermore, the Belgian Notary has established a citizen-oriented communication system, allowing users to submit inquiries, with notaries responding in real time to users' questions and carrying out notarial actions as requested.[44]

All notaries in Estonia, Lithuania, and Latvia utilize an electronic information system characterized by robust security mechanisms and a cross-border functionality among the notary offices of these three countries. This system provides open access to the notaries of the mentioned countries and integrates the registers that establish rights.[45]

The German Notary has developed an innovative system for the registration of limited liability companies, allowing the notary to create an electronic form by inputting the data of the interested parties. Based on the frequency of receiving these services, the platform

[40] *Chiarini A., Forte A.,* Excellence in Notary Services through ISO 9001 Certification: an Investigation from Italy, Huelva, 2016, 124-125.

[41] European Commission for the Efficiency of Justice, Working Group on the Evaluation of Judicial Systems, Specific Study of the CEPEJ on the Legal Professions: Notaries – 2018, Notaries of Europe (CNUE), 10

[42] *Hall E. G.,* The Common Law and Civil Law Notary in the European Union: a Shared Heritage and a Influential Future, London, 2015, 15.

[43] *Ruggeri L., Kunda I.,* Winkler S. (eds.), Family Property and Succession in EU Member States National Reports on the Collected Data, The European Commission, 2019.

[44] *Verboven F., Yontcheva B*., Private Monopoly and Restricted Entry - Evidence from the Notary Profession, 2022, 7.

[45] *Parsova V*., Gurskiene V., Kaing M., Real Property Cadastre in Baltic Countries, Jelgava, 2012, 158.

features an archiving function and is actively updated in accordance with both current and archived actions.[46]

The foremost requirement for modern notaries in the member states of the Council of Notaries of the European Union is the digitization of notarial acts; consequently, notary registries are now, to varying degrees, digitized. For instance, countries such as Austria, Belgium, Croatia, the Czech Republic, Estonia, France, Germany, Hungary, Latvia, Luxembourg, Malta, the Netherlands, Poland, and Romania maintain registers of wills and successions linked to the European Union's succession register. This system provides notaries in member states with information about inheritances issued in specific jurisdictions. A secondary consideration is the form in which the notarial deed is accessible in the said register. A notarial deed recorded in the electronic database must, in individual cases, be accompanied by either the notary's signature and seal or solely by electronic details (a unique code), without a physical signature.[47]

The Notary Chamber of Georgia has signed a memorandum of cooperation with the Federal Chamber of Notaries of Germany. This memorandum aims to enhance and develop notarial services through mutual cooperation between the Notary Chamber of Georgia and Germany. It ensures the exchange of experiences in the field of notarial information technology[48], emphasizing that this sharing of experience extends beyond theoretical learning to provide customized electronic services to users.[49]

5. Conclusion

Notaries maintain active contact with data subjects. The foundations of a notary's professional activity are grounded in the Constitution of Georgia, the law of Georgia on notaries, the Order of the Minister of Justice of Georgia "On Approving the Instruction on the Procedure for Notarial Acts," and other normative acts. The processing of personal data of individuals receiving notarial services is governed by the Law of Georgia "On Personal Data Protection."

It is crucial to establish the status of individuals with access to the notary electronic registry, as well as the fundamental standards of data security protection within the framework of access to both open and closed internal systems. These standards should address the status of both individuals with access to the registry and those without, outlining their duties and regulating their actions in accordance with data protection legislation.

Research has underscored the special significance of the functioning of the notary electronic registry and the necessity for its refinement, taking into account the requirements of the Law of Georgia "On Personal Data Protection," the development of user-adapted electronic services, and the practices of the member states of the Council of Notaries of the European Union. It is advisable that the notary electronic registry, when performing notarial activities, incorporates appropriate data security standards to facilitate automated individual decision-making. This enhancement would assist notaries in managing citizens' appeals and in drafting notarial deeds.

[46] *Rinne T.*, A Guide to Corporate Forms for Doing Business in Germany, Hamburg, 2017, 23.
[47] *Gabisonia Z.*, Digital governance and law technologies in the justice system, Journal. "Justice", No. 1[4], 2023, 41.
[48] See, Bock R., Some thoughts on the future of notary, Georgian-German Journal of Comparative Law, No. 2, 2022, 1-2; Bocki R., German Notary System, Georgian-German Journal of Comparative Law, No. 8, 2020, 6-8.
[49] *Wudarski A., Sirdadze L.,* Registry jungle in the 21st century, Georgian-German Journal of Comparative Law, No. 6, 2020, 30-31.

Bibliography:

1. Law of Georgia "On Personal Data Protection", 14/06/2023.
2. Law of Georgia on Notaries, 04/12/2009.
3. Order of the Minister of Justice of Georgia "On approval of the instruction on the procedure for performing notarial acts", 31/03/2010.
4. Convention for the Protection of Individuals with regard to the Processing of Personal Data (Convention 108+), 18/06/2018.
5. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), 28/01/1981.
6. 2022 report on the activities of the Personal Data Protection Service.
7. 2023 report on the activities of the Personal Data Protection Service.
8. *Asvanua N*., Personal data protection mechanisms, Tbilisi, 2023, 39-40.
9. *Bernsdorff N*., "Data Protection Law" of the European Union, Journal of Personal Data Protection Law, No. 2, 2023, 14-15.
10. Bock R., Some thoughts on the future of notary, Georgian-German Journal of Comparative Law, No. 2, 2022, 1-2.
11. *Bocki R*., German Notary System, Georgian-German Journal of Comparative Law, No. 8, 2020, 6-8.
12. *Chiarini A., Forte A.,* Excellence in Notary Services through ISO 9001 Certification: an Investigation from Italy, Huelva, 2016, 124-125.
13. *Elizbarashvili S*., Protection of human rights in the era of technological development: the beginning of regulation of artificial intelligence, collection of articles - Protection of human rights: European experience and national challenges, volume, 2023, 80-81.
14. European Commission for the Efficiency of Justice, Study on the Functioning of Judicial Systems in the EU Member States, Specific Study on the Facts and Figures from the CEPEJ Questionnaires 2012 to 2020, Strasbourg, 2022, 899-900.
15. European Commission for the Efficiency of Justice, Working Group on the Evaluation of Judicial Systems, Specific Study of the CEPEJ on the Legal Professions: Notaries – 2018, Notaries of Europe (CNUE), 7-10.
16. European Judicial Systems Efficiency and Quality of Justice, Specific Study of the CEPEJ, Council of Europe, №26, 2018, 220.
17. *Gabisonia Z.,* Digital governance and legal technologies in the justice system, journal. "Justice", No. 1[4], 2023, 41.
18. General Data Protection Regulation (GDPR), 27/04/2016.
19. *Hall E. G.,* the Common Law and Civil Law Notary in the European Union: a Shared Heritage and a Influential Future, London, 2015, 15.
20. Information Commissioner's Office (ICO), Guide to the General Data Protection Regulation (GDPR), 2018.
21. *Kharitonashvili N*., Conference "Digitalization of German and Georgian Notary", Georgian-German Journal of Comparative Law, No. 4, 2023, 88-89.
22. *Kharitonashvili N*., Digitization of the Georgian Notary, Georgian-German Journal of Comparative Law, No. 6, 2023, 149.
23. *Khubua G., Sirdadze L.,* Law technologies (legaltech) in Georgia, their use in private companies and public agencies, Georgian-German Journal of Comparative Law, No. 7,

2022, 10.Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), 28/01/1981.

24. *Kuner C., Bygrave L. A., Docksey C.,* The EU General Data Protection Regulation (GDPR) – a Commentary, Oxford University Press, Oxford, 2020, 25-27.
25. Personal Data Protection Service Manual Recommendations for Public Institutions "On Personal Data Protection" for the purpose of compatibility with the law of Georgia on issuing/updating intra-departmental legal acts, 2023, 1-2, 14.
26. Peterfalvi A., Esther D., When Our Machines Learn Us: European Union Efforts to Regulate AI-Based Decision-Making and Profiling, Journal of Personal Data Protection Law, No. 1, 2023, 72-74.
27. Recommendation of the Personal Data Protection Service "On rights and profiling related to automated individual decision-making", 2024.
28. Recommendation of the Personal Data Protection Service "On the implementation of measures related to the incident", 2024.
29. Recommendation of the Personal Data Protection Service "On the Principles of Personal Data Processing", 2024.
30. *Rinne T.,* A Guide to Corporate Forms for Doing Business in Germany, Hamburg, 2017, 23.
31. *Ruggeri L., Kunda I., Winkler S. (eds.),* Family Property and Succession in EU Member States National Reports on the Collected Data, the European Commission, 2019.
32. *Verboven F., Yontcheva B.,* Private Monopoly and Restricted Entry - Evidence from the Notary Profession, 2022, 7.
33. Wudarski A., Sirdadze L., Registry jungle in the 21st century, Georgian-German Journal of Comparative Law, No. 6, 2020, 22, 30-31.
34. Case of the Data Protection Authority (Italy) №9993548, 11/01/2024.
35. Case of the Data Protection Authority (Belgium) №52, 03/04/2024.
36. Case of the Data Protection Authority (Poland) №DKN.5131.31.2021, 07.02.2023.
37. Case of the Data Protection Authority (Belgium) №48, 08/04/2021.
38. Case of the Data Protection Authority (Spain) №PS/00044, 23/10/2020.

Maka Nutsubidze*

Protection of Personal Data in Action Logs

This article examines the current legal issues surrounding personal data protection in action logs (commonly referred to as "logs"). With the implementation of the new law in Georgia, "On Personal Data Protection," the necessity for a balance between the effectiveness of action logs as an information security measure and the high standard of protection for the personal data they contain has become increasingly urgent.

***Keywords**: activity log, personal data, data security, General Data Protection Regulation, personal data protection.*

1. Introduction

In the case Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González[1], the Court of Justice of the European Union (CJEU) stated: "In the process of automatic, continuous, and systematic exploration of the Internet to search for information published online, the operator of the search engine "collects" data, which it then "recovers", "writes", and "sorts" as part of its indexing programs. This data is then "stored" on servers and, when necessary, "disclosed", providing "access" to users in the form of a list of search results."[2] The court concluded that such actions constitute "processing", even if the search engine operator performs similar operations on other types of information and does not differentiate between personal data and non-personal data.

In accordance with EU legislation, it is stated that "taking into account the latest technologies, implementation costs, the nature, scope, context, and purposes of processing, as well as the potential threats to the rights and freedoms of the data subject, data controllers and processors must implement appropriate technical and organizational measures to ensure security [...]."[3]

These measures encompass the following aspects: pseudonymization and encryption of personal data; ongoing confidentiality, integrity, availability, and resilience of processing systems and services; timely restoration of access and availability of personal data in the

* Assistant Professor of Law Faculty at Ivane Javakhishvili Tbilisi State University, Doctor of Law.

[1] CJEU, Case 131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [GC], 13/05/2014.

[2] Ibid., paragraph 28.

[3] On May 25, 2018, the General Data Protection Regulation (GDPR) of the European Parliament and of the Council (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, entered into force. Official Journal of the European Union, L119/1, 27 April 2016. Available at: https://gdpr-info.eu [Accessed 02 July 2024]. See Article 5.

event of a physical or technical incident; and regular inspection and evaluation of the effectiveness of the technical and organizational measures in place for processing security.

According to international standards for personal data protection, "logging" is regarded as a mandatory requirement and serves as a safeguard for data security.

It is important to note that Georgian legislation does not recognize the terms "log" and "logging." Nevertheless, the Law of Georgia "On Personal Data Protection" aligns with the European Union standard, specifically the GDPR, and mandates that the controller must "ensure all actions performed against data in electronic form (including incidents, data collection, modification, access, and accounting for their disclosure, transmission, connection, and erasure of information)"—essentially, logging. [4]

Consequently, in accordance with Georgian legislation, "logging" is translated as "recording of actions," and "log" is translated as "log of recording of actions."[5]

As a general rule, the creation of logs involves the collection of personal information, which transforms these logs into a medium for processing personal data. This raises the necessity of maintaining a balance between the effectiveness of activity logs as an information security system and the protection of personal data contained within them.

Consequently, our research aims to examine the legal and procedural standards that facilitate this balance. Accordingly, the article will cover the following topics: The standard of protection for personal data in activity logs in accordance with the GDPR and Georgian legislation (Chapter Two); the principles of personal data protection in activity logs: minimization, pseudonymization, and depersonalization (Chapter Three); Activity logs as a data security guarantee: incident logging and notification (Chapter Four); Procedural requirements for activity logs: storage periods and access by authorized persons (Chapter Five).

2. The Standard of Protection for Personal Data in Activity Logs in accordance with the GDPR and Georgian Legislation

The Law of Georgia "On Personal Data Protection," in line with the General Data Protection Regulation (GDPR) of the European Union, establishes the obligation for both the controller and the processor to ensure data security. Specifically, paragraph 4 of Article 27 of the law states: "The controller and the processor are obliged to ensure the logging of all actions performed on personal data in electronic form, including data breach, collection, modification, access, disclosure (transmission), linking, and erasure of data."

The logging of actions performed on data in electronic form is used primarily for security purposes, to facilitate the investigation of incidents and to identify the entities involved. Logged data is collected by controllers, processors, and devices connected to the Internet.

Actions performed on personal data in electronic form are recorded chronologically in electronic logs. Data is generated continuously and everywhere. These logs typically include information about the time and date of the action; the specific action taken or attempted; the user or IP address; details about authorized or unauthorized users; the location where the action was performed, and any modifications made to the original data. The logs also record whether the user successfully completed the action and, in case of failure, the reason for that failure.

[4] Law of Georgia "On Personal Data Protection", 14/06/2023, Article 27, Paraghraph 4.

[5] In French, both in France and Canada, the terms 'logging' and 'log' are not used. Instead, the terms *'enregistrement d'actes'* and *'journal d'enregistrement d'actes'* are used (M.N.).

At the same time, activity logs may involve processing an indefinite amount of personal data, necessitating strict compliance with data protection standards.

According to the General Data Protection Regulation (GDPR) and the Law of Georgia "On Personal Data Protection"[6], personal data is any information related to an identified or identifiable natural person. A person is identifiable when they can be recognized directly or indirectly, such as through their name, identification number, geolocation data, identifiable electronic communication data, or physical, physiological, mental, psychological, genetic, economic, cultural, or social characteristics. For example, personal data may include an individual's schedule, location information, or even their IP address.

As a result, activity logs, which may contain such information, are subject to the data protection rules laid out in Article 5 and Article 32 of the GDPR, as well as obligations set by Georgian data protection law.

According to Article 5 of the GDPR and Article 4 of the Law of Georgia "On Personal Data Protection", personal data must only be processed to the extent necessary to achieve the legitimate purpose.

In order to comply with the principle of data minimization[7], it is necessary that the volume of processed data be:

The data processed should be restricted to what is essential for achieving the specific purpose. This means that only data relevant and necessary to accomplish the intended objective should be collected and processed.

Personal data shall be processed only if the purpose of the processing cannot reasonably be achieved by other means. In addition, the principle of data minimization is closely related to the principle of purpose limitation, and it can be observed only if specific purposes are clearly defined by controller. The controller must review each step of the personal information processing operation and each data element in the action logs to determine the necessity to achieve the purpose.

Data controllers must assess whether they need to process personal data to achieve the relevant purposes. They should verify whether the intended purposes could be achieved by processing a smaller amount of personal data, using less detailed or aggregated personal data, or without processing personal data at all. In cases where personal data is necessary, controllers should ensure that only the minimum amount of data required for achieving the purpose is processed.

Minimization also relates to the degree of identification. If the purpose of processing does not require the final set of data to refer to an identified or identifiable individual (for example, in the case of statistics), but such identification is necessary during the initial processing (for example, before data aggregation), the controller must erase or anonymize the personal data once the need for identification ceases. Additionally, if permanent identification is required for other processing activities, personal data should be pseudonymized to minimize risks to the rights of data subjects[8].

Activity logs contain vast amounts of data, a significant portion of which is personal data. The larger the organization, the more personal information is processed and stored in logs, including IP addresses and geolocation data. Since the retention of data in activity logs

[6] Law of Georgia "On Personal Data Protection", 14/06/2023, Article 3, Paragraph "a".
[7] Ibid., Article 4.
[8] Recommendation "On the Principles of Personal Data Processing", Personal Data Protection Service, 2024.

is often mandated by law, an effective approach is to filter the data in the activity log, such as by editing or deleting email addresses or phone numbers[9].

3. Protection of Personal Data in Action Logs

In any case, the processor must establish a system that guarantees the confidentiality, availability, and integrity of the data stored in the action logs. More specifically, the use of collected data should be formalized and documented through pre-established rules and procedures.

After achieving the purpose for which the data is processed, it must be stored in a form that prevents the identification of any individual.

The authorized person who has access to the processing must be informed about the rules for using the activity log, the types of data collected, and the duration of their storage. This can be accomplished, for example, through an informational message displayed during authentication or prior to access.

When processing data, it is essential to ensure their integrity, security, and protection against unauthorized or illegal processing, as well as against accidental loss, destruction, and damage[10].

Article 32 of the GDPR reinforces the fundamental principle of integrity and confidentiality established in Article 5, allowing for data protection through pseudonymization and depersonalization. This principle also applies to the processing of personal data in activity logs.

According to the Law of Georgia "On Personal Data", data depersonalization is the processing of data when it is impossible to connect them to the data subject or establishing such a connection requires disproportionately large efforts, costs and/or time; [11] And data pseudonymization is such processing of data when it is impossible to connect the data to a specific data subject without the use of additional information, and this additional information is stored separately and through technical and organizational measures, the data is not connected to an identified or identifiable natural person[12].

Taking into account new technologies, implementation costs, the nature, scope, context, and purposes of processing, as well as the anticipated risks to the rights and freedoms of the data subject and the principles of data processing, the data controller must adopt appropriate technical and organizational measures. These measures should be applied both when determining the means of processing and during the processing itself, including pseudonymization and other methods. Implementing these measures will ensure the effective application of data processing principles and the integration of protective mechanisms within the data processing process to safeguard the rights of the data subject.[13]

[9] Privacy Commissioner of Canada's Guide to Protecting Personal Data in Activity Logs <https://www.cyber.gc.ca/sites/default/files/itsap80085-journalisation-surveillance-securite-reseau-f.pdf> [02.07.2024].
[10] Ibid.
[11] Law of Georgia "On Personal Data Protection", 14/06/2023, Article 2, Paraghraph "C".
[12] Ibid., paragraph "d".
[13] Ibid., Article 26.

4. Activity Logs as a Data Security Guarantee: Data Breach Logging and Notification

According to Article 33 of the GDPR and Article 29 of the Law of Georgia "On Personal Data Protection," the data controller is required to document the data breach, its outcomes, the measures taken, and to notify the Personal Data Protection Service in writing or electronically no later than 72 hours after discovering the incident. This notification is only necessary if the incident is likely to cause significant harm and/or pose a significant threat to fundamental human rights and freedoms. Furthermore, the data processor must immediately inform the data controller about the incident.

Under the Law of Georgia "On Personal Data Protection"[14], the notification must include the following information:

a) Details regarding the circumstances, type, and time of the incident;

b) Information about the probable categories and number of data involved in the incident, including any that were disclosed, damaged, deleted, destroyed, obtained, lost, or changed without authorization, as well as the probable categories and number of affected data subjects.

Activity logs, which document the internal functioning of the system, serve as the sole database that enables both the data controller and the data processor to respond to and notify relevant parties regarding an incident.

5. Procedural Requirements for Activity Logs: Storage Periods and Access by Authorized Persons

5.1. Retention Periods for Action Logs

Article 30 of the GDPR and Article 28 of the Law of Georgia "On Personal Data Protection" establish the obligation to maintain records related to data processing and to notify the Personal Data Protection Service. Specifically, the data controller and their designated representative (if applicable) must provide written or electronic records containing information about data retention periods. If a specific retention period cannot be determined, they must specify the criteria used to establish that retention period. This ensures transparency and accountability in the processing of personal data, aligning with the principles of data protection.

Activity logs are often retained for extended periods due to their critical role in providing important information necessary for conducting effective investigations in the event of an incident or attempted incident. However, retaining personal data contained within these logs indefinitely or for an unjustifiably long duration poses an unreasonable risk.

While the GDPR does not specify an exact retention period for personal data, the Court of Justice of the European Union (CJEU) addressed the legality of data retention in the *Digital Rights Ireland*[15] case[16]. The CJEU highlighted the absence of objective criteria in the Data

[14] Ibid., Article 29.

[15] CJEU, Case C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [GC], 08/04/2014.

[16] The directive aimed to harmonize national provisions regarding the retention of personal data obtained and processed through publicly available electronic communications services or networks, which could be transferred to authorized agencies for the purpose of combating organized crime and terrorism. The Data Protection Directive mandated the retention of data 'for at least six months,' without differentiating between the categories of data outlined in Article 5 of the same Directive, regardless of its relevance to the intended purpose or the individuals to whom it pertained.

Retention Directive to determine the precise storage period, which ranged from a minimum of 6 months to a maximum of 24 months.

Thus, considering best practices[17] in EU countries, the retention period for activity logs typically ranges from six to 12 months. In exceptional cases, this period may be extended up to 24 months.

In accordance with Article 5 of the GDPR and Article 4 of the Law of Georgia "On Personal Data Protection", data may be retained only for the duration necessary to fulfill the corresponding legitimate purpose of processing. Once the purpose for which the data were processed has been achieved, the data must be deleted, destroyed, or stored in a depersonalized form, unless their processing is mandated by law or a subordinate normative act issued in accordance with the law. In such cases, the retention of data must be a necessary and proportionate measure to protect the overriding interests of a democratic society.

When determining the storage period, the data controller must consider a duration proportional to the intended purpose. The maximum retention period of 24 months must be justified. In any case, it is insufficient to justify this maximum duration solely on the basis of the statute of limitations for criminal offenses.

By considering various factors during processing, it is possible to determine a justified maximum storage period[18]. For example:

- When a specific retention period is mandated by legislation;
- For a specific purpose that can only be achieved using log data, such as allowing disputants to access documents and relevant materials to ensure transparency for interested parties;

When there is a need to conduct a post-attack or post-intrusion analysis, which is essential for assessing future threats in the long term.

It is essential for the data controller to clearly document the reasons for establishing a longer retention period, such as citing specific legal obligations or specificities related to the purpose[19]. The need to retain data for an extended duration may also be justified if this measure is the only means to conduct a Data Protection Impact Assessment (DPIA) or an equivalent study on high-risk individuals. This analysis should be performed on a case-by-case basis, applying GDPR principles where possible to determine the necessary safeguards regarding security conditions, accessibility, and data storage purposes.

5.2. Access to Activity Logs by Authorized Personnel

In accordance with Article 27, Paragraph 6 of the Law of Georgia "on Personal Data Protection", both the data controller and the data processor are obligated to define the scope of access to data based on the employees' responsibilities. They must also implement adequate measures to prevent, detect, and address instances of unlawful data processing by employees, including providing them with information about data security protection issues.

The individual granted access to activity logs is obligated to adhere to the limits of their authorized scope and to protect the secrecy and confidentiality of the data, even after the termination of their official authority[20].

[17] Resolution No. 2021-122 of the French National Commission for Information and Freedom ("CNIL") "On the Protection of Personal Data in Activity Logs".
[18] Ibid.
[19] Ibid.
[20] Law of Georgia "On Personal Data Protection", 14/06/2023, Article 27, Paragraph 5.

Any reprocessing of collected data that contravenes the original purpose constitutes a change in the final objective of the processing. Therefore, it is advisable for the data controller to implement technical and organizational measures to mitigate risks. For example, they could require authorized individuals accessing activity logs to adhere to predefined data usage rules or establish a warning system to prevent unauthorized modifications to the activity logs.

6. Conclusion and Recommendations

Research has demonstrated that activity logs provide an essential means to trace and identify threats related to incidents, as well as to plan and implement preventive measures for system protection. However, to ensure that personal data collected in logs is protected to a high standard in accordance with the GDPR and Georgian legislation, data controllers and processors should consider and implement the following recommendations:

- the processing of data in activity logs must adhere to the principles of fairness, legality, and transparency;
- The purpose of data processing must be specific, clearly defined, and legitimate. Data collected in activity logs may not be used for any other purpose;
- Activity logs should collect only the data necessary to ensure data security, to prevent, analyze, or investigate an incident or attempted incident;
- Data in activity logs should be retained only for a predetermined period;
- Activity logs should be stored securely, preferably on external servers, and kept separate from the main system. Access must be restricted to authorized personnel only, and the activity logging system should be equipped with preventive technical measures to avoid duplication, copying, or overwriting;
- It is recommended that personal data in activity logs be encrypted.

Bibliography:

1. General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council “On the protection of natural persons with regard to the processing of personal data and the exchange of such data,” 27/04/2016. <https://gdpr-info.eu/> [02.07.2024].
2. Law of Georgia “On Personal Data Protection”, 14/06/2023.
3. Privacy Commissioner of Canada's Guide to Protecting Personal Data in Activity Logs <www.cyber.gc.ca> [02.07.2024].
4. Recommendation “On the Principles of Personal Data Processing”, Personal Data Protection Service, 2024. <https://personaldata.ge> [02.07.2024].
5. Resolution No. 2021-122 of the French National Commission for Information and Freedom (“CNIL”) “On the Protection of Personal Data in Activity Logs”, <www.cnil.fr> [02.07.2024].
6. CJEU, Case 131/12, *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González [GC]*, 13/05/2014.
7. CJEU, Case C-293/12 and C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [GC]*, 08/04/2014.

Nino Khubulia*

Challenges in the Processing of Children's Personal Data

The protection of children's personal data is a topical and problematic issue. The urgency of this issue is determined by the status of children as data subjects, their rights, and the peculiarities of legislative regulations regarding the expression of these rights. Particularly noteworthy is the impact of digital technologies on children's daily lives and their ability to exercise these rights. This article reviews national and international standards for the processing of children's personal data to identify the expected risks and challenges.

Keywords: *Personal Data Protection Service of Georgia, Protection of personal data of Children, processing of personal data of Children.*

1. Introduction

The purpose of the Law of Georgia "On Personal Data Protection" is to safeguard fundamental human rights and freedoms, including the rights to privacy in personal and family life, personal space, and communication, in the context of personal data processing. In this regard, special consideration must be given to the status of children as data subjects, their rights, and the exercise of these rights independently or through a representative, and the evaluation of key risks. This includes oversight of data controllers, such as schools, the healthcare sector, and other institutions, along with identifying violations, prevention, raising awareness, and fostering a culture of personal data protection.

It is important to assess the legal framework governing the processing of children's personal data and to identify the expected risks. Additionally, it is crucial to determine how well the new Law of Georgia "On Personal Data Protection" addresses existing challenges and what considerations data controllers should take into account when handling children's data.

2. A Specific Regulation on the Processing of Children's Data

In June 2023, the Parliament of Georgia adopted the Law "On Personal Data Protection," which introduces unique innovations and serves as a fundamental legal document for the protection of personal data in Georgia.

* PhD Student at Ivane Javakhishvili State University, Faculty of law; Inviting Lecturer; International Relations and Legal Matters Coordinator of International Relations, Analytics and Strategic Development Department of Personal Data Protection Service of Georgia.

The novelty of the regulation is based on the need to harmonize with international legal standards, (Council of Europe Convention 108 for the Protection of Individuals with Automatic Processing of Personal Data, Protocol amending Convention 108, Modernized Convention 108, General Data Protection Regulation etc.)[1] To introduce protective measures and mechanisms into Georgian legislation, and enhance the effectiveness, institutional independence, and impartiality of the Personal Data Protection Service, while implementing relevant recommendations. The importance of this law lies in its sectoral, functional, and fundamental nature.[2]

Article 7 of the law outlines the procedures and conditions for obtaining consent to process personal data of children. It specifies that if a child commits an administrative offense, it is considered as mitigating circumstance[3]. Conversely, processing data of children in violation of this law is regarded as an aggravating circumstance for administrative offenses under this law.[4]

Processing of data about a child is permitted based on the child's consent if they are 16 years old or older. For children under the age of 16, data processing requires the consent of a parent or legal guardian, unless otherwise specified by law. This includes cases where data processing is necessary for children aged 16 to 18, where the consent of a parent or legal guardian may also be required.[5]

Data controller is required to take all reasonable and appropriate measures to verify the consent of a parent or legal guardian for a child under the age of 16. Processing of special category data about a child is permitted only with the written consent of a parent or legal guardian, unless otherwise explicitly provided by law.

An overview of international standard-setting acts highlights the significance of the 1989 UN Convention on the Rights of the Child, adopted by the United Nations General Assembly. This document was the first international legal instrument to formally acknowledge the need for special care and protection for children.

The Global Privacy Assembly ("GPA") Resolution 2021 on the Digital Rights of the Child underscores that children require special protection and are entitled to the rights recognized by the Convention. It emphasizes that children should be able to enjoy these rights in all areas, including the online environment. The resolution explains that the digital environment significantly affects a child's development, daily life, future prospects, and opportunities.

The 2021 Declaration by the Committee of Ministers on the need to protect the privacy of children in the digital environment outlines the importance of safeguarding children's privacy online. It also highlights the risks that minors encounter when using modern technologies.

According to Article 38 of the General Data Protection Regulation ("GDPR"), children are granted special rights regarding the protection of their personal data, as they may be less aware of the risks, consequences, and available remedies involved in its processing.

---

[1] See: Council of Europe, Guide to European Data Protection Law, Luxembourg, Publishing House of the European Union, 2018, 20-21.

[2] Comp.: *Goshadze K.,* Constitutional-legal guarantees of personal data protection and processing, University of Georgia, Tbilisi, 2017, 43.

[3] Law of Georgia "On Personal Data Protection", 3144-XIms-Xmp, 14/06/2023, Article 61, paragraph 1, Sub-paragraph "B".

[4] Ibid., paragraph "c" of Article 62.

[5] see *Shudra T.,* Protecting the Personal Data of Minors in the Digital Environment with Different Expectations of Parents and Children, Personal Data Protection Law Journal, 1/2023, 112-115.

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) and the Modernized Convention 108 both address the issue of data protection. Article 5(2) of the Modernized Convention 108 refers to the data subject's consent. In EU law, consent as a lawful basis for data processing is strictly defined in Article 6 of the GDPR. Article 8 of the Charter of Fundamental Rights also clearly emphasizes this principle. The specific characteristics of valid consent are outlined in Article 4 of the Regulation, while the conditions for obtaining such consent are detailed in Article 7. Special rules for obtaining consent from children in relation to information society services are established in Article 8 of the Regulation.

3. A Child as a Data Subject

Being informed is an integral part of a person's free development, based on the ability to grow according to one's own will, decisions, and choices. A thorough understanding of information regarding personal data processing enables individuals, including children, to protect and control their personal sphere. Under EU and Council of Europe legislation, "personal data" is defined as any information that identifies or can identify a natural person, either directly or through additional information.[6] The German Constitutional Court stated in 1983 that "in the case of automatic data processing, there is no longer any insignificant information.[7] Any information relating to an individual, no matter how seemingly innocuous, may fall into a special category."[8] Therefore, personal data includes any information, whether it relates to a person's personal life, work, economic or social environment, or individual capabilities.[9] According to "GDPR", 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.[10] According to the Universal Declaration of Human Rights:[11] Data protection is a universal right and extends beyond the citizens of individual countries[12].

According to the recital of the General Data Protection Regulation (GDPR), children have a special right to the protection of their personal data, as they may be less aware of the risks, consequences, protection mechanisms, and rights associated with data processing.[13] Special right to protection should apply to:

- The use of personal data of children for marketing purposes;
- The creation of personal profiles or accounts for children;

[6] 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 (1); 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, article 2 (a).

[7] German Federal Constitutional Court, 1 BvR 209/83, 269/83, 362/83, 420/83, 440/83, 484/83, 15 December 1983, margin number 150.

[8] Commission of the European Communities, COM (90) 314, final, 13 September 1990, 19.

[9] see.: WP29, Opinion 4/2007 on the concept of personal data, 20 June 2007, 6.

[10] General Data Protection Regulation, GDPR, Recital 14 sentence 1.

[11] Convention on the Rights of the Child, International Treaty and Agreement, 1948, Article 8.

[12] General Data Protection Regulation, GDPR, Recital 14.

[13] General Data Protection Regulation, GDPR, Recital 38.

- The collection of personal data related to children when they use services directed specifically at them.[14]

Children assume the status of data subjects in various situations, particularly in the digital age, where their personal data is collected, processed, and stored for multiple purposes. For example, several scenarios may be considered:

Online Services and Social Media: Today, children are not restricted from using various online platforms, social networks, applications, or websites that collect their personal data, including personal information, photos, videos, or other identifying details.

Educational Institutions: Schools and other educational institutions collect and store data about their students for administrative, educational, or security purposes. This data includes attendance records, grades, behavior reports, and health information, making children data subjects within the educational environment.

Health Care Services: When a child receives medical care or treatment, health care providers collect and process information about the child's health. This includes medical records, diagnoses, treatment plans, and prescriptions.

Games and Entertainment: Online games, applications, and entertainment platforms often collect data from children as they interact with virtual environments and characters. This data is typically used to enhance the user experience and tailor content to individual preferences.

Research and Surveys: Children's data may be processed for research or survey purposes, particularly in educational or psychological studies. In such cases, it is crucial to respect their privacy and ensure their data is handled appropriately.

4. Key Considerations for Processing Children's Personal Data

The new law of Georgia "On Personal Data Protectio" stipulates that the processing of children's personal data must be carried out in accordance with the best interests of the child. However, the list of personal data processing principles does not include any specific modifications for processing children's data. This suggests that the general principles of data processing apply equally. Consequently, the data controller is responsible for identifying the individuals whose personal data is being processed, ensuring compliance with these principles.

The Code on the Rights of the Child does not prohibit the processing of a child's personal data for various purposes, such as in health care, education, and social protection. However, such processing must be conducted in the best interests of the child and in full compliance with Georgian legislation.[15]

The Supreme Court of Georgia has emphasized in one of its decisions that Article 71 of the Code on the Rights of the Child strictly protects a child's personal data. According to the first part of this article, it is prohibited to publicly disclose any personal data of a child involved in administrative or court proceedings, including through media. This includes information that could reveal or indirectly indicate the child's identity, such as images, detailed descriptions of the child or their family members, names, addresses, and audio or video recordings. The second part of the article prohibits the public disclosure of any document or record containing the child's personal data related to disciplinary measures, cases of violence

[14] General Data Protection Regulation, GDPR, Recital 38.

[15] *Kiladze S., Turava P.,* commentaries on the Code of Children's Rights, Tbilisi, 2021, 278.

involving or committed by the child, the child's health condition, or participation in social assistance or charity programs, among other similar information. Third part of the article stipulates that processing a child's personal data is permitted only in accordance with Georgian legislation. Therefore, the processing of personal data, including the publication of photographs, is allowed only with the consent of the data subject, except in legally defined circumstances.[16]

The court emphasizes that when taking any action involving a child, personal data must be protected to a much higher standard, and the child's best interests must be paramount. The court explained that, in the case under consideration, given the context, the topic, and the information conveyed, publishing the image of the minor in the story did not serve the child's best interests, did not protect the child's rights, and could cause negative feelings for the child.

The court notes that, in any action taken against a child or in any decision affecting them, there must be a primary focus on evaluating and safeguarding the child's best interests in both public and private contexts.[17]

The court points out that while the first and second parts of Article 71 of the Code on the Rights of the Child outline specific cases where publishing a minor's image is prohibited, these should not be considered an exhaustive list. Each case involving a minor must be evaluated individually, considering the unique circumstances to best serve the child's interests. Similarly, the Charter of Journalistic Ethics mandates the protection of children's rights as a distinct principle, requiring journalists to prioritize the child's interests in their professional activities and to avoid creating or publishing content that could be harmful to children.[18] Therefore, in each case, journalists should assess the potential negative risks and consequences that may arise from identifying a minor. If there is a risk that identifying the minor in a particular story could negatively affect their rights and best interests, the child's image should be presented in a way that does not reveal their identity.[19]

5. Risks and Challenges in Processing Children's Data

Data processing refers to any action or set of actions performed on personal data or data sets, whether through automated or other means. This includes, for example, collecting, recording, organizing, structuring, storing, adapting or modifying, retrieving, disclosing, using, transmitting, distributing, or otherwise making the data available, as well as grouping, combining, restricting, deleting, or destroying the data.

a. Internet Use and the Processing of Children's Data on Social Networks

The issue of internet use by children requires significant attention. Children may use online resources more frequently than their parents realize, and as a result, parents might not perceive this as a threat, especially since online tools simplify communication in daily life. However, when accessing online resources, there are risks[20] of personal data disclosure, privacy violations, and potential criminal actions such as coercion, fraud, and other threats,

[16] Decision No. As-488-2023 of the Supreme Court of Georgia of September 21, 2023.
[17] Decision No. A-1351-SH-33-2023 of the Supreme Court of Georgia of December 25, 2023.
[18] Comp.: *Firtskhalashvili A., Kardava E., Turava P.,* Handbook of Social Law, Tbilisi, 2023, 347-348.
[19] Decision No. As-488-2023 of the Supreme Court of Georgia of September 21, 2023.
[20] *Gurgenidze M.,* Protection of child's personal data in the Internet space, East European University, Tbilisi, 2020, 31-32.

which are particularly concerning. It is important to consider whether the online platform has a personal data protection policy and how its scope of use impacts the daily lives of children. Additionally, it should be assessed whether parents or children themselves are familiar with the privacy and security settings of the platforms they frequently use. Publicly disclosing a child's data online, in a way accessible to everyone, can have negative consequences, such as making the child a target of bullying or other unwanted treatment.[21]

b. Monitoring the Behavior of Children at School and the Processing of Student Data

Schools are authorized to conduct video surveillance on school premises, but only for purposes such as ensuring personal safety, protecting property, safeguarding children from harmful influences, and securing confidential information. Video recording is permitted only at entry points and the external perimeter. Surveillance is strictly prohibited in changing rooms and hygiene areas. Schools also have the right to monitor student entry and exit from the building and to record the name, surname, identification document details, address, dates and times of entry and exit, as well as the reasons for the visit. The retention period for this data must not exceed the limit defined by law.[22] Schools may take photos or videos and make the learning process public, but only with the consent of the data subject.[23] The best interests of the student must be prioritized when obtaining consent. Throughout the student's time on school grounds, whether during classes or breaks, the purposes for which the school may process the student's personal data must be clearly defined. For instance, video monitoring may be used to ensure that lessons proceed smoothly and that students remain in the classroom during instruction. Additionally, surveillance can be employed to prevent students from leaving the school premises during lessons or to ensure that unauthorized individuals do not enter the school grounds.[24] Educational institutions, their employees, as well as parents and family members of children, must take more responsibility for the disclosure of children's data and act in the best interests of the child.[25]

c. Processing of Children's Data in Medical Institutions

When disclosing data related to the health of minors, special attention must be given to assessing the risks associated with further use of this information. Children's data requires heightened protection, and each data processor must act primarily in the best interest of the child. Regardless of parental consent, disclosing health-related data or other sensitive information to third parties as public information is not permitted and is considered disproportionate and inappropriate for data processing purposes.[26] When assessing risks, it is crucial to determine the legal basis for processing a minor's personal data.[27]

---

[21] European Union, Children's Online Privacy and Data Protection in European Countries, 2021, No. 2021-020137, The Law Library of Congress, Global Legal Research Directorate, 18-19.

[22] European Data Protection Supervisor, Study on the Essence of the Fundamental Rights to Privacy and to the Protection of Personal Data, EDPS 2021/0932, December 2022.

[23] Guide to the General Data Protection Regulation, Bird & Bird, 2020, 6-7.

[24] See: *Sukhashvili N.,* Personal data protection of school students during distance education, collection of articles: current problems and challenges of personal data protection, Tbilisi, 2021, 9-10.

[25] *Gorgiladze A.,* Protection of personal data of abused children, Peculiarities of personal data protection (collection of articles), 2020, 55.

[26] Decisions of the State Inspector's Service, processing of health data, 2020.

[27] See: *Archuadze T.*, Depersonalization of personal data as a guarantee of data subject protection, Journal of Constitutional Law, 5/2020, 117.

In the context of personal data processing, the following issues should be considered according to the Code on the Rights of the Child:

- The right to life and personal development of the child implies that the child has a fundamental right to life and to develop personally. The state is required to take all necessary measures to protect the child's life and to create conditions conducive to their harmonious development. This is in accordance with the Code on the Rights of the Child, the Constitution of Georgia, the Convention on the Rights of the Child and its additional protocols, other international agreements to which Georgia is a party, and other relevant legal acts;
- The child's right to education means that every child is entitled to quality and inclusive education, with equal access. The state ensures that all children have equal access to an inclusive education system.
- The child's right to private and family life means that the child has the right to a private space and to conduct personal correspondence. Any illegal restriction of this right, including unjustified and unlawful interference with the child's personal space, family life, or personal correspondence, is not permitted.

The child's rights to freedom of opinion, information, media, and the internet mean that the child has the right to express their opinions freely. The child also has the right to be heard in decisions affecting them, with their views considered in accordance with their age, mental, and physical development. Additionally, the child has the right to seek, receive, and disseminate information through various means and forms. The child is entitled to access mass media and the internet and to use the internet freely.

In response to these challenges, the provisions introduced by the new law of Georgia "On Personal Data Protection" should be broadly interpreted. Article 7 of this law outlines the procedure and conditions for obtaining consent to process data about a minor. It specifies that the data controller must consider and protect the best interests of the minor. Consent from the minor, their parent, or other legal representative is not valid if the data processing threatens or harms the minor's best interests.

In 2022, the Personal Data Protection Service examined 39 cases involving the processing of minors' personal data. Of these, 27 cases were initiated by the Service, while 12 were based on citizen complaints or notifications. The reported issues primarily concerned the illegal disclosure of minors' personal data by medical institutions, breaches of video surveillance regulations, violations related to data processing for direct marketing purposes, and other instances where the processing of minors' data did not comply with legal requirements.

6. Conclusion

The scope of challenges related to processing minors' personal data is broad and complex. Uncertainty remains among data controllers regarding the appropriate forms and extent of processing for minors' data..

Given that one of the main objectives of the Personal Data Protection Service is to inform the public about data protection status and significant related events, it is crucial not only to raise awareness about the processing of children's personal data but also to develop strategies, inspection protocols, and flexible models with relevant standards for implementing Article 7 of the new law.

Alongside the implementation of Georgia's new "On Personal Data Protection" law, it is important to ensure that controllers of minors' personal data adhere to the law's requirements. Increasing minors' awareness of their rights is crucial for the timely identification of data protection challenges and will aid in taking appropriate countermeasures.

Bibliography:

1. Convention on the Rights of the Child, 1948.
2. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS No. 108), 1981.
3. General Data Protection Regulation (GDPR), 2016.
4. Modernisation of Convention 108, 2018.
5. Law of Georgia "Code on the Rights of the Child," No. 5004-I, September 20, 2019.
6. Law of Georgia "On Personal Data Protection," No. 3144-XIms-Xmp, June 14, 2023.
7. *Archuadze, T*. "Depersonalization of Personal Data as a Guarantee of Data Subject Protection," *Journal of Constitutional Law*, No. 5, 2020, 117.
8. Commission of the European Communities, COM (90) 314, final, 13 September 1990, 19.
9. Council of Europe, Guide to European Data Protection Law, Luxembourg, Publishing House of the European Union, 2018, 20-21.
10. European Data Protection Supervisor, Study on the Essence of the Fundamental Rights to Privacy and to the Protection of Personal Data, EDPS 2021/0932, December 2022.
11. European Union, Children's Online Privacy and Data Protection in European Countries, 2021, No. 2021-020137, The Law Library of Congress, Global Legal Research Directorate, 18-19.
12. *Firtskhalashvili A., Kardava E., Turava P*., Handbook of Social Law, Tbilisi, 2023, 347-348.
13. *Gorgiladze, A.* "Protection of Personal Data of Abused Children," *Peculiarities of Personal Data Protection* (collection of articles), 2020, 55.
14. *Goshadze, K*. "Constitutional-Legal Guarantees of Personal Data Protection and Processing," University of Georgia, Tbilisi, 2017, 43.
15. Guide to the General Data Protection Regulation, Bird & Bird, 2020, 6-7.
16. Gurgenidze M., Protection of child's personal data in the Internet space, East European University, Tbilisi, 2020, 31-32.
17. ICO, Children and the GDPR, 2018, 1.
18. *Kiladze S.,* Turava P., commentaries on the Code of Children's Rights, Tbilisi, 2021, 278.
19. *Shudra T*., Protecting the Personal Data of Minors in the Digital Environment with Different Expectations of Parents and Children, Personal Data Protection Law Journal, 1/2023, 112-115.
20. *Sukhashvili N*., Personal data protection of school students during distance education, collection of articles: current problems and challenges of personal data protection, Tbilisi, 2021, 9-10.
21. WP29, Opinion 4/2007 on the Concept of Personal Data, 2007, 6.
22. Decision No. As-1351-SH-33-2023 of the Supreme Court of Georgia of December 25, 2023.
23. Decision No. As-488-2023 of the Supreme Court of Georgia dated September 21, 2023.
24. Decisions of the State Inspector's Service, processing of health data, 2020.

Nino Tsagareishvili*

Legal Regulation of International Transfer of Personal Data (International and National Standards)

The cross-border transfer of personal data presents a complex challenge in both Georgian and international contexts. Notably, within the framework of international cooperation, substantial amounts of personal data are exchanged across various sectors. This reality necessitates effective regulation to ensure the protection of data subjects' rights. The article aims to explore the legal frameworks governing these transfers, focusing on both international standards and Georgia's national regulations.

Keywords: *International/Cross-Border Transfer of Personal Data, Personal Data Protection Service, Adequacy Decision, Appropriate Data Protection safeguards, Data Subject Rights.*

1. Introduction

In today's world, the transfer of personal data across borders is becoming increasingly significant. Continuous data exchanges between states and international organizations are essential for fostering cooperation across various sectors. While such transfers are beneficial for enhancing collaboration, they also introduce specific risks related to the protection of personal data. Balancing the benefits with the need for effective safeguards remains a critical challenge at both international and national levels.

First and foremost, an analysis of the compatibility between national personal data protection legislations is essential. Divergent approaches to key issues can lead to violations of data subjects' rights and undermine personal data protection standards. Consequently, several critical questions emerge: What national and international legal mechanisms govern the international transfer of personal data? If personal data is inadequately protected in a specific country, how is the transfer of such data restricted? In the absence of comprehensive legal regulation, what measures can be taken to ensure the protection of personal data? Additionally, what authority does the Personal Data Protection Authority wield in regulating cross-border data transfers?

This article will evaluate the legal aspects of the international transfer of personal data, with a focus on the requirements outlined in Chapter V[1] of the Law of Georgia "On Personal Data Protection." The discussion will analyze how these provisions regulate cross-border data

* Master of International Law at Ivane Javakhishvili Tbilisi State University, Faculty of Law; Researcher-Analyst in the International Relations, Analytics, and Strategic Development Department of the Personal Data Protection Service of Georgia.

[1] Law of Georgia "On Personal Data Protection", 14/06/2023.

transfers and ensure compliance with international standards. The international legal framework and standards, including recommendation documents developed by the European Commission[2] and the European Data Protection Board (EDPB)[3], as well as the practices of foreign data protection supervisory authorities, will be presented in this article. Through the analysis of these sources, answers to the posed questions will be provided.

2. National Regulation of International Data Transfer

On March 1, 2024, the Law of Georgia "On Personal Data Protection" (the Law) [4] came into force, with the primary objective of ensuring robust standards and guarantees for the protection of personal data. This new law addresses key issues in the field of data protection, including the regulation of international data transfers, to align Georgia with evolving global data protection norms. The transfer of personal data to another state or international organization is regulated by Article 37 of the Law of Georgia "On Personal Data Protection." According to this provision, such transfers are permitted only if the requirements for data processing, as outlined in the Law, are met, and the recipient state or international organization ensures adequate data protection standards. Furthermore, appropriate safeguards must be in place to protect the rights of the data subject.[5]

In addition to the above, according to paragraph 2 of Article 37, the transfer of data to another state or international organization is allowed if:

- The international agreements and treaties of Georgia provide for the transfer of personal data;
- The data controller provides appropriate guarantees for the protection of personal data;
- The data transfer is carried out in accordance with the legislation outlined in subsection "C," including the Criminal Procedure Code; the Law of Georgia "On the Legal Status of Aliens and Stateless Persons"; the Law of Georgia "On International Cooperation in the Field of Criminal Law"; the Law of Georgia "On International Cooperation in the Field of Law Enforcement"; and the Organic Law of Georgia "On the Prevention of Money Laundering and Terrorism Financing," adopted based on the Law of Georgia.
- After receiving information about the lack of adequate data protection guarantees and potential threats in the relevant state, the data subject requests written consent.
- The data transfer is necessary to protect the vital interests of the data subject, and the data subject is physically or legally unable to provide consent for data processing.
- There is a significant public interest in accordance with the law—such as crime prevention, investigation, detection, prosecution, execution of sentences, and the

[2] European Commission, the Executive Body of the European Union, <https://commission.europa.eu/about-european-commission_en> [03.08.2024].
[3] The European Data Protection Board, <https://www.edpb.europa.eu/about-edpb/who-we-are/european-data-protection-board_en> [03.08.2024].
[4] Law of Georgia "On Personal Data Protection", 14/06/2023.
[5] Ibid. the first paragraph of Article 37.

implementation of operational-search measures—and the data transfer is deemed a necessary and proportionate measure in a democratic society.[6]

It should be noted that if the data controller provides appropriate guarantees[7] in accordance with the contract, data can be transferred only after obtaining permission from the Personal Data Protection Service, the procedure for which is established by a normative act issued by the head of the Personal Data Protection Service.[8] In this case, the data transfer agreement should include enforceable conditions with legally binding force.[9] In addition, when transferring data on the listed grounds, the controller/processor is obliged to implement the necessary organizational and technical measures to ensure the safe transfer of data.[10] According to paragraph 6 of the same article, further transfer of data to another state or international organization by a third party is permitted only if it aligns with the original purposes, complies with the grounds for data transfer outlined in this article, and ensures appropriate data protection guarantees.

3. Supervisory Mechanisms of the Personal Data Protection Service regarding Cross-Border Data Transfers

One of the main functions of the Personal Data Protection Service (hereinafter referred to as 'the Service') is to supervise the lawfulness of cross-border transfers of personal data. Specifically, when international agreements or agreements to be concluded on behalf of Georgia provide for the possibility of cross-border personal data transfers, the Service conducts a legal examination of these documents upon the request of the relevant agency.

During the examination of a contract, the Service considers whether appropriate data protection guarantees exist in the relevant state or international organization. In this process, the Service reviews the drafts of the submitted agreements, as well as the legislative and institutional mechanisms related to personal data protection in the party state. Based on this review, if necessary, the Service will issue recommendations for amendments to the draft agreement.

The Personal Data Protection Service of Georgia assesses the existence of appropriate data protection guarantees in another state and/or international organization based on their international obligations and data protection laws, the guarantees for the rights and freedoms of data subjects (including effective legal protection mechanisms), the rules for further international data transfers, and an analysis of the existence, powers, and activities of the independent data protection supervisory authority.[11]

According to Order No. 23 of February 29, 2024, issued by the President of the Personal Data Protection Service, a list[12] of countries with appropriate guarantees for personal data protection has been approved. In these countries, data transfers are considered safe if proper

[6] Ibid. paragraph 2 of Article 37.
[7] Ibid. Article 37, Paragraph 2, Sub-paragraph “b”.
[8] Ibid. paragraph 3 of Article 37.
[9] Ibid. paragraph 5 of Article 37.
[10] Ibid. paragraph 4 of Article 37.
[11] Ibid. the first paragraph of Article 38.
[12] Order No. 23 of February 29, 2024 of the President of the Personal Data Protection Service “On approval of the list of countries with appropriate guarantees of personal data protection”.

grounds exist. The list includes both EU member states and countries for which the European Commission has adopted an adequacy decision. [13]

In accordance with Article 38, Paragraph 3 of the Law of Georgia "On Personal Data Protection", the specified list must be reviewed at least once every three years. If a state and/or international organization no longer meets the legal requirements, appropriate changes must be made to the list as determined by the normative act, which will not have retroactive effect.

In addition, based on Order No. 33 of March 1, 2024, issued by the President of the Personal Data Protection Service, the procedure for issuing permission for the transfer of personal data to another state or international organization has been developed, and the application form has been approved. This procedure outlines the process for submitting the application and relevant documentation, reviewing them, making a decision, and issuing permissions, along with their terms and conditions.[14]

4. International Standards for Cross-Border Transfer of Personal Data

4.1. General Overview of the International Legal Framework

Article 12 of the Council of Europe Convention 108, "On the Protection of Individuals with regard to Automatic Processing of Personal Data"[15] (hereinafter "Convention 108"), addresses the cross-border transfer of personal data. It establishes conditions for transferring personal data across borders by any means. According to paragraph 3, parties generally may not obstruct the transfer of personal data to the territory of another party or require specific authorization for such transfers solely for data protection reasons. However, paragraph 3 also specifies certain exceptions in which a party may deviate from the principles set out in paragraph 2:

- The legislation of a party contains specific provisions for certain categories of automated personal data files, provided that equivalent protection is not already ensured under the legislation of the receiving party.
- The data transfer is routed through an intermediary in another country, ultimately reaching a state that is not a party to the Convention.

The Additional Protocol to Convention 108 of the Council of Europe[16] addresses issues related to supervisory authorities and the cross-border exchange of personal data. The preamble emphasizes the importance of safeguarding human rights and fundamental freedoms, particularly the right to privacy, amid the increasing flow of personal data between

[13] See 3.2. Chapter: "Transfer of personal data to a non-EU country based on a adequacy decision taken by the European Commission".

[14] Order No. 33 of the President of the Personal Data Protection Service dated March 1, 2024 "On the procedure for issuing permission for the transfer of personal data to another state and international organization and the approval of the application form for the transfer of personal data to another state and/or international organization".

[15] CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series - No. 108, 1981.

[16] CoE, Additional Protocol to the Convention for The Protection Of Individuals with Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Crossborder Data Flows, European Treaty Series - No. 181, 2001, <https://rm.coe.int/1680080626> [03.08.2024].

states. Article 2 of this Protocol governs the transfer of personal data to recipients outside the jurisdiction of a Convention party. According to the first point, the recipient state or organization must ensure an adequate level of data protection during such transfers. Pursuant to paragraph 2, each party may transfer personal data if:

- The transfer is based on domestic legislation, particularly where specific interests are tied to the content of the data or involve overriding legitimate interests.
- The data controller, in line with contractual provisions, implements security measures that align with the domestic legal requirements set by the relevant authorities.

Article 14 of the modernized Council of Europe Convention 108[17] includes provisions governing the cross-border transfer of personal data, aiming to facilitate the free flow of information. This article defines international data transfer as the sharing of personal data with recipients in other jurisdictions. Such transfers to recipients outside the jurisdiction of a Contracting State are permitted only when an adequate level of data protection is ensured.[18]

Chapter 5 of the EU General Data Protection Regulation[19] (GDPR) sets out rules for transferring personal data to third countries[20] or international organizations. When making such transfers, data protection standards must be upheld.[21] This process follows a "two-step approach":[22] first, the transfer must comply with EU data protection laws and be based on the data subject's consent or another lawful authorization. Second, the transfer must meet the specific conditions outlined in the regulation. If adequate data protection safeguards are not in place, the transfer of personal data is prohibited.[23]

Under EU law, the exchange of personal data with countries in the European Economic Area (EEA) for purposes such as the prevention, investigation, detection, prosecution, or enforcement of criminal offenses is governed by the Directive on the processing of personal data in the police and criminal justice sectors.[24] The goal is to ensure that the exchange of personal data between authorized bodies within the European Union is not prohibited or restricted due to data protection concerns. [25]

[17] CoE, Convention 108 +, Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 2018.

[18] CoE, Council of Europe Treaty Series - No. 223, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2018, §102 <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a> [03.08.2024].

[19] EU, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 201 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), <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [03.08.2024].

[20] Third countries are non-EU countries.

[21] Ibid. Article 44.

[22] The EU General Data Protection Regulation (GDPR), A Practical Guide, 117.

[23] Ibid.

[24] Directive (EU) 2016/680 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 by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of such Data, and repealing Council Framework Decision 2008/977/JHA.

[25] Handbook on European data protection law, Luxembourg, 2018, 287.

4.2. Transfer of Personal Data to a Non-EU Country Based on an Adequacy Decision by the European Commission

Under Article 45 of the EU General Data Protection Regulation (GDPR), the European Commission is empowered to decide whether a non-EU country, territory, or specified sector ensures an adequate level of data protection. The process of adopting an adequacy decision involves the following steps:

- A proposal by the European Commission;
- An opinion from the European Data Protection Board (EDPB);
- Adoption of adequacy decision by European Commission.

Based on an adequacy decision, personal data can be transferred to third countries without the need for additional safeguards. In this case, the same data protection standards that apply within EU member states will be upheld in the recipient country, ensuring equivalent levels of protection.

The European Commission is required to periodically review adequacy decisions to ensure ongoing compliance, and must report the findings of these reviews to the European Parliament and the Council. If the requirements under the GDPR are violated, the European Parliament or the Council may, at any time, request that the Commission maintain, amend, or revoke the adequacy decision.[26]

4.3. Transfer of Personal Data to Non-EU Countries Based on Appropriate Data Protection Guarantees

In non-EU countries where no adequacy decision has been made, the transfer of personal data is not categorically prohibited. In such cases, the data controller must ensure adequate protection for personal data through alternative measures. Additionally, individuals must still be able to exercise their rights as granted under the GDPR.[27]

Article 46 of the GDPR outlines various mechanisms that private organizations can utilize to ensure appropriate safeguards in the absence of an adequacy decision. Specifically, the following measures should be developed:

- Standard data protection clauses;[28]
- Binding corporate rules;[29]
- Codes of conduct;
- Certification mechanisms;
- Standard contractual clauses for direct data transfers[30].[31]

Additionally, the transfer of personal data to third countries without an adequacy decision may be permitted based on the following grounds: the explicit consent of the data

[26] European Commission, Adequacy decisions, <https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en> [03.08.2024].
[27] GDPR, Third Countries, <gdpr-info.eu> [03.08.2024].
[28] Standard data protection clauses (SCCs).
[29] Binding corporate rules (BCRs).
[30] Ad hoc contractual clauses.
[31] EDPB, International Data Transfers, <edpb.europa.eu> [03.08.2024].

subject, which must be freely given; the necessity of fulfilling contractual obligations; the protection of vital public interests; or other specified legal bases under the GDPR.[32]

In relation to this issue, it is important to note the decision of the Court of Justice of the European Union (CJEU) in the "Maximillian Schrems" case[33], which emphasized the necessity of implementing additional measures when transferring personal data outside the European Economic Area, alongside the presence of appropriate safeguards. According to the court's assessment, data controllers and processors must evaluate the potential impact of the legislation and practices of the non-EU country on the effectiveness of these safeguards during data transfers.[34]

The European Data Protection Board (EDPB) has developed guidelines for the transfer of personal data between EU member states and organizations, as well as to non-member countries and organizations. The purpose of these guidelines is to regulate international data transfers in the absence of an adequacy decision, while taking into account the requirements established by the GDPR. The parties to the agreement are encouraged to include additional guarantees in their contracts. The document outlines key issues that should be addressed in the agreement, including: terms of the contract, principles of data processing, rights of the data subjects, obligations of the parties, restrictions on data transfers, and more.[35]

The European Commission has issued a document[36] outlining standard contractual clauses for the transfer of personal data to third countries, in line with the requirements of the General Data Protection Regulation (GDPR). It emphasizes that, in the context of modern technologies, the demand for cross-border data transfer is increasing to promote international cooperation and trade. In this process, ensuring the proper protection of personal data is essential.[37]

According to the first paragraph of Article 46 of the General Data Protection Regulation (GDPR), in the absence of an adequacy decision, the transfer of personal data is permissible if appropriate data protection guarantees are in place, including the rights of the data subjects and legal remedies. These guarantees must be aligned with the standard data protection clauses adopted by the European Commission, as outlined in Article 46, paragraph 2, subparagraph (c).[38]

The purpose of the standard data protection clauses developed by the European Commission is to ensure appropriate guarantees during the international transfer of personal data. The parties to the agreement are not restricted from including additional measures to enhance data protection within the contract. The accompanying document includes an appendix that outlines the standard contractual terms related to international data transfers.[39]

Additionally, the European Data Protection Board (EDPB) has produced a document detailing appropriate data protection safeguards for the cooperation between data

[32] Ibid.
[33] CJEU, Case C-311/18 (Schrems II), Judgment of the Court (Grand Chamber), 16 July 2020.
[34] EDPB, International Data Transfers, <edpb.europa.eu> [03.08.2024].
[35] EDPB, Guidelines 2/2020 on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for Transfers of Personal Data between EEA and non-EEA Public Authorities and Bodies, 15/12/2020, <edpb.europa.eu> [03.08.2024].
[36] European Commission, Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, <eur-lex.europa.eu> [03.08.2024].
[37] Ibid.
[38] Ibid.
[39] Ibid.

protection supervisory authorities within the European Economic Area (EEA) and third countries. The standards outlined in this guidance are based on Articles 70(1)(u) and 50(a) of the General Data Protection Regulation (GDPR).[40]

4.4. Overview of Practices of Data Protection Supervisory Authorities in Foreign Countries on International Data Transfers

Data protection supervisory authorities in various countries have addressed issues related to the international transfer of personal data in numerous cases. This chapter presents the practices of several countries as illustrative examples, providing a general overview of the existing approaches to international data transfers.

a. Sweden

The Swedish Data Protection Authority (IMY) has examined the legality of personal data processing through Google Analytics by a data controller. In this case, personal data was transferred to the United States via the platform.

The supervisory authority assessed the compatibility of this data transfer with the requirements of Chapter V of the GDPR, specifically Article 44. Drawing from the "Schrems II" case, the authority noted that merely having standard contractual clauses is insufficient for ensuring adequate data protection; a thorough analysis of the national legal framework is also necessary.

Ultimately, the supervisory authority concluded that the data transfer did not comply with the requirements established by Chapter V of the GDPR, as the data controller failed to adequately protect the rights of data subjects, resulting in a violation of Article 44 of the General Data Protection Regulation.[41]

b. Spain

The Spanish Data Protection Authority has investigated the legality of personal data processing by the telecommunications company Vodafone, particularly in the context of international data transfers.

In this case, Vodafone had a contract with a data processor required to process data in Peru, resulting in the transfer of personal data to a third country. However, the agreement did not address the issues related to international data transfers, thereby failing to provide adequate data protection guarantees.

Considering these circumstances, the supervisory authority determined that the data controller violated Article 44 of the GDPR.[42]

[40] EDPB, Toolbox on Essential Data Protection Safeguards for Enforcement Cooperation between EEA Data Protection Authorities and Competent Data Protection Authorities of Third Countries, 14/03/2022, <edpb.europa.eu> [03.08.2024].
[41] Decision of the Swedish DPA (IMY), 30/06/2023, <gdprhub.eu> [03.08.2024].
[42] Decision of Spanish DPA, 10/03/2021, <gdprhub.eu> [03.08.2024].

c. Austria

The decision of the Austrian Data Protection Authority pertains to the transfer of personal data to the United States by a company through Facebook, conducted without a relevant legal basis.

The supervisory authority evaluated the legality of the international data transfer and its compliance with the requirements set forth in Chapter V of the GDPR. Similar to other supervisory bodies, reference was made to the CJEU's ruling in the "Schrems II" case[43]. Following this analysis, it was concluded that there was no legal basis for the transfer of personal data. Specifically, the adequacy decision issued by the European Commission regarding data transfers from the European Union to the United States was deemed invalid. Consequently, both the data receiver and transmitter could not rely on Article 45 of the GDPR.

The supervisory authority determined that the data controller violated the requirements of Chapter V of the GDPR due to the unlawful transfer of personal data to the United States.[44]

d. Italy

The Italian Data Protection Authority (Garante) has examined the legality of transferring personal data to the United States by a website operator utilizing Google Analytics.

In its assessment, the supervisory authority noted that there was a low probability of access to personal information by U.S. authorities; however, this was not sufficient to absolve the data controller of responsibility for ensuring adequate safeguards. The authority determined that the encryption of personal data was an inadequate technical security measure.

Consequently, it found violations of Articles 44 and 46 of the GDPR. The supervisory body issued a re to the data controller, instructing them to achieve compliance with Article 46 within 90 days. Failure to do so would result in the cessation of the personal data transfer.[45]

e. Finland

The Finnish Data Protection Authority has also assessed the legality of personal data processing using the Google Analytics platform. In this case, personal data was transferred to the United States by the data controller, the Meteorological Institute. Citing the "Schrems II" decision, the supervisory authority evaluated the legality of the data transfer.

According to its findings, the transfer of personal data by the data controller did not have an appropriate legal basis under Chapter V of the EU General Data Protection Regulation, and adequate data protection guarantees were not provided.

As a result, the data controller unlawfully transferred personal data of the data subjects to the United States using Google Analytics. The supervisory authority determined that Articles 44 and 46 of the GDPR were violated. Consequently, it issued a reprimand to the data controller and ordered the deletion of the personal data transferred to the United States without a legal basis.[46]

[43] CJEU, Case C-311/18 (Schrems II), Judgment of the Court (Grand Chamber), 16 July 2020.
[44] Decision of Austrian DPA, 06/03/2023, <gdprhub.eu> [03.08.2024].
[45] Decision of Italian DPA, 9/06/2022, <gdprhub.eu> [03.08.2024].
[46] Decision of Finnish DPA, 24/03/2023, <gdprhub.eu> [03.08.2024].

5. Conclusion

The intensive exchange of personal data between states and international organizations necessitates effective regulation to adequately protect the rights of data subjects. The issues addressed in this article, including the practices of the Court of Justice of the European Union and foreign data protection supervisory authorities, highlight the significance of international data transfers and the challenges associated with them.

As noted, if no adequacy decision has been made regarding a non-EU country and adequate data protection guarantees are not in place, the transfer of personal data is still possible, provided that the issue can be addressed through an agreement. In this case, it is advisable to include in the contract definitions of key terms, principles of data processing, rights of the data subject, obligations of the parties, and other relevant provisions.

Before transferring personal data, it is crucial to assess the national legislation and data protection standards of the specific country. Additionally, it is important to determine the existence of appropriate safeguards. For this purpose, the international legal framework and standards discussed in this article should be considered, along with the requirements set out in Chapter V of the Law of Georgia "On Personal Data Protection."

Bibliography:

1. Law of Georgia "On Personal Data Protection", 14/06/2023.
2. Order No. 23 of the President of the Personal Data Protection Service "On approval of the List of Countries with Appropriate Guarantees of Personal Data Protection", 29/02/2024.
3. Order No. 33 of the President of the Personal Data Protection Service, "On the Procedure for Issuing Permission for the Transfer of Personal Data to Another State and International Organization, and Approval of the Application Form for the Transfer of Personal Data to Another State and/or International Organization," 01/03/2024.
4. CoE, Additional Protocol to the Convention for The Protection Of Individuals with Regard to Automatic Processing of Personal Data Regarding Supervisory Authorities and Crossborder Data Flows, European Treaty Series - No. 181, 2001.
5. CoE, Convention 108 +, Modernized Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 2018.
6. CoE, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, European Treaty Series - No. 108, 1981.
7. CoE, Council of Europe Treaty Series - No. 223, Explanatory Report to the Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 2018.
8. Directive (EU) 2016/680 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 by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of such Data, and repealing Council Framework Decision 2008/977/JHA.

9. EDPB, Guidelines 2/2020 on articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for transfers of personal data between EEA and non-EEA public authorities and bodies, 15 December 2020.
10. EDPB, Overview of International Data Transfers.
11. EDPB, Toolbox on Essential Data Protection Safeguards for Enforcement Cooperation between EEA Data Protection Authorities and Competent Data Protection Authorities of Third Countries, 14 March 2022.
12. EU, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 201 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).
13. European Commission, Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.
14. European Commission, Information Regarding the Adequacy Decisions.
15. GDPR, Information Regarding the Third Countries.
16. Handbook on European data protection law, Luxembourg, 2018, 287.
17. The EU General Data Protection Regulation (GDPR), a Practical Guide.
18. Case of the Data Protection Authority (Sweden), 30/06/2023.
19. Case of the Data Protection Authority (Spain), 10/03/2021.
20. Case of the Data Protection Authority (Austria), 06/03/2023.
21. Case of the Data Protection Authority (Italy), 09/06/2022.
22. Case of the Data Protection Authority (Finland), 24/03/2023.
23. CJEU, Case C-311/18 (Schrems II), Judgment of the Court (Grand Chamber), 16 July 2020.

Davit Kantaria*

Inviolability of the Private Life of a Child in Conflict with the Law and the Protection of Their Personal Data

The inviolability of the private life of a child in conflict with the law presents a challenging issue, making it crucial to balance the legitimate objectives established by law. The state bears a number of obligations to provide sufficient guarantees for the protection of children's rights.

In this regard, the provisions of the Juvenile Justice Code and the Law of Georgia "On Personal Data Protection" are particularly noteworthy. These laws emphasize the importance of shielding children in conflict with the law from stigmatization and ensuring their smooth reintegration into society. Achieving these goals requires the implementation of complex, practical measures that safeguard their rights while adhering to data protection standards.

Keywords: *Child in Conflict with the Law, Stigmatization, Personal Data, Privacy, resocialization, Professional Ethics.*

1. Introduction

The inviolability of a child's personal data must be safeguarded at all stages of the criminal justice process, in line with EU data protection principles. Central to juvenile justice is the goal of fostering the child's reintegration and positive resocialization into society. Achieving this, however, is challenging. When a child commits a criminal offense, even a serious one, society may often overlook the child's age, favoring a punitive approach that conflicts with the values of a democratic society. Equally, protecting child victims from secondary victimization is essential to uphold their dignity and emotional well-being.

Juvenile justice, in this regard, is particularly complex. Its practical implementation demands careful consideration, as determining what constitutes a proportionate response for a child can be challenging.

The handling of cases involving a child in conflict with the law is marked by distinct considerations and often conflicts with the right to public trial, as well as the rights to freedom of expression and access to information.

The right to privacy is a broad and evolving concept, not fully encompassed by the numerus clausus principle. This article aims to explore the complex legal issues surrounding

* PhD Student of Ivane Javakhishvili Tbilisi State University, Faculty of Law, Legal Matters Specialist of the Office of the President of the Personal Data Protection Service.

minors' privacy in juvenile justice and to assess the positive impact of the law of Georgia on Personal Data Protection in this context.

2. Protecting the privacy Child in Conflict with the Law

The Constitution of Georgia recognizes and guarantees human rights, with the right to personal life holding particular significance. Personal life encompasses not only an individual's inner world but also their ability to engage with the external environment. The inviolability of personal life is essential for the healthy development and sustainability of society. [1] Consequently, any exploitation of this right for personal gain or political purposes is strictly prohibited. The right to privacy is a fundamental value that permeates everyday life and stands as one of the cornerstones of a democratic society. In an era of rapid technological advancement, where progress continually reshapes our external environment, the right to privacy takes on new dimensions.

Article 15 of the Constitution of Georgia safeguards an individual's right to the inviolability of personal and family life, personal space, and communication. This right inherently transcends the confines of a single constitutional article. Consequently, both the European Court of Human Rights and the Constitutional Court of Georgia recognize that the fundamental significance of the right to privacy is tied to its multifaceted nature. This includes considerations related to race or ethnicity, beliefs and convictions, as well as biometric or genetic information. However, it is impossible to exhaustively enumerate all aspects of this right in advance.[2]

The protection of the right to private life is particularly crucial when it comes to minors. Interactions involving children necessitate a special approach, especially from a justice perspective, and legal regulations must reflect a comprehensive understanding of these factors. In recent years, the field of minors' rights protection has undergone significant transformation. Historically, minors were not recognized as having independent rights, but the "Geneva Declaration", adopted in the 1920s, marked a significant turning point. Subsequent developments have further advanced this field. Thus, it is important to examine the progress we have made and how current legislation safeguards the personal lives of minors.

Children's rights, including the right to privacy, are easily susceptible to violation. Therefore, society holds the primary responsibility for protecting children's interests and promoting the safeguarding of their rights.

The first significant step taken to protect children's rights was the Geneva Declaration, which enabled the recognition of children's rights and emphasized several crucial aspects[3], including child development, support, protection, and overall well-being. This declaration laid the groundwork for the adoption of the United Nations' Declaration of the Rights of the Child in 1959, which established the standard of the "best interests of the child". In 1985, the so-called "Beijing Rules" were introduced, addressing key issues related to the administration of juvenile justice. These rules helped prevent the stigmatization of minors by prohibiting the

[1] Ivanidze M., A minor and his/her best interests, analysis of the legislation of minors and judicial practice, Tbilisi, 2017, 545.

[2] Gogniashvili N., The importance of personal life protection and its specificity in relation to a minor, Georgian German Law Journal, 2023, 3.

[3] Imerlishvili I., Minor's rights: international experience and the current situation in Georgia, in the collection: Protection of human rights, constitutional reform and the rule of law in Georgia, Tbilisi, 2017.

disclosure of identifying information about them by the media and public institutions. In 1989, the "Convention on the Rights of the Child" was adopted, which has since been ratified by 195 countries worldwide. The United Nations subsequently adopted several supporting instruments for the Convention, aimed at creating more accessible standards and providing guidelines for professionals engaged in this field.[4]

Equally significant are the "Havana Rules," adopted in 1990, which outline essential principles of juvenile justice. This document emphasizes that the juvenile justice system should incorporate rights and guarantees that promote the physical and mental well-being of young individuals. The treatment of juveniles accused or convicted of offenses must differ from that of adults in similar situations. This distinction is based on several grounds: a child is considered less responsible for their actions, with their level of responsibility increasing with age; compared to adults, children who commit crimes are generally more amenable to rehabilitation and can learn alternative behaviors; and young individuals placed in pre-trial detention or prisons are particularly vulnerable to violence and abuse, making it more difficult for them to defend themselves. Additionally, the UN's "Riyadh Guidelines" represent a critical framework for addressing crimes committed by minors. These guidelines stress the importance of engaging youth in legal, socially beneficial activities while fostering a humane attitude toward society.[5]

International standards affirm that children, unlike adults, possess the right to full respect for their privacy at all stages of legal proceedings. The Committee on the Rights of the Child, in its General Comment 10, emphasizes that "all stages of case management" begin with the first contact with law enforcement authorities, including requests for information and identification, and extend to supervision or detention.[6]

The purpose of the right to respect for private life is to prevent the harm that may be caused to the child by unjustified publicity of the case. Negative publicity can stigmatize the child and have a negative impact on the child's ability to get an education, find a job and a place to live, as well as his reintegration in general[7]. The Committee on the Rights of the Child interpreted the right to privacy of children in conflict with the law in a broad sense. States should make clear in their legislation that when a child is tried for a crime, the hearing must be held in camera.[8]

The principle and purpose of the disclosure ban are clearly articulated in Section 102 of the Uganda Children's Act (1996), which aims "to protect the right to respect for private life and to limit publication." A child's right to privacy must be upheld throughout the judicial process to prevent undue publicity, and no individual should publish any information regarding a child before the Family and Children's Court that could lead to the child's identification. Furthermore, any person who violates the provisions protecting and limiting this right may be subject to fines and penalties.[9]

---

[4] Gogniashvili N., The importance of personal life protection and its specificity in relation to a minor, Georgian German Law Journal, 2023, 3.

[5] Eremadze St., Basic rights for freedom, book two, Ilia State University Publishing House, 2021, 201.

[6] Committee on the Rights of the Child, General Comment N10 (2007); paragraph 64.

[7] Rule 8 of the Beijing Rules. See also Committee on the Rights of the Child General Comment N10 (2007); paragraph 64.

[8] Hamilton K., Guidelines for Juvenile Justice Law Reform, 2011, at 88.

[9] See Uganda Children Act, 1996, Sec. 102.

The legal framework for the data protection of minors in conflict with the law in national legislation is still in the process of being established and refined. Part 2 of Article 13 of the Code of Juvenile Justice of Georgia, which is somewhat ambiguous, directs us to the law "On Personal Data Protection". However, the processing of personal data concerning minors in conflict with the law is further complicated by various subordinate normative acts. Each public institution, from investigative bodies to penitentiary facilities, determines, on a case-by-case basis, what data is processed, how long it is stored, and the method of destruction. These regulations do not provide adequate guarantees for protecting a minor's right to personal data and privacy, as the subordinate legal acts governing this issue are often incomplete[10].

In accordance with international standards, it is essential that "special requirements" are integrated into legislation to ensure that the needs of children are appropriately addressed. Such "special requirements" include respecting the minor's right to private life throughout all stages of case proceedings. Legislation must explicitly prohibit the disclosure of the identity of a minor in conflict with the law by individuals present at the hearing. From this perspective, it is crucial to establish a robust legal safeguard to protect the right of a minor to private life. The study revealed that the national legal framework governing children's rights does not contain a specific prohibition on media representatives disclosing the identity of children involved in the juvenile justice system. The Code on the right of the Child [11] includes a dedicated article that addresses the protection of minors' personal data by the media. However, this provision does not apply to cases of criminal and administrative offenses, as the Code indicates that these matters are regulated by the Juvenile Justice Code. However, the Juvenile Justice Code lacks specific provisions regarding the protection of minors' personal data by the media.

To address this issue, it is recommended to strengthen the mechanisms for responding to breaches of professional ethics by journalists within the framework of self-regulation, enabling effective responses to violations through disciplinary measures. Furthermore, since instruments for the protection of children's rights necessitate stricter actions against journalists who significantly infringe on the right to private life of minors, establishing an appropriate legal framework is imperative. Notably, Croatia has introduced a specific article in its Criminal Code to protect the right to private life of minors, which enables criminal prosecution of individuals who infringe on a child's right to private life by disclosing photos or other identifiable details, especially if such disclosure has subjected the child to ridicule from peers or otherwise endangered the child's well-being. Additionally, if such actions are committed by a public official or media representative, it constitutes an aggravating circumstance.

3. Protection of a Minor from Labeling

The phenomenon of labeling is prevalent. An illustrative example of this is Robert Rosenthal's study, which suggests that poor and minority students underperform in school

[10] *Kvrivishvili T., Guarantees of protection of the right to private life of a minor in conflict with the law in juvenile justice, dissertation (TSU), 2022, 47.*

[11] *Shekhiladze Kh.,* Prioritizing the best interests of a minor in conflict with the law in the process of juvenile justice (criminal proceedings), Tbilisi, 2019.

due to teachers' low expectations, resulting in treatment that assumes a lack of talent. This, in turn, fosters the very behaviors that teachers anticipate.[12]

Labeling theory posits that deviance is defined not by specific actions but by society's perception of the individual. From this perspective, deviance is shaped by reactions rather than behaviors. Labeling theory describes the following stages in the development of a criminal identity: 1) committing an initial offense; 2) difficulties in reintegrating the offender into society; 3) the offender's acknowledgment of their status; 4) formation of a criminal identity; and 5) committing subsequent offenses.

According to labeling theory, deviant behavior can result from various factors, but once an individual is labeled as deviant, they often face additional challenges linked to societal responses and stereotypes[13]. The theory primarily explores the consequences of being labeled as deviant: 1) Labeling an individual as deviant increases the likelihood of future deviant behavior. This label creates a barrier between the individual and society; furthermore, the deviant label acts as a "qualification" that shapes how society evaluates the individual. Society perceives the person as deviant overall, not just in a specific context, which fosters expectations of further deviance and subsequent treatment accordingly. For example, a person labeled a "thief" may no longer be trusted, even after serving their sentence, as friends might avoid them due to fears of theft or association with a damaged reputation. 2) This approach limits the labeled individual's chances for a normative life, often leading them to adopt a deviant lifestyle or career. Labeled individuals frequently identify with others who have received similar labels, forming close ties and demonstrating solidarity.[14]

Labeling theory suggests that this process contributes to secondary deviance, as well as a "self-fulfilling prophecy" – a phenomenon whereby an anticipated event creates conditions for its own realization. In this case, societal expectations about an individual's deviant future behavior contribute to the manifestation of that behavior.

From this review of labeling theory, it can be concluded that stigmatizing a juvenile as delinquent can significantly impact their future[15]. If information regarding a juvenile's conviction is not kept confidential, this labeling, rather than incarceration alone, may result in more detrimental outcomes. This could lead to peer rejection and association with others who possess deviant self-concepts, heightening the juvenile's risk of reoffending. For these reasons, safeguarding the right to privacy throughout the juvenile justice process to prevent disclosure and stigmatization is essential.

4. Reporting on Juvenile Cases

The right to freedom of expression is a guaranteed right for all individuals. It encompasses the right to hold opinions, the right to receive and impart information and ideas

[12] *Rosenthal, L. Jacobson, P*ygmalion im Unterricht. Lehrererwartungen und Intelligenzentwicklung der Schüler. Beltz 1983. S.129

[13] *Kvrivishvili T.,* Guarantees of protection of the right to private life of a minor in conflict with the law in juvenile justice, dissertation (TSU), 2022, 56.

[14] *Akhalashvili N*., Legal Psychology, Tbilisi, 2009, 244.

[15] *Shalikashvili M., Mikanadze G.,* Juvenile justice (manual), second edition, Tbilisi, Freiburg, Strasbourg, 2016, 48.

without interference from public authorities. However, states retain the authority to impose licensing requirements on broadcasters, television stations, or film enterprises.[16]

This right is a fundamental element of a democratic society, essential for societal progress and the self-realization of individuals. The scope of freedom of expression extends beyond favorably regarded or neutral information and ideas and includes content that may be offensive, shocking, or disturbing.

Media representatives are regarded as public watchdogs who play a pivotal role in democratic society. They are tasked with disseminating information and informing the public on matters of public interest, which the public has a right to receive[17]. A journalist's freedom of expression is not absolute; it carries both rights and responsibilities. In this context, "rights" refer to the journalist's prerogative to perform professional duties and report on matters of public interest, while "responsibilities" entail the journalist's duty to act in good faith and provide accurate and reliable information in line with journalistic ethics.[18]

Journalists are required to verify facts before publication; however, this requirement does not apply when reporting opinions or conveying points of view[19]. Nevertheless, opinions should also be grounded in a factual basis. The role and influence of the media on juvenile justice is evident in three areas: the media's influence on children, its role in shaping juvenile legislation, and its impact on the juvenile justice process.[20]

It is crucial to emphasize that, when covering court proceedings, judicial personnel are expected to demonstrate competence and responsibility in the legal field. This standard also applies to representatives of the media, thereby upholding the respect and integrity of their profession[21]. This requirement becomes even more pertinent given the heightened attention on cases involving minors.[22]

There exists a balance between two competing rights: freedom of expression and the inviolability of a minor's private life. Freedom of expression is not an absolute right. The Constitutional Court of Georgia has established that restrictions on freedom of expression are permissible based on the principle of proportionality, provided they adhere to formal legal requirements and serve clearly defined legitimate objectives.[23]

Numerous international and European instruments establish standards for media coverage involving minors in conflict with the law. The "Beijing Rules" deem it inadmissible for the media to publish information about minors involved in legal conflicts. The guidelines on "child-friendly justice" provide detailed measures for safeguarding the privacy of minors when informing the public through the media. Necessary measures include, among others, granting anonymity or pseudonyms to minors, concealing identities by altering voices,

---

[16] Danelia N., Coverage of children's issues in the Georgian television space, Media Development Fund, Tbilisi 2011, 38.

[17] Khidesheli S., Protection of children's rights in the media – an important aspect of the formation of a democratic state, in the collection: Protection of human rights and democratic transformation of the state, Korkelia K. (ed.), Vol., 2020, 37.

[18] Gotsiridze E., Freedom of expression in the context of fair balancing of conflicting values, TbIlisi., 2007. 27.

[19] Goshadze K., Basic right to personal data protection, 2020. 102.

[20] Jorbenadze S., Bakhtadze U., Macharadze Z., media law, Jorbenadze S. (ed.), Vol., 2014, 59.

[21] Alvarti H., The principle of publicity according to the German criminal law process, in the collection: The influence of European and international law on Georgian criminal procedural law, Tumanishvili G., Jishkariani B., Shrami E. (ed.), vol., 2019, 437-438

[22] I. Sarkeulidze, Juvenile crime and its causes in juvenile justice systems, Law Journal, No. 2, 2013.

[23] Decision No. 2/6/1311 of the Constitutional Court of Georgia dated December 17, 2019 in the case of "Stereo+ LLC", Luka Severin, Lasha Zilfimiani, Robert Khakhalev and Davit Zilfimiani against the Parliament of Georgia and the Minister of Justice of Georgia.

removing names or other identifiable details from documents, and prohibiting any form of recording (photo, audio, and video). Additionally, the guidelines allow for an exception to this rule in specific circumstances where the publication of identifying information is in the best interest of the child and where disclosing certain case details would yield beneficial outcomes for the minor.

The "Code on the rights of the Child," adopted by the Parliament of Georgia in 2019, establishes the legal framework for safeguarding the fundamental rights of children and supporting the child welfare system. This code includes a specific article regulating the protection of minors' personal data by the media. Under the first part of Article 71, the media is prohibited from disclosing the personal data of a child involved in administrative or court proceedings, preventing both direct and indirect identification. The second part of this article further prohibits, among other things, the disclosure of documents or records related to cases of violence involving a child. However, the legislator notes that these provisions do not extend to criminal and administrative offense proceedings, which are governed by the Code of Juvenile Justice.[24]

To safeguard the privacy rights of children within the justice system in the context of media coverage of criminal cases, it is appropriate to extend Article 71 of the "Code on the rights of the Child" to include criminal offenses[25]. Alternatively, a third section could be added to Article 13 of the Code of Juvenile Justice, containing similar wording, which would prohibit media representatives from disclosing any identifiable personal data of a child involved in the juvenile justice process, whether directly or indirectly.[26]

The European Court of Human Rights has confirmed in several rulings that freedom of expression can be restricted to protect the best interests of minors. One such case is Handyside v. United Kingdom. In this case, a London publishing house published The Little Red Textbook, intended for school children aged 12 to 18, discussing issues related to sexual education. When a UK court banned the book's publication, the applicant claimed this action violated Article 10 of the Convention. The European Court raised concerns about the book's potential negative impact on young, impressionable minds and its capacity to encourage behavior contrary to the law. The court concluded that the actions of state authorities fell within the framework of "strict necessity."[27]

Responsible journalism requires that journalists conduct themselves professionally, act with integrity, and adhere to journalistic ethics in their reporting. Journalists should provide balanced coverage by contacting relevant parties for comments before publication.

A critical factor in legal assessment is whether personal information is published by a journalist adhering to responsible journalism principles or by tabloid publications that share information solely for public curiosity. Responsible journalists enjoy greater protection of freedom of expression. However, it is not for the national government to determine the methods journalists should use in their reporting.

---

[24] Law of Georgia "The Code on the right of the Child", Parliament of Georgia, 20/09/2019, Article 2, first paragraph.

[25] Shekhiladze Kh., Prioritizing the best interests of a minor in conflict with the law in the process of juvenile justice (criminal proceedings), Tbilisi, 2019, 39.

[26] Kvrivishvili T., Guarantees of protection of the personal life of a minor in conflict with the law, dissertation (TSU), 2022, 194.

[27] Handyside v United Kingdom [1976] ECHR 5 at para. 48, (1976) 1 EHRR 737, [1976] ECHR 5493/72 (7 December 1976), European Court of Human Rights.

When reporting on minors, journalists must observe the highest standards. In Georgia, these standards were implemented gradually over time. In past years, such standards did not exist for juvenile cases. Due to the nature of their profession, journalists have the potential to create an "enemy icon" out of individuals, particularly minors, which requires utmost care. This poses a significant risk of labeling. Given that the primary goal of juvenile justice is the resocialization of the minor, this risk becomes a considerable obstacle. Presently, on various internet platforms, there are stories that effectively create an "enemy icon" out of minors, which should not be accessible to the public, as they harm the legitimate interests of minors.

Today, in Georgian practice, journalists demonstrate relatively high professionalism in reporting on cases involving minors, but further progress is necessary to ensure children are protected from additional stigmatization.

5. Safeguarding the Personal Data of Child in Conflict with the Law as a Guarantee of Their Right to Privacy

The protection of personal data is one of the foremost challenges of the 21st century[28]. Data protection concerns human autonomy and is regarded within the context of human rights and freedoms, specifically as an element of the inviolability of private life.

While the Constitution of Georgia does not specifically reference "personal data," the Constitutional Court has established that personal data is integral to the constitutional right to privacy, safeguarded by Article 15 of the Constitution. Additionally, the court considers the interest in shielding individuals from the unauthorized disclosure of personal data within the framework of the right to informational self-determination, as guaranteed by Article 18, paragraph 3 of the Constitution.[29]

Within children's rights law, the protection of personal data forms part of the child's right to private life, as protected by Article 16 of the Convention on the Rights of the Child. This obligation to respect privacy extends to all individuals involved in the process, from the initiating body to the child's legal representative. The Convention mandates that the relevant authority uphold the confidentiality of a minor's personal data at all stages of proceedings, thereby safeguarding against its unauthorized disclosure.

The protection of minors' privacy rights in the digital age presents additional complexities, as technological advancements heighten the risks of unlawful intrusion. Public and private institutions involved in the collection, use, storage, and disclosure of children's data play a critical role and must act in the child's best interests. Data processing authorities are further obligated to secure personal data against unauthorized access by third parties or the public, preventing any infringement of the minor's right to privacy. Disclosing personal data online carries specific risks, including the potential for cyberbullying.[30]

The protection of minors' personal data is upheld through a comprehensive mechanism, which includes both international norms in personal data protection and specific international and national legislation regarding children's rights, such as Georgia's Law "On Personal Data Protection" and a range of sectoral laws. European advisory and oversight bodies, along with

[28] *Goshadze K., Basic right to personal data protection, 2020, 6.*

[29] *Kopaleishvili M., Balance set by the Constitution between the right of public access to judicial acts and the right to protect personal data from access, research and recommendations on the need for legislative regulation in accordance with the decision of the Constitutional Court, 2020, 17.*

[30] *Pachulia T., Dangers of sharing personal data of minors on the Internet, in the collection: current problems and challenges of personal data protection, Toloraya L., Firtskhalashvili A. (ed.), 2021, 45.*

the National Data Protection Authority—Georgia's Personal Data Protection Service—also oversee the legality of personal data processing activities.

The protection of a minor's personal data within the context of legal conflict is a component of the right to private life. Both national and international instruments recognize that when processing the data of minors in legal conflicts, they are entitled to the right to personal data protection. Given a minor's inherent vulnerability, the disclosure of personal data could have profound adverse effects on their future. Consequently, there exists an enhanced interest in protecting the personal data of minors over that of adults.

Under the law "On Personal Data Protection," a minor's conviction is classified as a special category of data, which is treated separately from standard personal data protection regulations. As particularly sensitive data, it receives enhanced protection guarantees to safeguard the minor's interests. Confidentiality of such data must be maintained throughout all stages of the legal process to prevent harm to the minor[31]. Generally, processing of special data categories is prohibited; however, exceptions are allowed under legally defined circumstances. Specifically, the data of minors involved in criminal proceedings may be processed for managing personal records and registers within the criminal justice system, addressing individualized sentencing or parole issues, or when substituting remaining sentences with lighter penalties. This also applies when data is processed to enforce the provisions of the "Law of Georgia on Crime Prevention, Non-Custodial Sentence Enforcement, and Probation." Additionally, the data may be processed to support the resocialization and rehabilitation of juvenile convicts, prevent recidivism, and coordinate juvenile referrals.

The "Child-Friendly Justice" guidelines underscore the need to protect minors' personal data and encourage member states to ensure that identifying information about minors remains confidential and unpublished. Access to records involving minors should be strictly limited, and where information sharing is essential, states are encouraged to implement robust data protection laws. Although juvenile cases are typically non-public, such records may be accessible for research purposes, provided the information is fully anonymized to ensure privacy.

A Constitutional Court decision, issued before relevant legislative updates, has led to inconsistencies in accessing judgments against minors[32]. Some courts issue anonymized versions of judgments, others require the consent of the data subject, and some deny access entirely. For instance, the Tbilisi City Court denied requests for public access to judgments against minors, stating that "to protect minors' interests, criminal cases involving minors are held in closed sessions... court decisions from such cases are not processed for public databases."[33]

International and regional frameworks on children's rights protection focus on aspects such as data storage duration and the necessity of data destruction after a specific period. National legislation, through the "Personal Data Protection" law, provides a general guideline stating that one of the core principles in data processing is the limitation on data retention.

---

[31] *Kopaleishvili M., Balance set by the Constitution between the right of public access to judicial acts and the right to protect personal data from access, research and recommendations on the need for legislative regulation in accordance with the decision of the Constitutional Court, 2020, 17.*

[32] *Decision No. 1/4/693,857 of the Constitutional Court of Georgia of June 7, 2019 in the case "A(A)IP Media Development Fund" and A(A)IP Freedom of Information Development Institute" against the Parliament of Georgia.*

[33] *Kvrivishvili T., Guarantees of personal life protection of minors in conflict with the law, Tbilisi, 2022, 159.*

Specifically, "data may be stored only for the period required to achieve the legitimate purpose of data processing. Upon fulfilling this purpose, data must be deleted, destroyed, or anonymized, unless continued processing is mandated by law and is necessary and proportionate to the democratic interests of society."[34]

In S. and Marper v. United Kingdom[35], the European Court of Human Rights found that indefinite retention of a minor's fingerprints and DNA data, even following acquittal, violated Article 8 of the European Convention on Human Rights. One of the applicants in this case was an 11-year-old accused of a criminal offense who, despite his acquittal, had his fingerprints and DNA sample retained indefinitely by the police in England and Wales. The European Court explained that, under Council of Europe data protection instruments, data retention must be proportionate to its purpose and time-limited, a requirement particularly relevant to police data. The legislation in England and Wales allowed indefinite retention of this data, which the court found to be a disproportionate interference with the applicant's right to privacy. Furthermore, the court expressed particular concern over the potential harm to minors due to indefinite data retention, given the importance of a minor's development and social reintegration. The court emphasized the need to protect the right to privacy of minors under criminal law, as outlined in Article 40 of the 1989 UN Convention on the Rights of the Child. Special attention, it argued, should be directed toward shielding minors from harm resulting from governmental retention of personal data after an acquittal.[36]

It is equally essential that third parties permitted by a judge to attend a juvenile's court hearing are bound to maintain confidentiality regarding the juvenile's information. A strong legal guarantee is necessary to safeguard the right to privacy for minors. Several norms in the Criminal Procedure Code of Georgia address this matter. Article 104 of the Civil Code grants the court the authority, based on justice and the parties' interests, to protect case participants or those present in the courtroom from public disclosure of case data, either at a party's request or at the court's initiative. Additionally, Article 182, Part 7 of the Civil Code allows the court to require individuals present at closed sessions to refrain from disclosing any information learned during the session. However, these articles provide the judge with the right—but not the obligation—to warn attendees about confidentiality. It would be advisable to amend Article 29 of the Civil Code to obligate judges to inform individuals present at a minor's court session of the requirement to keep the minor's information confidential. This security measure, as stipulated in current practice, would incur criminal liability under Article 381 of the Criminal Code of Georgia if breached.

Adherence to guiding principles under the law "On Personal Data Protection" is critical, as these principles represent the core tenets of data protection law, with breaches resulting in legal offenses.

6. Conclusion

Research highlights significant challenges in protecting minors from stigmatization, particularly when their rights are compromised by media coverage. To address this, the Supreme Council of Justice of Georgia is encouraged to ensure that juvenile courtrooms are suitably equipped, including designated areas for attendees, to minimize exposure of minors'

[34] *Law of Georgia "On Personal Data Protection", Article 4, Section 1, Sub-section "e".*
[35] *S. and Marper v. The United Kingdom, [2008] ECHR, nos. 30562/04 and 30566/04, §124.*
[36] *S. and Marper v. The United Kingdom, [2008] ECHR, nos. 30562/04 and 30566/04, §124.*

identities. The closed-door policy in general courts has raised concerns about further risks of identification for minors involved in legal conflicts.

Additionally, discussions are underway regarding the assignment of specialized journalists to cover cases involving minors, which would ideally lead to more sensitive reporting. With Georgia's updated "Personal Data Protection" law, stronger protections are established for minors' privacy, placing clear obligations on data controllers to handle minors' data in their best interests. This law indicates the legislative intent to safeguard minors' privacy rights rigorously.

The primary focus of this paper was to explore the privacy protections for minors in the context of juvenile justice, evaluating how well Georgian laws align with international and European standards. The research highlights the need for high standards to prevent the stigmatization of minors in conflict with the law by preserving their anonymity. The Convention on the Rights of the Child identifies this right as essential for ensuring a fair trial, underscoring that minors have all the rights afforded to adults, though these are tailored to account for minors' age, psychological development, and other specific circumstances.

Georgian legislation, particularly the law "On Personal Data Protection, already offers significant safeguards for minors' data. Importantly, this law now recognizes offenses against minors as aggravating circumstances, which is an important legislative development aimed at strengthening protections for this vulnerable group.

Bibliography:

1. Constitution of Georgia, 1995.
2. Juvenile Justice Code, 2015.
3. Code on the rights of the Child, 2019.
4. Law of Georgia "On Personal Data Protection", 2013.
5. The UN Standard Minimum Rules for Juvenile Justice (the so-called "Beijing Rules").
6. United Nations Rules for the Protection of Juveniles Detained (Havana Rules), 1990.
7. *Alvarti H.,* The principle of publicity according to the German criminal law process, in the collection: The influence of European and international law "On Georgian criminal procedural law, *Tumanishvili G., Jishkariani B., Shrami E.* (Ed.), Tbilisi, 2019.
8. *Akhalashvili N*., Legal Psychology, Tbilisi, 2009.
9. *Gogniashvili N*., The importance of protecting personal life and its specificity in relation to minors, Georgian German Law Journal, 2023.
10. *Goshadze K*., Basic right to personal data protection, 2020.
11. *Gotsiridze E*., Freedom of expression in the context of fair balancing of conflicting values, Tbilisi, 2007.
12. *Danelia N.,* Coverage of children's issues in the Georgian television space, Media Development Fund, Tbilisi, 2011.
13. *Eremadze K*., Basic rights for freedom, book two, 2021.
14. *Ivanidze M*., A minor and his best interests, analysis of the legislation of minors and judicial practice, Tbilisi, 2017.
15. *Imerlishvili I.,* Minors' rights: international experience and the current situation in Georgia, in the collection: Protection of human rights, constitutional reform and the rule of law in Georgia, Tbilisi., 2017.

16. *Kopaleishvili M*., The balance established by the constitution between the right of public access to judicial acts and the right to protect personal data from access, research and recommendations on the need for legislative regulation in accordance with the decision of the Constitutional Court, 2020.
17. Pachulia T., Dangers of sharing personal data of minors on the Internet, in the collection: current problems and challenges of personal data protection, Toloraya L., Firtskhalashvili A. (Ed.), 2021.
18. *Kvrivishvili T.,* Guarantees of personal life protection of minors in conflict with the law, Tbilisi, 2022.
19. *Shalikashvili M., Mikanadze G*., Juvenile justice (manual), second edition, Tbilisi, Freiburg, Strasbourg, 2016.
20. Shekhiladze Kh., Prioritizing the best interests of minors in conflict with the law in the process of juvenile justice (criminal proceedings), Tbilisi, 2019.
21. *Sarkeulidze I.*, Juvenile crime and its causes in juvenile justice systems, Law Journal, No. 2, 2013.
22. *Khidesheli S*., Protection of children's rights in the media - an important aspect of the formation of a democratic state, in the collection: Protection of human rights and democratic transformation of the state, Korkelia K. (Ed.), Tbilisi, 2020.
23. *Jorbenadze S., Bakhtadze U., Macharadze* Z., media law, *Jorbenadze S*. (Ed.), Tbilisi., 2014.
24. Hamilton st. Guidelines for Juvenile Justice Law Reform, 2011.
25. Rosenthal, L. Jacobson, Pygmalion im Unterricht. Lehrererwartungen und Inteligentwicklung der Schüler. Beltz, 1983.
26. Decision No. 2/6/1311 of the Constitutional Court of Georgia dated December 17, 2019 in the case of “Stereo+ LLC”, Luka Severin, Lasha Zilfimiani, Robert Khakhalev and Davit Zilfimiani against the Parliament of Georgia and the Minister of Justice of Georgia.
27. Decision No. 1/4/693,857 of the Constitutional Court of Georgia dated June 7, 2019 in the case “Media Development Fund” and Freedom of Information Development Institute” against the Parliament of Georgia.Handyside v United Kingdom [1976] ECHR 5 at para. 48, (1976) 1 EHRR 737, [1976] ECHR 5493/72 (7 December 1976), European Court of Human Rights.
28. S. and Marper v. The United Kingdom, [2008] ECHR, nos. 30562/04 and 30566/04.

Luka Pavlenishvili*

Supervision and Control of Covert Investigative Actions by the Personal Data Protection Service of Georgia

The article examines the legality and oversight of personal data processing in the context of covert investigative activities, with a focus on evaluating the effectiveness and alignment of the current control mechanisms with international standards.

Specifically, the article assesses the mandate and authority of the Personal Data Protection Service (hereafter - PDPS) in supervising and regulating such activities. This issue has gained particular significance following the enactment of Georgia's new law "On Personal Data Protection," which granted the PDPS the authority to assess the legality of data processing classified as a state secret.

***Keywords**: personal data, covert investigative activities, oversight mechanisms, Criminal Procedure Code, Law of Georgia "On Personal Data Protection".*

1. Introduction

In the digital age, where individuals leave a pervasive digital footprint, the assessment of the legality of data processing in specific cases often falls outside the strict boundaries of legal regulation. Particular attention is warranted when it comes to covert investigative activities, especially given their association with the investigation of serious or particularly serious crimes. Such investigative actions frequently involve the processing of large volumes of diverse types of data, necessitating strict compliance with both criminal procedural law and personal data protection legislation. In these cases, adherence to the principle of data minimization is crucial.

The principle of data minimization in the context of covert investigations extends beyond being a mere organizational, technical, or procedural issue;

It is important to note that while the control of covert investigative activities is not governed by the General Data Protection Regulation (GDPR), it is regulated by the Law Enforcement Directive (LED), which sets specific rules for the processing of personal data within the police and law enforcement sector. The newly enacted law "On Personal Data Protection" of Georgia, which came into force on March 1, 2024, is largely aligned with international standards, including those set forth by the LED.

The LED outlines key principles for the processing of personal data in the context of preventing, investigating, detecting, or prosecuting criminal offenses by law enforcement

* Master's Student at Ilia State University, Faculty of Law (Criminal Law). Junior Lawyer at the Legal Department of the Personal Data Protection Service of Georgia.

agencies. These principles include legality, fairness, transparency, respect for human dignity, processing for a specifically defined and legitimate purpose, data minimization, data accuracy, limited retention periods, and robust data security measures. These guidelines ensure that investigative data processing operations are necessary, proportionate, and conducted in a manner that upholds individuals' rights and freedoms.[1]

The purpose of this study is to examine the legal framework governing the oversight of covert investigative activities. The study will explore the principle of data minimization, along with best practices and methodologies that are of particular relevance following the implementation of Georgia's new law "On Personal Data Protection." Emphasis will be placed on the role of law enforcement agencies in balancing their operational needs with the protection of fundamental rights and freedoms in a democratic society.

2. Legal framework for Conducting Covert Investigative Action

The legal framework governing the interaction between covert investigative actions conducted by law enforcement agencies and the protection of personal data is inherently complex. Harmonizing this process with the law presents significant challenges, yet it is essential for safeguarding the fundamental human right to privacy.

Covert investigative actions, or operational-search measures, serve as an Ultima Ratio, allowing for the collection of evidence through various methods or techniques, naturally without prior notification to the individuals involved.[2] These actions are carried out by the Operational-Technical Agency of the State Security Service and pertain to specific crimes investigated by the authorities outlined in Article 34(1) of the Criminal Procedure Code.[3]

Unlike other investigative measures, covert investigative actions are reserved for serious or particularly serious crimes, as well as certain offenses listed under Article 143^3(2)(a) of the Criminal Procedure Code. The crimes eligible for such investigative actions include, but are not limited to:

- Crimes against health;
- Threats to life and health;
- Crimes against sexual freedom and inviolability;
- Crimes against human rights and freedoms;
- Economic crimes;
- Crimes against entrepreneurial or other economic activities;
- Crimes within the monetary and credit system;
- Crimes against public health and morality;
- Cybercrime;
- Crimes against environmental protection and the use of natural resources;
- Crimes against the constitutional order and national security of Georgia;
- Violations of the legal regime in occupied territories;
- Official misconduct.

In addition to defining these investigative actions, it is essential to consider the legitimate objectives that warrant their use, namely:

[1] Article 4 of the Law Enforcement Directive (LED).
[2] *Akubardia I.,* Control mechanisms over secret investigative actions, collection of articles - Revaz Gogshelidze 65, Tbilisi, 2022, 200.
[3] Article 34(1) of the Criminal Procedure Code of Georgia.

- Ensuring national security;
- Ensuring public safety;
- Preventing public disorder;
- Preventing crime;
- Protecting the country's economic well-being;
- Protecting the rights and freedoms of others.

The scope and intensity of covert investigative actions must be proportionate to these legitimate goals, aligning with the general requirements of international human rights law, the jurisprudence of the European Court of Human Rights (ECtHR), and other international or regional legal standards.[4]

In line with the conclusions of the Legal Issues Committee on recent legislative amendments, the ECtHR has underscored the state's discretionary power in determining the duration of covert investigative actions. Extending the timeframe for such actions to achieve legitimate objectives, including public order protection and effective crime prevention, may be justified as long as necessary, provided there is appropriate oversight and due process guarantees.[5]

Any covert investigative action conducted for a legitimate purpose is intended to gather evidence relevant to a criminal case. However, the mere necessity of obtaining such evidence or preventing a crime is not, in itself, sufficient grounds for a court to authorize such measures. The requesting party must also demonstrate that obtaining the evidence or achieving the objective through other investigative or procedural means is either impossible or would require an unreasonable level of effort.[6]

The burden of proof to meet these standards lies with the state prosecutor, who petitions the court to authorize covert investigative actions. The prosecutor's request must be considered by the court within 24 hours, after which the judge decides whether to grant or deny the request. The judge's decision is issued in four copies: two for the prosecutor, one for the court, and one copy, containing only the operative details and resolution, is delivered to the PDPS in physical form within 48 hours.

Covert investigative actions may also be conducted under urgent circumstances, in which case the prosecutor must send one copy of the resolution to the PDPS.

3. Control Over Covert Investigative Actions and Activities Carried out in the Central Bank of Electronic Communication Identifying Data

3.1. Mandate of the Personal Data Protection Service

The oversight of the legality of personal data processing in Georgia dates back to 2013. With the legislative amendments introduced in 2014, the scope of the Law of Georgia on Personal Data Protection was expanded to cover the automatic processing of data classified

[4] *Fafiashvili L., Tumanishvili G*. and others, Commentary of Criminal Procedure Code Georgia (as of October 1, 2015), Tbilisi., 2015, 428-429.

[5] Conclusion of the Committee on Legal Issues "On Amendments to the Criminal Procedure Code of Georgia" on the Law of Georgia (No. 1614-VIIIms-Xmp, 7/06/2022) regarding the motivated remarks of the President of Georgia (No. 07-1/14, 23/06/2022).

[6] *Fafiashvili L., Tumanishvili G.* and others, Commentary of Criminal Procedure Code Georgia (as of October 1, 2015), Tbilisi., 2015, 429.

as state secrets for the purposes of crime prevention, investigation, operational-search measures, and law enforcement. At that time, the Personal Data Protection Inspector was granted the authority to oversee covert investigative actions, as well as the activities conducted within the data banks of law enforcement bodies. Following further legislative changes, effective from March 31, 2015, the Personal Data Protection Inspector was empowered to supervise investigative actions outlined in Articles 136-138 and subsections "a" and "b" of Article 143^1(1) of the Criminal Procedure Code of Georgia.[7]

From 2019 to 2022, these functions were assumed by the State Inspector Service, the successor of the Personal Data Protection Inspector.

As of March 1, 2022, the mandate for overseeing such activities was transferred to the PDPS. One of its core responsibilities is the supervision and enforcement of personal data protection regulations in Georgia, including the monitoring of the legality of data processing.

In any democratic state, it is essential to ensure the legality of covert investigative activities conducted by law enforcement agencies, particularly when processing personal data or accessing identifiable electronic communication data.

3.2. Oversight Mechanism

As previously noted, one of the key functions of PDPS is to oversee activities conducted within the central database of electronic communication identification data and covert investigative actions. This oversight can be viewed as a safeguard against abuse, given that covert investigative actions are inherently sensitive and may become a tool for severe infringements on fundamental rights, which the state itself is responsible for protecting.

PDPS supervises covert investigative actions as outlined in Article 143^1(1) of the Criminal Procedure Code of Georgia and ensures compliance with the provisions set forth in Chapter XVI^1 of the same Code. To fulfill its mandate, PDPS is granted 24-hour access to the essential information and portions of court rulings authorizing covert investigative activities. In cases of urgent necessity, it also receives the essential details and portions of prosecutor's resolutions authorizing covert investigative actions, along with protocols prepared by law enforcement agencies regarding such actions.

Additionally, PDPS receives notifications from electronic communications companies regarding the transfer of personally identifiable communication data to law enforcement agencies. Upon receiving this documentation, PDPS cross-references the information with electronic systems, records the relevant data in its internal system for documenting covert investigative actions, and conducts an analysis. Beyond these mechanisms, PDPS employs electronic and specialized control systems to monitor covert investigative activities—specifically, the covert monitoring and recording of telephone communications. An electronic control system is also used to oversee activities within the central database of electronic communication identification data.[8]

Furthermore, PDPS ensures the legality of data processing within the central database of electronic communication identification data through its control system, which includes conducting checks and inspections of the data processor or authorized individual responsible for data handling.[9]

[7] Office of the Personal Data Protection Inspector 2015 Report, 34.
[8] Activity statistics of the Personal Data Protection Service for 12 months of 2023 (January-December), 7.
[9] Law of Georgia "On Personal Data Protection", 14/06/2023, Article 49, subsection "c".

3.3. Statistical Information

It is noteworthy that, in an effort to establish uniform methodologies for producing statistical data within PDPS and to introduce relevant standards, a comprehensive methodology has been developed to summarize and analyze statistical data on the Service's activities.[10]

For example, PDPS's statistics from the previous year indicate that the mechanism for halting the covert monitoring and recording of telephone communications (via the electronic control system) was employed in 76 instances. These interruptions were due to the delayed submission of court decisions (74 cases), an illegal notification of covert investigative actions initiated by the prosecutor's resolution in urgent circumstances (1 case), and the termination of a covert investigative action (1 case).

Key data points include:

- Covert monitoring and recording of telephone communications: The court considered 859 petitions, of which 87% (744) were fully approved, 9% (80) were denied, and 4% (35) were partially approved.
- Extension of telephone communication surveillance and recording periods: The court reviewed 228 petitions, approving 87% (199), partially approving 9% (21), and rejecting 4% (8).
- Covert video and/or audio recording and photography: The court evaluated 1,024 motions, fully approving 93% (952), rejecting 6.6% (68), and partially approving 0.4% (4).
- Extension of covert video and/or audio recording and photography periods: The court reviewed 120 petitions, of which 87% (105) were approved, 11% (13) were rejected, and 2% (2) were partially approved.
- Removal and fixation of information from communication channels or computer systems: The court considered 3 petitions, approving 1 and rejecting 2.
- Collection of internet traffic data: The court reviewed and approved 1 petition for the ongoing collection of internet traffic data.
- Prosecutor's resolutions on urgent covert investigative actions: PDPS received 92 resolutions, of which 83% (76) were for covert video and/or audio recording and photography, and 17% (16) were for covert telephone communication monitoring and recording. Court rulings and prosecutor's resolutions under Article 136 of the Criminal Procedure Code: Of the documents submitted, 2% were prosecutors' resolutions and 98% were court decisions, totaling 1,490 court rulings. Additionally, PDPS received 34 prosecutor's resolutions regarding urgent investigative actions under Article 136.
- Notifications to the "Operational-Technical Agency of Georgia": PDPS notified the Agency 6 times regarding ambiguities or inaccuracies in court-issued permits for

[10] Methodology for production of annual statistics on the state of personal data protection, conduct of covert investigative actions and control of activity carried out in the central bank of electronic communication identifying data, 2024.

covert telephone communication monitoring and recording (via the electronic control system).

- Monitoring through the electronic control system: No incidents were detected during the covert monitoring and recording of telephone communications.
- Data issued by the Central Bank of Identifying Data of Electronic Communication: The Operational-Technical Agency issued data 71 times, based on relevant court decisions.
- Oversight of the Central Bank of Identifying Data of Electronic Communication: No errors or incidents were detected during the oversight of activities conducted within the Central Bank.[11]

The rise in these statistics, compared to previous reports, reflects the increased efficiency of PDPS and the strengthening of its mandate. This development is a positive step forward, as an area once beyond legal oversight has now come under regulatory supervision. Notably, the 2016 report highlighted that, in six cases, a copy of the resolution was not submitted to the supervisory body. The Chief Prosecutor's Office attributed this to time constraints and the high volume of investigative actions conducted in response to urgent needs. Additionally, in the same year, three instances of late submission of resolutions were identified.[12]

3.4. Destruction of Information Obtained through Covert Investigative Action

The information obtained from covert investigative actions is destroyed by the supervisor of the relevant case investigation, the state prosecution supporter, or their superior prosecutor. This process takes place in the presence of the judge who authorized the covert investigative action or, in cases of urgent necessity, the judge who retrospectively approved the action. The destruction of such information is conducted regardless of whether the investigative activity was deemed legal or illegal. A protocol documenting the destruction of the material, signed by the responsible prosecutor and judge, is then submitted to PDPS and recorded in the court's register of covert investigative actions.[13]

The Law Enforcement Directive (LED) provides an intriguing perspective on the destruction of information gathered during covert investigative activities. According to the LED, Member States must establish appropriate time limits for the deletion of personal data and periodically review the necessity of retaining such data. The enforcement of these time limits must be ensured through procedural safeguards, which can be seen as closely aligning with the Georgian model.

4. International Standards

4.1. Regulatory Bodies

During the conduct of covert investigative actions, the subject of such actions is granted the opportunity to fully protect their rights only after the conclusion of the covert operation.

[11] Activity statistics of the Personal Data Protection Service for 12 months of 2023 (January-December), 9.

[12] 2016 report on the state of personal data protection and inspector's activities, <https://old.pdps.ge/ka/download/2870> [05.08.2024].

[13] *Akubardia I.,* Control mechanisms over secret investigative actions, collection of articles - Revaz Gogshelidze 65, Tbilisi, 2022, 228.

Therefore, it is crucial to monitor the actions of the executing body during the course of the operation. Proper oversight before notifying the subject of the investigative actions serves as the sole legal safeguard protecting individuals and third parties from potential abuse of power.

Surveillance and other covert measures are typically carried out by national security services. In Georgia, for instance, the Operational-Technical Agency operates under the State Security Service. The supervisory authorities overseeing the activities of security services vary across countries. Research documents from international bodies such as the United Nations, Council of Europe, and Venice Commission outline best practices and provide key recommendations for the establishment and effective operation of supervisory institutions.

According to a 2015 research report by the Council of Europe, no member state's supervisory system fully adheres to internationally recognized standards and principles. There is also no universally accepted model for effective oversight. However, certain practices and approaches stand out from a human rights perspective.[14] The report highlights that, within Council of Europe member states, the supervisory authorities for security services include parliamentary committees, independent supervisory institutions, courts, and quasi-judicial bodies.

4.2. Practice of the European Court of Human Rights

a. Roman Zakharov and Others v. Russia[15]

The applicant, who was the editor-in-chief of a publishing company, initiated legal proceedings against three mobile network operators, alleging interference with his right to privacy in telephone communications. He claimed that under the applicable national legislation, mobile network operators had installed equipment that allowed the Federal Security Service (FSB) to monitor telephone communications without prior judicial authorization. The applicant sought to have the equipment removed and to restrict access to telecommunications to authorized individuals only.

The national courts rejected the applicant's request, ruling that he had not provided sufficient proof that his telephone conversations had been monitored or that the mobile network operators had shared information with unauthorized parties. The court further found that the mere installation of the system or equipment did not in itself constitute a violation of the security of his communications.

Before the European Court of Human Rights, the applicant contended that Russia's system of secret surveillance of mobile phone communications did not comply with the requirements set forth in Article 8 of the European Convention on Human Rights. On 11 March 2014, the Trial Chamber relinquished jurisdiction in favor of the Grand Chamber.

In this case, the challenged legislation had a direct impact on all mobile phone service users, as it established a covert surveillance system where anyone using a national carrier's mobile service could be subject to surveillance without ever being informed. Moreover, national legislation failed to provide effective protection for individuals suspected of being

[14] Council of Europe Commissioner for Human Rights, Democratic and Effective Oversight of National Security Services, 2015, 8, <https://rm.coe.int/1680487770> [31.07.2024].
[15] *Case of Roman Zakharov v. Russia*, (Application no. 47143/06), <hudoc.echr.coe> [31.07.2024].

monitored. Therefore, assessing the relevant legislation in abstracto was justified, meaning that the applicant did not need to demonstrate a personal risk of surveillance. He was entitled to claim victim status under the Convention.

In this ruling, the issue of supervision was critical. The national legislation's ban on the registration and recording of surveillance rendered it impossible for supervisory bodies to identify cases where surveillance had been conducted without judicial authorization. Despite the fact that the competent authorities possessed the technical capability to conduct direct surveillance, this legal provision rendered any supervisory mechanism in the country ineffective, as it deprived authorities of the ability to check the legality of the surveillance.

Although the legal framework theoretically provided for some level of prosecutorial oversight, in practice, the legislation failed to establish adequate and effective safeguards against arbitrary actions.

b. Podchasov v. Russia[16]

On February 13, 2024, the European Court of Human Rights delivered its judgment in the case of *Podchasov v. Russia*, addressing the critical issue of indefinite access to electronic communication systems by law enforcement agencies, particularly regarding access to the "weak encryption mechanism" of correspondence and its content.

Under the provisions of the Code of Criminal Procedure of the Russian Federation and the Act on Operative-Investigative Activities, electronic communication companies were mandated to store communication data for one year and their content for six months. Additionally, data, including information that could assist law enforcement in deciphering communications, was to be provided to electronic communication companies upon request.

In this case, the Federal State Security Service of Russia requested that the electronic communication company "Telegram" submit system information that would enable the service to decrypt communications linked to six mobile numbers. Notably, the users of these numbers had utilized the "secret correspondence" function of the "Telegram" platform to encrypt their messages.

The complainant contended that the indefinite access granted to law enforcement authorities was in violation of Article 8 of the European Convention on Human Rights.

The Court emphasized the importance of mechanisms ensuring the privacy of electronic communications in the digital age, including encryption measures that facilitate the protection of fundamental rights. It recognized that encryption enables users to safeguard their data and prevent the disclosure of confidential information. The Strasbourg Court found the requirement to decrypt data stored within an electronic communication system to be disproportionate, as the national legislation lacked provisions for appropriate and sufficient justification.

The Court underscored that protecting personal data is vital for the realization of an individual's right to respect for private and family life. National law must provide adequate safeguards to prevent the processing of personal data that contravenes Article 8 of the Convention. Such measures are particularly crucial when data is automatically processed for law enforcement purposes. The Court further clarified that interference in areas protected by Article 8, for law enforcement reasons, must not rely solely on modern technologies in a

[16] The European Court of Human Rights made a decision on the inadmissibility of groundless and indefinite access to the electronic communication system by law enforcement agencies, see <pdps.ge/ka> [31.07.2024], referred to: Case of Podchasov v. Russia, Application no. 33696/19, 13 February 2024.

disproportionate manner. Therefore, clear and detailed rules governing data storage, usage, and access are necessary. Additionally, the duration of data retention should be proportionate to the legitimate purpose of collection.

In assessing the factual circumstances of the case, the European Court of Human Rights noted that the long-term retention of all data and metadata in the system would impact all users of Internet communications, regardless of any suspicion regarding their involvement in criminal activities. Thus, the Court determined that the requirement for data retention and access infringed upon data confidentiality and failed to provide sufficient protections for the rights of data subjects.

Consequently, the Court concluded that the national legislation, which mandated the storage of communications from all Internet users and permitted direct access by security services to electronic communication systems without adequate data protection guarantees, could not be deemed necessary in a democratic society. As a result, the Court found a violation of Article 8 of the European Convention on Human Rights.

Members of the European Parliament emphasized the necessity for both ex ante and ex post supervision, aligning with the Court's approach.[17]

c. Ekimdzhiev and Others v. Bulgaria[18]

The case of *Ekimdziev et al. v. Bulgaria* addresses the inadequacy of legal safeguards against illegality and abuse of power concerning covert surveillance, as well as the storage and access to data obtained through wiretapping.

Factual Circumstances: The plaintiffs consist of two lawyers and two non-governmental organizations associated with them. They assert that they are at risk of surveillance and interception of communications by the Bulgarian state based on their activities and the existing Bulgarian legislation on surveillance and its practical application. Notably, the plaintiffs do not claim that state authorities have conducted surveillance or wiretapping of their communications.

Evaluation by the European Court: The European Court of Human Rights reviewed the application of Bulgarian legislation regarding surreptitious surveillance, acknowledging significant improvements since its prior decision in the case of *Association for European Integration and Human Rights and Ekimdzievi v. Bulgaria*. However, the Court concluded that the legislation did not meet the minimum standards of protection against illegality and abuse of power required by Article 8 of the Convention.

A crucial aspect of the Court's evaluation pertains to the issue of supervision. It found that national legislation failed to establish clear rules governing the storage, access, review, use, communication, and destruction of communication data. Such data was retained within criminal cases, accessible to anyone, which resulted in inadequate protection and created a substantial risk of disproportionate intrusion into the personal lives or correspondence of individuals and legal entities.

[17] European Parliament Resolution of 12 March 2014 on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs (2013/2188(INI)).

[18] Case of Ekimdzhiev and Others v. Bulgaria, (Application no. 70078/12), <https://hudoc.echr.coe.int/fre#{%22itemid%22:[%22001-214673%22]}> [05.08.2024].

Furthermore, the existing supervisory framework was deemed incapable of effectively assessing potential abuses of power. Although the Personal Data Protection Commission possessed the authority to examine data collection practices by communications service providers, it lacked the capacity to scrutinize the actions of public authorities with access to such data.

Consequently, the European Court determined that the current Bulgarian legislation regarding the storage and access to data obtained from communication interception did not fully comply with the requirement of "law," thus failing to ensure that any "interference" was "necessary in a democratic society." This inadequacy resulted in a violation of Article 8 of the European Convention on Human Rights.

5. Conclusion

Ensuring the inviolability of an individual's right to private life, as protected by Article 15 of the Constitution of Georgia, stands as one of the paramount responsibilities of a democratic state. This right serves as the foundation for human growth and development, allowing individuals to flourish as persons. It functions as a shield through which citizens can express their opinions, embrace individuality, and hold diverse perspectives without facing negative repercussions. Consequently, the investigative activities undertaken by law enforcement agencies, particularly covert investigative actions, necessitate meticulous oversight and various legislative safeguards. This highlights the importance of enhancing and linking the mandate of the Personal Data Protection Service to established Western practices.

This is evidenced by the annual reports and statistics published by the Service, as well as the high rate of implementation of recommendations from international organizations discussed in the article. Such accomplishments position the Personal Data Protection Service as a robust supervisory mechanism for ensuring the effectiveness of covert investigative actions.

Bibliography:

1. Law of Georgia "On Personal Data Protection", 14/06/2023;
2. Criminal Procedure Code of Georgia, 09/10/2009.
3. Article 4 of the Directive on the processing of personal data in the police sector;
4. Conclusion of the Legal Issue Committee "On Amendments to the Criminal Procedure Code of Georgia" on the Law of Georgia (No. 1614-VIIIms-Xmp, 7/06/2022) regarding the motivated remarks of the President of Georgia (No. 07-1/14, 23/06/2022);
5. *Akubardia I.,* Control mechanisms over secret investigative actions, collection of articles - Revaz Gogshelidze 65, volume, 2022, 200, 228;
6. Council of Europe Commissioner for Human Rights, Democratic and Efective Oversight of National Security Services, 2015, 8, <https://rm.coe.int/1680487770> [31.07.2024].
7. European Parliament Resolution of 12 March 2014 on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs (2013/2188(INI));
8. *Fafiashvili L., Tumanishvili G*. and others, Criminal Procedure Commentary of Georgia (as of October 1, 2015), Tb., 2015, 428-429;
9. Personal Data Protection Inspectorate Office 2015 Report, 34;

10. Statistics of the activity of the Personal Data Protection Service for 12 months of 2023 (January-December), 7, 9.Council of Europe Commissioner for Human Rights, Democratic and Effective Oversight of National Security Services, 2015, 8, <https://rm.coe.int/1680487770> [31.07.2024];
11. *Case of Roman Zakharov v. Russia*, (Application no. 47143/06);
12. *Case of Podchasov v. Russia,* Application no. 33696/19, 13 February 2024.

Mariam Shaishmelashvili*

Protection of Personal Data in Consumer Relations (Review of International and National Standards)

In light of the development of modern trade relations, the refinement of trade relations has become an urgent necessity. This refinement is inconceivable without the implementation of high standards for consumer rights protection, a process that involves identifying the need for the processing of consumers' personal data. Such processing serves as the basis for both marketing activities and the establishment of rights and obligations outlined in consumer contracts.

It is noteworthy that the state has enacted two new special laws aligned with European directives in both of these fields: the Law of Georgia "On the Protection of Consumer Rights" dated June 1, 2022, and the Law of Georgia "On Personal Data Protection" dated June 14, 2023.

This article will examine the legal guarantees governing consumer relations established by the Law of Georgia "On Protection of Consumer Rights" and the Law of Georgia "On Personal Data Protection," along with the European directives upon which these legislative acts are based.

Keywords: *consumer, trader, personal data, consumer relation, personal data protection.*

1. Introduction

In the modern era, marked by the rapid development of trade relations, the need to refine legal regulations has become increasingly essential. It is precisely these legal regulations that provide the necessary guarantees to swiftly and effectively address both current and future challenges.

The flexibility of trade relations is driven by two key factors: technological advancements, on the one hand, and legal regulations that ensure the security of the parties involved in these relations, on the other.

As a private legal relationship, trade relations are inherently complex, and the protection of the parties' rights is ensured by several branches of law. Among these, it is

* PhD Student at Ivane Javakhishvili Tbilisi State University, Faculty of Law, Head of the training research center of the Georgian Competition and Consumer Protection Agency.

particularly important to highlight the protection of consumer rights and the interaction of personal data protection standards within the framework of consumer relations.

The Law of Georgia "On Personal Data Protection"[1] was adopted in 2011, and the Law of Georgia "On the Protection of Consumer Rights"[2] was enacted in 1996, establishing general standards. On July 18, 2014, Georgia signed the Association Agreement with the European Union[3] (hereinafter referred to as the "Association Agreement"), which entered into full force on July 1, 2016. From September 1, 2014, the trade-related provisions of the agreement, including the Deep and Comprehensive Free Trade Area (hereinafter referred to as "DCFTA")[4] with the European Union, commenced implementation. Georgia committed to aligning its national legislation with the obligations set forth in the agreement.

As a result of this ongoing process, new versions of special laws, in accordance with European standards, were developed in both fields of law to ensure a high level of protection for the subjects of legal relations.

Undoubtedly, a significant portion of the country's development is rooted in free trade relations, which are further bolstered by the DCFTA[5]. Modern trade relations, characterized by the exchange and processing of vast amounts of information, are becoming increasingly flexible.

On the other hand, personal data protection legislation provides crucial safeguards[6] for the processing of data within trade relations, confirming the interconnection between these two fields.

2. Legal Safeguards for the Protection of Consumers Rights

Consumer relations significantly impact the daily life of society due to the wide range of issues and relationships encompassed within this field. For this reason, the protection of consumer rights is essential, relevant, and fundamental for developed countries.

On March 20, 1996, the Parliament of Georgia adopted the Law of Georgia "On the Protection of Consumer Rights." This law was repealed on May 8, 2012, and the current Law "On the Protection of Consumer Rights" came into force on June 1, 2022[7].

The new Law of Georgia "On the Protection of Consumer Rights"[8] aligns with many European directives[9], and the process of convergence with the latest directives is ongoing.

[1] Law of Georgia "On Personal Data Protection", №5669, 28/12/2011.
[2] Law of Georgia "On the Protection of Consumer Rights", No. 151, 20/03/1996.
[3] Association Agreement between Georgia on the one hand and the European Union and the European Atomic Energy Union and their member states on the other hand <https://matsne.gov.ge/ka/document/view/2496959?publication=4> [29.07.2024] .
[4] Free trade with the European Union, <https://dcfta.gov.ge/ge/agreement> [29.07.2024].
[5] Free trade with the European Union, <https://dcfta.gov.ge/ge/agreement> [29.07.2024].
[6] Law of Georgia "On Personal Data Protection", No. №3144-XIმს-Xმპ, 14/06/2023, Article 12.
[7] Law of Georgia "On the Protection of Consumer Rights", №1455-VIIIმს-Xმპ, 29/03/2022
[8] Law of Georgia "On the Protection of Consumer Rights", №1455-VIIIმს-Xმპ, 29/03/2022
[9] Noteworthy:
- Directive of the European Parliament and the Council of October 25, 2011 on "Consumer Rights", which replaces the Directives 92/13 of the Council and 1999/44 of the European Parliament and Directive 97/7 of the European Parliament and the Council;
- Directive 98/6/EC of the European Parliament and the Council of February 16, 1998 "On consumer protection in the indication of prices for products offered to consumers";

This law establishes the general principles for the protection of consumer rights in legal relationships with traders for the use of goods or services for personal consumption[10]. Among the rights and prohibited actions outlined in the Law of Georgia "On the Protection of Consumer Rights", Article 24, which prohibits unfair commercial practices. Unfair commercial activity is defined as activity that contradicts the principles of good faith and significantly alters, or is likely to alter, the economic behavior of the average consumer concerning the goods or services offered or intended for them. It also includes activities that adversely affect the economic behavior of the average member of a group of consumers when the target of the commercial activity is a defined group of consumers. Unfair commercial practices include misleading or aggressive commercial activities. Pursuant to Article 27, section 1, subsection "c" of this law, it is considered unfair and prohibited to systematically make unsolicited offers to customers by telephone or other remote communication methods, except when necessary to fulfill contractual obligations.

It should be noted that in order for the actions stipulated in Articles 24 and 27 to be deemed inconsistent with the Law "On the Protection of Consumer Rights," several conditions must be met. Specifically, the disputed action must be that of the trader, it must harm the collective interest of a broad group of consumers, and it must be contrary to the law.

The basis of the aforementioned prohibition lies in the fact that direct marketing, which conveys advertising content and aims to sell or promote the sale of goods or services, as well as to influence the economic behavior of the recipient, constitutes an effort to impact the consumer and encourage the use of their financial resources for the purchase of goods or services.

It is important to highlight that advertising possesses two essential characteristics: the information must pertain to the recipient's economic, commercial, financial, or professional activities, and the information provided must encourage the purchase or use of goods[11]. Accordingly, the violation mentioned above is a serious matter and is also addressed by Directive 2005/29/EC of the European Parliament and Council "On Unfair Commercial Practices.".[12]

It is clear that a trader cannot make the offer outlined in subparagraph "c" of the first paragraph of Article 27 without processing the personal data of consumers. This processing is regulated by Article 12 of the Law of Georgia "On Personal Data Protection," which provides safeguards for the processing of personal data in the context of direct marketing.

- Directive 2005/29/EC of the European Parliament and the Council of May 11, 2005 "On unfair business-to-consumer commercial practices in the internal market" ("Unfair Commercial Practices Directive");
- Directive 1999/44/EC of the European Parliament and the Council of May 25, 1999 "On certain aspects of the sale of consumer goods and related guarantees";
- Council Directive 93/13/EEC of April 5, 1993 "On unfair terms in consumer contracts";
- Directive 2009/22/EC of the European Parliament and the Council of April 23, 2009 "On Measures to Protect Consumer Interests";
- Regulation of October 27, 2004 "On cooperation between national authorities responsible for the enforcement of laws on consumer protection (Regulation on cooperation in the field of consumer protection)", with respect to which national legislation should be brought closer to the following articles: 3 (c); 4(3) – (7); 13 (3); 13(4).

[10] Law of Georgia "On the Protection of Consumer Rights", №1455-VIIIმს-Xმპ, 29/03/2022, Article 2 (1),

[11] Decision No. 04/141 of the National Competition Agency of Georgia dated March 22, 2023, <https://gcca.gov.ge/uploads_script/user_rights/tmp/php8oEZGi.pdf> [29.07.2024].

[12] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005, Annex 1, 26, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02005L0029-20220528&qid=1673608274813> [29.07.2024].

Furthermore, according to European Union principles, the state must provide consumers with a flexible and efficient mechanism for the protection of their rights. The protection of consumer rights through an effective legislative framework will contribute to safeguarding the economic interests of citizens and promote consumer awareness of their rights and their ability to demand such protections. To this end, the legislator designated the main enforcement body of the law as the Competition and Consumer Protection Agency of Georgia, which is responsible for "protecting consumer rights." The agency considers complaints regarding potential violations of the "Consumer Protection Law" and makes a decision within one month or within three months in cases of complexity.[13]

3. Legal Safeguards of Personal Data Protection

Given that the harmonization and consolidation of personal data protection legislation is a commitment undertaken by Georgia under the Association Agreement with the European Union and the Association Agenda, a new law "On Personal Data Protection" was adopted in 2023 to fulfill this obligation. This law is based on the European Union's General Data Protection Regulation (GDPR), the Council of Europe Convention 108 and its Additional Protocol, as well as EU Framework Decision 2008/977/JHA of November 27, 2008, and Recommendation No. R (87)15 of the Committee of Ministers of the Council of Europe, dated November 15, 1987. Furthermore, in accordance with the "Roadmap for Georgia's EU Integration," one of the key future directions is to further align Georgia's data protection legislation with the latest European data protection standards.[14]

As a counterpart to Articles 24 and 27 of the Law of Georgia "On the Protection of Consumer Rights," Article 8 of the previous version[15] of the Law of Georgia "On Personal Data Protection" provided the following regulation: for the purposes of direct marketing, it was permissible to process data obtained from publicly available sources, regardless of the purpose for which the data were collected. Only specific data, such as name(s), address, telephone number, e-mail address, and fax number, could be processed for direct marketing purposes, and only with the written consent of the data subject as required by the law.

The data subject had the right to request that the data controller cease using their data for direct marketing purposes at any time. In response, the data controller was obligated to halt the processing of the data for such purposes and ensure that processor also ceased processing within 10 working days of receiving the request.

When processing data for direct marketing purposes, the data controller was required to inform the data subject of this right and ensure that the data subject could request the cessation of data processing for direct marketing purposes in the same form in which the direct marketing was conducted. Additionally, the controller had to establish an accessible and adequate means for the data subject to request termination of processing for direct marketing purposes.

In the new law, Article 12 introduces a higher standard for the processing of personal data for direct marketing purposes. Regardless of how the data were collected or their availability, personal data may only be processed for direct marketing purposes with the data

[13] Order No. 45 of the Chairman of the National Competition Agency of Georgia "On approval of the case study procedure and procedure", 29/09/2022, paragraphs 1 and 2 of Article 7.
[14] Law of Georgia "On Personal Data Protection №3144-XIმს-Xმპ, 14/06/2023.
[15] Law of Georgia "On Personal Data Protection №5669-რს, 28/12/2011.

subject's explicit consent. Before obtaining consent, the data controller or processor must explain to the data subject, in clear, simple, and comprehensible language, their right to withdraw consent at any time and the procedure for exercising this right. Additionally, while the previous law provided for a 10-day period for the processor to stop data processing upon the data subject's request, this period has been reduced to no more than 7 days under the new law.[16]

4. Practical Aspects of Personal Data Protection in Trade Relations

Despite their differing constitutional foundations[17], consumer rights protection and personal data protection law have increasingly converged through the process of harmonization with European legislation[18]. Modern trade relations have become digitalized, relying on the exchange of personal data. The regulation of distance trade is a significant achievement of the Law of Georgia "On the Protection of Consumer Rights," as this form of trade renders consumers vulnerable on one hand, while on the other, it makes trade relations more efficient by reducing the time, human effort, and financial resources required to purchase goods and services.

In the context of remote trade, the user/data subject is required to provide the trader with various pieces of information, including in some cases registering on the trader's website. The information shared may include email address, password, full name, bank card details, residential address, telephone number, and other personal details, without which the consumer would be unable to receive the purchased goods or services. Furthermore, traders may process additional data such as the amount of time spent on the website and the user's search history, which can be utilized for marketing purposes. The most crucial step before the exchange of such data is to ensure that the data subject/user is properly informed.

Articles 24 and 25 of the Law of Georgia "On Personal Data Protection" reinforce the mechanisms for ensuring the data subject's awareness, thus highlighting its importance. Article 24 outlines the information that must be provided to the data subject by the data controller when the data is collected directly from the subject, whereas Article 25 pertains to situations where the data is not collected directly from the data subject[19]. These provisions are in line with European standards, specifically the European Union's General Data Protection Regulation (GDPR)[20], which focuses on the proper means of informing consumers to enable them to make informed decisions. The principle of informed consent serves as the primary legal basis for the lawful processing of personal data. In addition, the GDPR provides a detailed list[21] of information that data subjects must be informed about, including the purposes of data processing and all other relevant information necessary to ensure the fairness of the process. The GDPR further establishes standards[22] regarding the form in which

[16] Law of Georgia "On Personal Data Protection №3144-XIმს-Xმპ, 14/06/2023, Article 12 (1).
[17] EU Charter of Fundamental Rights, Art. 7, <https://www.europarl.europa.eu/charter/pdf/text_en.pdf> [29.07.2024].
[18] *Zuiderveen Borgesius F., Helberger N., Reyna A.,* Common Market Law Review, Volume 54, Issue 5, 2017.
[19] Law of Georgia "On Personal Data Protection №3144-XIმს-Xმპ, 14/06/2023.
[20] General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council "On the protection of natural persons with regard to the processing of personal data and on the exchange of such data", 27/04/2016, Article 6, paragraph 1, subparagraph "a" <https://gdpr -info.eu/> [29.07.2024].
[21] Also, Article 14.
[22] Also, Article 14.

information must be provided, stipulating that data subjects must be informed in a concise, clear, and easily understandable manner, using straightforward language.

Articles 5, 6, and 10 of the Law of Georgia "On the Protection of Consumer Rights" establish a high standard of consumer awareness in trade and consumer relations. These provisions outline the information that must be provided in both distance and on-site trading. Notably, in the case of distance trading, the standard for informing the consumer is higher, as the consumer must be able to make a purchase decision based on an "informed choice" before committing to the purchase of goods or services. In such cases, essential information must be provided, including the main characteristics of the goods or services, tailored to the nature of the goods or services and the medium of communication (unless such information is self-evident from the context).[23]

In alignment with the standards set by the General Data Protection Regulation (GDPR), Article 5 of the Law "On the Protection of Consumer Rights" also mandates clarity in the provision of information. Specifically, it states: "Before concluding a contract, the trader is obligated to provide the consumer with the following clear and complete information in the state language of Georgia, in a manner that is clear and comprehensible (unless this information is self-evident)...".

This standard aligns with the European Parliament and Council Directive 2011/83/EC[24] of October 25, 2011 (hereinafter referred to as Directive 2011/83/EC), whose purpose is to enhance the proper functioning of the internal market by ensuring a high level of consumer protection. This is achieved by harmonizing certain aspects of the laws, regulations, and administrative provisions of the Member States relating to consumer contracts. Articles 5 and 6 of Chapter 3 of Directive 2011/83 outline the information that a trader must provide to the consumer before entering into a contract. Article 5 specifically details the information that must be provided to the consumer for all contracts, except for distance contracts. Furthermore, under Article 6(9) of Directive 2011/83, the burden of proof regarding the provision of information to the consumer rests entirely on the trader. Thus, in the event of a dispute between the parties, it is the trader's responsibility to demonstrate that they have fully met their obligations under the directive and provided the consumer with the appropriate level of information.

When examining the legality of processing personal data in consumer relations, it is essential to consider practical examples, such as a case study conducted by the National Competition Agency of Georgia. In one instance[25], the agency evaluated a possible violation of Articles 24 and 27 of the Law of Georgia "On the Protection of Consumer Rights" by a Trader. The consumer in question had reported receiving persistent short text messages with advertising content, and all attempts to stop these messages had been unsuccessful. According to the complainant, this form of aggressive commercial activity not only affected them personally but also impacted the interests of other consumers.

[23] Decision No. 04/612 of the Georgian Competition and Consumer Protection Agency of July 11, 2024, <https://gcca.gov.ge/uploads_script/user_rights/tmp/phpwMZgnd.pdf> [29.07.2024].

[24] On consumer rights, amending Council Directive 93/13/EEC and European Parliament and Council Directive 1999/44/EC and repealing Council Directive 85/577/EEC and European Parliament and Council Directive 97/7/EC, <https://matsne. gov.ge/ka/document/view/4488461?publication=0> [29.07.2024].

[25] Decision No. 04/141 of the National Competition Agency of Georgia dated March 22, 2023, <https://gcca.gov.ge/uploads_script/user_rights/tmp/php8oEZGi.pdf> [29.07.2024].

The agency also analyzed Directive 2005/29/EC of the European Parliament and Council "On Unfair Commercial Practices,"[26] which classifies persistent and unsolicited advertising through telephone, fax, email, or other remote means as an aggressive commercial practice, except in cases allowed by national legislation. Both Article 27(1)(c) of the Law and Directive 2005/29/EC consider the systematic sending of text messages with irritating and tiresome frequency as an aggressive commercial practice. Furthermore, the agency took into account that marketing text messages should pertain to the recipient's economic, commercial, financial, or professional activity and that the provided information should encourage the purchase or use of goods or services. In this specific case, the agency evaluated the frequency and content of the text messages sent by the trader. It concluded that the messages did not exhibit a systematic nature. Moreover, based on the evidence provided by the merchant, it was established that the consumer had given consent to receive marketing messages, and all marketing offers sent by the merchant included an opt-out mechanism. However, the consumer had not utilized the available means to unsubscribe. Consequently, the agency concluded that no violation of the Law of Georgia "On the Protection of Consumer Rights" had occurred in this case.

5. Conclusion

Based on the legal aspects discussed in this article, it can be concluded that the legal regulation of the two distinct fields of consumer rights protection and personal data protection complements each other, thereby ensuring the safeguarding of individual rights. The Law of Georgia "On Protection of Consumer Rights," which has been in effect for two years, has successfully established a high standard within the trade sphere. In conjunction with the new Law "On Protection of Personal Data," it creates a framework analogous to the European standards for the protection of consumer and data subject rights, which have been implemented in the majority of EU member states for decades.

Bibliography:

1. Association Agreement between Georgia, on the one hand, and the European Union and the European Atomic Energy Union and their member states, on the other hand, 27/06/2014, <https://matsne.gov.ge/ka/document/view/2496959? publication=4> [29.07.2024].
2. Decision No. 04/141 of the National Competition Agency of Georgia dated March 22, 2023, <https://gcca.gov.ge/uploads_script/user_rights/tmp/php8oEZGi.pdf> [29.07.2024].
3. Decision No. 04/612 of the Georgian Competition and Consumer Protection Agency of July 11, 2024, <https://gcca.gov.ge/uploads_script/user_rights/tmp/phpwMZgnd.pdf> [29.07.2024].
4. Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005, Annex 1, 26, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02005L0029-20220528&qid=1673608274813> [29.07.2024].

[26] Directive 2005/29/EC of the European Parliament and of the COUNCIL of 11 May 2005, Annex 1, 26, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02005L0029-20220528&qid=1673608274813> [29.07.2024].

5. EU Charter of Fundamental Rights, <https://www.europarl.europa.eu/charter/pdf/text_en.pdf> [29.07.2024].
6. General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council "On the protection of natural persons with regard to the processing of personal data and the exchange of such data", 27/04/2016, <https://gdpr-info.eu/> [29.07 .2024].
7. Law of Georgia "On Personal Data Protection", No. 3144-XIms-Xmp, 14/06/2023.
8. Law of Georgia "On Personal Data Protection", № 5669, 28/12/2011.
9. Law of Georgia "On the Protection of Consumer Rights", No. 1455-VIIIms-Xmp, 29/03/2022.
10. Law of Georgia "On the Protection of Consumer Rights", No. 151, 20/03/1996.
11. On consumer rights, amending Council Directive 93/13/EEC and European Parliament and Council Directive 1999/44/EC and repealing Council Directive 85/577/EEC and European Parliament and Council Directive 97/7/EC, <https:// matsne.gov.ge/ka/document/view/4488461?publication=0> [29.07.2024].
12. Order No. 45 of the Chairman of the National Competition Agency of Georgia "On approval of the case study procedure and procedure", 09/29/2022.
13. *Zuiderveen Borgesius F., Helberger N., Reyna A.,* Common Market Law Review, Volume 54, Issue 5, 2017.
14. <https://dcfta.gov.ge/ge/agreement> [29.07.2024].

Norbert Bernsdorff*

The New Data Protection Law in Georgia - A Brief Outline**

With the General Data Protection Regulation (GDPR), data protection law in the European Union (EU) was regulated in a largely uniform manner. The GDPR replaced the previously applicable Data Protection Directive 95/46/EC with a regulation that is directly applicable in all EU member states. In this way, it creates a uniform level of protection for the right of all EU citizens to the protection of their personal data.

In this context, there was and is an immediate need for action on the part of the Georgian legislator. Even if the GDPR automatically "grows into" Georgia's national legal order as a priority right when Georgia joins the EU, Georgian data protection law must be adapted to it. Upon Georgia's accession to the EU, all provisions of European data protection law are directly applicable. Because the GDPR enjoys priority of application over Georgian data protection law, after accession Georgian data protection law is only relevant for those matters that the GDPR does not regulate, but which it leaves to the EU member states to regulate with so-called opening clauses. It then has a mere supplementary function.

The Georgian legislature has responded to the need for action described above with the "Law on Personal Data Protection", which will come into force in large parts in 2024. It replaces the Law of Georgia on Personal Data Protection, which dates back to 2011/2012.

Who or what does the new law protect?

First and foremost, the new Data Protection Act protects personal data. According to its Article 3 letter a, personal data are particulars of the personal or material circumstances of a specific person which can be identified directly or indirectly on the basis of specific elements. In this sense, the Data Protection Act protects personal data that allow certain conclusions to be drawn about a person.

What is the content of the "Law on Personal Data Protection"?

The new Georgian data protection law deals with

- the legal bases for the processing of personal data (Article 4 and sequent);
- Rights of the persons concerned (Article 13 and sequent);
- the obligations of controllers and processors (Article 23 and sequent);
- Questions of liability and sanctions (Article 58 and sequent, Article 64, 65, Article 66 and sequent);
- the scope of the law, definitions and general principles for the processing of personal data (Article 2, Article 3 and sequent);
- Rules on data protection officers of public and non-public bodies (Article 33);
- the rules governing the Personal Data Protection Service, its status and functions (Articles 39 and sequent);

---

* Doctor of Law, Professor at the Philipps University of Marburg; Retired Judge of the German Federal Court of Social Affairs; Former Data Protection Commissioner of the Lower Saxony Judiciary. The Author is a Member of the Editorial Board of the "Journal of Personal Data Protection Law".

** The publication represent the text of the report presented by the author in October 2023 within the framework of public lectures held in the scope of cooperation of Ivane Javakhishvili Tbilisi State University Law Faculty and Institute of Administrative Sciences. The event was dedicated to the issues of Georgia's integration with the European Union.

- Remedies (such as judicial redress) (Article 63);
- the conditions for data transfers to third countries and international organisations (Articles 37, 38), etc.

The new Georgian "Law on the Protection of Personal Data" shows that the Georgian legislator has given intensive thought and carefully analysed the EU's sometimes complicated data protection law. For this, it deserves hearty congratulations! Overall, Georgia has already largely brought its national data protection law up to the standards of the GDPR through the new law.

It should be noted in addition

The rules in Article 33 of the new Georgian Data Protection Act on "data protection law compliance" by "data protection officers", so-called internal control, are very extensive and much more detailed than, for example, in German data protection law. The law could have exempted the courts from the obligation to appoint a data protection officer. However, this has already been done in the regulation on the scope of application of the Georgian Data Protection Act - Article 2 paragraph 2.

The Georgian "Law on the Protection of Personal Data" contains many regulations for data transfers to third countries and international organisations in Article 37 and sequent. If Georgia joins the EU, Article 45 of the GDPR will automatically apply to the country: The EU Commission must allow the transfer of data by means of an adequacy decision. However, a member state can challenge this decision in court. This is stated in the "Safe Harbour" decision of the Court of Justice of the EU from 2015 (C-362/14). Georgia could then regulate this in its data protection law.

PERSONAL DATA
PROTECTION SERVICE

Address: №7 Nato Vachnadze, Tbilisi, 0105
Batumi, Baku street №48, 6010
Web: www.personaldata.ge
Tel.: (+995 32) 242 1000
E-mail: office@pdps.ge