Norbert Bernsdorff*

The "State of Play" of Data Protection in Georgia – 2024 Communication on EU Enlargement Policy**

The article discusses the main findings of the EU Commission's recent staff-working document "Georgia 2024 Report", which assesses the country's progress since December 2023, when the European Council granted Georgia candidate status. The paper aims to contemplate the main findings and assessments concluded in the Report regarding Georgia's progress in aligning the data protection legal framework with the EU acquis. Furthermore, the paper suggests a legal analysis of the EU Commission's conclusions on Georgia's legal compliance with the Council of Europe's legal instruments on data protection. Lastly, a specific chapter is dedicated to discussing the Georgian data protection authority's effectiveness in ensuring the protection of personal data and its supervisory role.

Keywords: *Georgian Personal Data Protection Law, progress report, EU acquis, Personal Data Protection Service of Georgia, legal compliance*.

1. Starting Point: "Georgia 2024 Report"

In October 2024, the European Commission (EU Commission) presented its staff-working document "Georgia 2024 Report"[1] . The "Georgia 2024 Report" accompanies the EU Commission's "2024 Communication on EU enlargement policy" to the European Parliament, the Council, the European Economic and Social Committee, and

* 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 represents a statement submitted in the scope of cooperation with the Georgian Personal Data Protection Service. It is dedicated to the issues of Georgia`s integration with the European Union.

[1] Brussels, 30 October 2024, SWD (2024) 697 final.

the Committee of the Regions. The report covers the period from 15 June 2023 to 1 September 2024. In its "Main Findings" on page 7, the EU Commission takes the view that its recommendations from 2023 were not implemented and remain valid. For 2025, it recommends that Georgia "aligns the data protection legal framework with the EU acquis: Regulation (EU) 2016/679 and Directive (EU) 2016/680." Under the heading "Chapter 23: Judiciary and Fundamental Rights," on page 41 of its report, the EU Commission states that, despite the adoption of its new Law on the Protection of Personal Data, the protection of personal data in Georgia is not fully aligned with the relevant EU secondary legislation[2] and that Georgia has still not signed the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, as modernised[3] . The EU Commission certifies that the Personal Data Protection Service (PDPS) does a "generally satisfactory job of monitoring the lawfulness of data processing and activities carried out at the central database for electronic communication identification data"; however, the PDPS must play a more active role, particularly in monitoring covert investigations. The EU Commission refers to statistical data for 2022 and 2023 provided by the PDPS itself.

Under the heading "Chapter 10: Digital Transformation and Media," the EU Commission complains on page 73 of its report that Georgia has only partially aligned its national law in the field of digital services with Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on open data and the reuse of public-sector information[4] . It also makes the same accusation regarding other, more recent, secondary EU legislation.[5] In preparing its "Georgia 2024 Report," the EU Commission is using a "new method" developed for the conduct of accession negotiations in February 2020. This method involves grouping individual negotiation chapters into thematic clusters. In this context, compliance with the requirements of negotiation chapter 23, "Judiciary and Fundamental Rights," is being monitored particularly closely.

[2] 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 the Directive 95/46/EC ("General Data Protection Regulation"), OJ L 119, 4 May 2016, pp. 1 et seq.; 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, OJ L 119, 4 May 2016, pp. 89 et seq.

[3] Basic document: European Treaty Series – No. 108.

[4] OJ L 172, 26 June 2019, pp. 56 et seq.

[5] General Data Protection Regulation, OJ L 119, 4 May 2016, pp. 1 et seq.; Regulation (EU) of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC ("Digital Services Act"), OJ L 277, 27 October 2022, pp. 1 et seq.; Regulation (EU) of the European Parliament and of the Council of September 14, 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 ("Digital Markets Act"), OJ L 265, 12 October 2022, pp. 1 et seq.

2. The Dilemma of Blanket and Unfounded Legal Criticism

In its "Georgia 2024 Report," the EU Commission regularly fails to provide concrete evidence for its conclusions, including in its assessment of the "state of play" of data protection in Georgia. Instead, it provides the following general reference in footnote 2 on page 4:

"It (this report) is based on inputs from a variety of sources, including contributions from Georgia, EU Member States, European Parliament Reports and information from various international and non-governmental organisations. It also includes the results of comparative assessments and indices produced by other stakeholders, in particular in the area of the rule of law."

Of course, there are technical limitations to providing concrete evidence for a report on the state of play of reforms in more than 30 negotiation chapters or six clusters. Nevertheless, blanket and unfounded legal criticism without concrete examples or evidence is difficult to understand and leaves no room for improvement for the institutions being criticised.

One of the basic requirements of objective legal criticism is that it must clearly state the premises on which the criticism is based. It must be verifiably justified and include both positive and negative aspects. The basic function of legal criticism is the methodical identification of shortcomings, errors, and contradictions with the aim of improving practical procedures or conditions. Blanket and unfounded criticism of the law poses several problems. Above all, it can lead to a decline in cooperation because it is not constructive and does not offer any suggestions for improvement. It can also undermine trust in the criticising institution—in this case, the EU Commission—and create a negative atmosphere. Blanket criticism can "obscure" actual problems instead of solving them. Constructive criticism of the law can be recognised by the following characteristics: It cites specific evidence for the behavior being criticised and offers constructive suggestions for change. It is aimed at improving the situation. In terms of form, it must be expressed in a respectful and appreciative manner.

Unfortunately, the „Georgia 2024 Report“ on pages 41 and 73 does not meet the criteria for such a positive approach – including in terms of atmosphere – to Georgian data protection law and the PDPS, the institution that administers it, for the following reasons.

3. The Modernised Council of Europe Convention No. 108 for the Protection of Individuals with Regard to Automatic Processing of Personal Data

Convention No. 108 in its original version was opened for signature on 28 January 1981, and was the first legally binding international treaty to establish principles of

data protection. In 2001, it was supplemented by an additional protocol. A modernised version of Convention No. 108 has now been available for ratification for some time. This "Convention No. 108+" will enter into force when 38 member states of the Council of Europe have ratified it.

It is understandable that the EU Commission calls on Georgia in its report to sign (and subsequently ratify) the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data in its modernised version. With Georgia's ratification of Convention No. 108+, its entry into force is finally one-step closer.

However, the European Court of Human Rights (ECtHR) – with its rulings -has long since assumed the role of a central decision-making authority on data protection issues for the member states of the Council of Europe. It does use Convention No. 108 as an interpretative aid. However, since 1987, it has derived the right to protection of personal data independently and decisively from the human rights enshrined in the European Convention on Human Rights (ECHR), in particular from Article 8 ECHR ("Right to Respect for Private and Family Life, Home and Correspondence"). Because the ECtHR does not rule directly on the basis of Convention No. 108, but on the basis of the human rights of the ECHR, the legal significance of Convention No. 108 "takes a back seat." Furthermore, this international treaty still only lays down general principles for the protection of personal data, such as the need for a legal basis for processing, transparency of processing, the right to information and rectification, and the establishment of control mechanisms.

Since the *Leander versus Sweden* judgement of 1987[6], in which the ECtHR analysed, for the first time, the question of the storage by a public authority of an individual`s personal data, the case-law in this field has seen significant development. Over the years the Court has examined many situations in which questions related to this issue have been raised. A broad spectrum of operations involving personal data, such as the collection, storage, use and dissemination of such data, is now covered by a body of case-law of the ECtHR. This case-law has developed in line with the rapid evolution in information and communication technologies.

The right to the protection of personal data is not an autonomous right among the various ECHR rights and freedoms. The Court has nevertheless acknowledged that the protection of personal data is of fundamental importance to a person`s enjoyment of his or her right to respect for private and family life, home and correspondence, as guaranteed by Article 8 of the ECHR[7]. This Article is the main vector through which personal data is protected in the ECHR system, even though considerations related to this protection may also come into play under other provisions of the ECHR and its Protocols.

[6] ECtHR, Case of Leander v. Sweden, Application no. 9248/81, hudoc.

[7] ECtHR, Case of Z v. Finland, Application no. 22009/93, hudoc; Case of Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, Application no. 931/13, hudoc; Case of L.B. v. Hungary, Application no. 36345/16, hudoc.

As a result, Georgia is already unable to evade the legal standards established by the Council of Europe for data protection. Regardless of whether it signs (and subsequently ratifies) Convention No. 108+, Georgia is already bound by the established data protection case law of the ECtHR, meaning that "adoption" of Convention No. 108+ would, at most, be of a supplementary nature.

4. Alignment with the General Data Protection Regulation, the Digital Services Act, and the Digital Markets Act

In its "Georgia 2024 Report" on page 73, the EU Commission does not explain why it believes that the three legal texts mentioned, all of which are EU regulations ("Regulation," "Acts"), required Georgia to align its data protection law in advance of accession. From a legal perspective, EU directives are limited to prescribing a specific result to EU member states. They leave it up to the member states themselves to achieve this result; the member states must implement directives within certain time limits through their own national legislation. In contrast, EU regulations are directly and immediately binding on all EU member states and not, like a directive, only with regard to the result to be achieved. EU regulations do not, in principle, need to be transposed into national law.

The adoption of EU law upon accession to the EU – known as "adoption" or "transition" – is an automatic process.[8] The technical instrument for this is the "accession" of the candidate country. This takes place through the (international) accession agreement with all other EU member states. From the date of accession, the candidate country becomes a party to all EU treaties in their current version. All EU legislation adopted on the basis of these treaties up to the date of accession automatically becomes binding on the acceding state. It takes precedence over any national law. For EU data protection law, this means that it also automatically becomes part of the national legal system as primary law upon accession. It „grows“ into the national legal order.

Against this background, the EU Commission has failed to explain why, unlike existing EU Member States, the candidate country Georgia is required to "substitute" the content of the aforementioned EU regulations in its national data protection law prior to accession, i.e., to "anticipate" the EU regulations even before accession. If EU regulations also require the establishment of a minimum level of "enabling environment" in national law, corresponding clarifications and an outline of this "enabling environment" would have been desirable.

However, even if there were a need for the Digital Services Act to be "substituted" in Georgia's national data protection law, or at least to a greater extent, it would not be clear, without knowledge of the results of the TAIEX workshop in June

[8] See *Norbert Bernsdorff,* "Data Protection Law" of the European Union, Journal of Personal Data Protection Law, N2, 2023, pp. 13 et seq.

2024, where and in what respects further alignments would have had to be made by September 2024:

The EU's Digital Services Act creates a single set of rules for online services to promote a safe digital environment and protect consumers.[9] Key points include stronger obligations for online platforms such as social networks and marketplaces to moderate content and deal with user complaints. The Digital Services Act calls for greater transparency regarding moderation processes and advertising, contains measures against hate speech and disinformation, and strengthens the protection of minors. Stricter rules apply to very large platforms.

In view of the extensive provisions of the Law of Georgia on Personal Data Protection regarding its scope (Article 2), it is not clear why the Law does not also require online intermediaries such as online platforms, social networks, marketplaces, and app stores to take responsibility for illegal content. It also needs to be explained why the complaint mechanisms set out in Chapter III of the Law ("Rights of Data Subjects") are not sufficient to take legal action against decisions made by platform operators. Finally, the Law of Georgia on Personal Data Protection contains numerous provisions on the obligations of controllers and processors (Article 23 et seq.). Under the PDPS, a national supervisory authority monitors compliance with data protection law, including by digital service providers (Article 49 et seq.).

The Digital Markets Act is an EU regulation that aims to promote competition in digital markets by regulating large online platforms with a dominant market position, known as so-called gatekeepers. The aim is to create fair conditions and prevent the abuse of market power. The Digital Markets Act prohibits certain behaviors by so-called gatekeepers, such as favoring their own services or hindering data transfer, and instead prescribes greater interoperability and fair conditions.

It is not obvious, nor does the EU Commission explain, why the "Do‘s" and "Don'ts" imposed on so-called gatekeepers in the Digital Markets Act in the interest of fair competition cannot already be enforced using the conventional instruments of Georgian data protection law (Article 13 et seq., Article 18, Article 64, Chapter X). Restricting consumers' use of third-party digital services may also be prohibited under Georgian data protection law, and so-called gatekeepers may be required to uninstall certain computer applications or software in the event of a conflict.

As far as the General Data Protection Regulation is concerned, the provisions of the Law of Georgia on Personal Data Protection already come very close to its requirements.[10] The law incorporates many principles from the General Data Protection Regulation, including data subject rights, transparency, security obligations, and data breach notifications.

[9] For further information: *Bernsdorff N.,* E-Commerce and Data Protection – The Digital Services Act and its National Implementation, Journal of Personal Data Protection Law, N2, 2024, pp. 7 et seq.

[10] See *Bernsdorff N.,* The New Data Protection Law – A Brief Outline, Journal of Personal Data Protection Law, N1, 2024, pp. 101 et seq.

5. Effective Supervision by the Personal Data Protection Service

Data protection authorities generally have to answer questions from all areas of data protection across all industries and as part of so-called cross-sectional audits. Where they can place trust in the controllers and processors of personal data, less supervision is needed, while in other areas, focused audits must be carried out on a regular basis. There is always a great need for advice and education in this area. When auditing data protection compliance, not all questions are always equally relevant. There are no "off-the-shelf" data protection solutions; measures applied by data protection authorities must correspond to the specific data protection risk identified. An impact assessment must also be carried out before such measures are taken. Against this background, it is almost impossible to assess whether data protection authorities – and thus the Georgian PDPS – are actively managing data and pursuing an effective data protection concept.

It is certainly not convincing to use staggered "case numbers" after several years (2022, 2023) to measure activity (and take as a basis for future forecasts), as the EU Commission has done in the graphic attached to its "Georgia 2024 Report" on page 41. This graphic shows a linear increase in all areas. With regard to the PDPS „Special Report“ on the activities for the first six months of 2025[11] , the EU Commission's suggestion that the PDPS should play a "more active role" here does not seem justified. In the first half of 2025, the number of inspections/examinations was 155. According to its statistics, the PDPS had received 496 applications/notifications. The Service identified 278 administrative offenses and imposed administrative sanctions in 277 cases. 369 instructions and recommendations were issued. The international activities of the PDPS, which it reported on in another "Special Report"[12] , are also worth highlighting. In view of the numerous checks described in the "Special Report" on the activities of the PDPS for the first six months of 2025 in the field of monitoring covert investigative actions[13] , which the PDPS is obliged to carry out under Chapter VII of the Law of Georgia on Personal Data Protection, it is not clear why, in the opinion of the EU Commission, there is still a need for increased action in this area.

[11] Statistics of the Activities of the Personal Data Protection Service of Georgia for 6 Months of 2025/January-June.
[12] International Activities carried out by the Service in 2022-2024 to implement the Best European Practices and Standards of Personal Data Protection Law.
[13] Pages 8 to 11.

Bibliography:

1. Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108) European Treaty Series No 108 (1981).
2. 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.
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 the Directive 95/46/EC ("General Data Protection Regulation").
4. 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 (General Data Protection Regulation) [2016] OJ L119/1.
5. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act) [2022] OJ L265/1.
6. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.
7. *Bernsdorff N.,* "Data Protection Law" of the European Union, Journal of Personal Data Protection Law, N2, 2023, pp. 13 et seq.
8. *Bernsdorff N.,* E-Commerce and Data Protection – The Digital Services Act and its National Implementation, Journal of Personal Data Protection Law, N2, 2024, pp. 7 et seq.
9. *Bernsdorff N.,* the New Data Protection Law – A Brief Outline, Journal of Personal Data Protection Law, N1, 2024, pp. 101 et seq.
10. Case of L.B. v. Hungary, Application no. 36345/16, hudoc.
11. *European Commission***,** Staff Working Document SWD (2024) *697 final* (Brussels, 30 October 2024).
12. International Activities carried out by the Service in 2022-2024 to implement the Best European Practices and Standards of Personal Data Protection Law.
13. OJ L 172, 26 June 2019, pp. 56 et seq.
14. OJ L 119, 4 May 2016, pp. 1 et seq.
15. Statistics of the Activities of the Personal Data Protection Service of Georgia for 6 Months of 2025/January-June, Personal Data Protection Service of Georgia.

16. Case of Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland, Application no. 931/13, hudoc.
17. ECtHR, Case of Leander v. Sweden, Application no. 9248/81, hudoc.
18. ECtHR, Case of Z v. Finland, Application no. 22009/93, hudoc.