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.