Beka Meladze*

Data Processing in Cloud Systems - Challenges and Opportunities

We live in an era where information drives every decision. Accurate and rapid data analysis fuels industries, shapes societies, and accelerates progress. At the heart of this transformation are cloud systems — revolutionizing how governments, businesses, and individuals operate. While this technology unlocks immense opportunities and streamlines daily processes, it also presents significant challenges, particularly in the legal and ethical processing of personal data.

Keywords: *Personal data, cloud systems, controller, processor, international data transfer, data security.*

1. Introduction

Cloud computing has emerged as one of the fastest-growing technologies of the past decade, revolutionizing data processing by surpassing the limitations of traditional physical infrastructure. By offering scalability, flexibility, and efficiency, cloud computing enables organizations to manage the ever-increasing volume of data in today's digital landscape. In 2024 alone, global spending on cloud computing services exceeded $600 billion[1], with projections nearing $1 trillion by 2027. This rapid growth is driven by widespread adoption across industries, as businesses recognize the cost-effectiveness and strategic advantages of cloud-based solutions[2].

* Master of Law (LL.M.) at Ivane Javakhishvili Tbilisi State University; Lawyer at the Private Sector Oversight Department, Personal Data Protection Service of Georgia.

[1] Public cloud services end-user spending worldwide from 2017 to 2024, <https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/> [21.02.2025].

[2] NexQloud will revolutionize the cloud technology market with a decentralized platform, 2024, <https://forbes.ge/nexqloud-set-to-disrupt-cloud-computing-with-decentralized-platform/> [21.02.2025].

While cloud computing offers flexibility and speed, it also introduces significant challenges in processing personal data through third-party servers. Key concerns include defining the roles and responsibilities of entities involved, ensuring data security, and addressing jurisdictional complexities related to data processing locations, which may impose various legal and regulatory obligations.

This paper explores the role of cloud systems in personal data processing, examining their capabilities while analyzing the challenges associated with confidentiality and security.

2. The Essence of Cloud Systems

Cloud systems enable individuals to utilize the infrastructure of service providers via the Internet, allowing them to store, manage, and process data from anywhere in the world.

In simple terms, cloud technology allows users to upload data, files, multimedia content, or applications to a provider's servers and access or modify them at any time, from any device. Today, numerous companies worldwide offer cloud-based solutions for various purposes. The leading providers in this field include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP).

According to the US National Institute of Standards and Technology ("NIST"), cloud systems have 5 characteristics[3]:

- On-demand self-service - Users can access and manage services at any time (e.g., opening and modifying their database) without requiring approval or assistance from the infrastructure provider;
- Broad Network Access - Data can be accessed, edited, deleted, or added from multiple devices simultaneously, ensuring seamless connectivity;
- Resource pooling - Service providers dynamically allocate infrastructure resources among multiple users based on demand, optimizing efficiency;
- Rapid elasticity - Users can scale resources up or down as needed, such as adjusting storage capacity on platforms like Google Drive;

[3] National Institute of Standards and Technology (NIST) - Cloud Computing Synopsis and Recommendations, Special Publication, 2012, 80-146.

- Measured Service – Costs are based on actual resource consumption, ensuring a flexible and usage-based pricing model.

It is important to note that cloud systems encompass a wide range of services, categorized into several key models:

- Software as a Service (SaaS) – Provides users with cloud-based applications, such as email and document storage services (e.g., Google Drive, Dropbox, Gmail, Outlook 365), eliminating the need for local installations.
- Platform as a Service (PaaS) – Offers a cloud-based environment for developers to build, test, and deploy applications without managing the underlying infrastructure (e.g., Google App Engine).
- Infrastructure as a Service (IaaS) – Primarily used by enterprises, this model allows organizations to utilize cloud providers' computing resources (e.g., servers, storage, and networking) instead of maintaining their own physical infrastructure.

It is important to note that, in accordance with Article 2, Paragraph 1 of the Law of Georgia "On Personal Data Protection"[4] the legislation applies to the processing of personal data through automated and semi-automated means within the territory of Georgia. Consequently, if an individual or entity processes personal data within Georgia—including cases where they merely access a cloud system—the provisions of the Law of Georgia "On Personal Data Protection" remain applicable. This holds true regardless of the physical location of the cloud system, the service provider, or the jurisdiction to which they belong[5] (For further details on cloud system locations and relevant jurisdictional considerations, see Chapter 5.1 of this article).

Despite the wide range of cloud system applications, Software as a Service (SaaS) stands out in the context of personal data processing. This model is of particular interest, as it is frequently utilized by data controllers for the storage, sharing, and processing of personal data.

[4] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023.
[5] EDPS, Guidelines on the Use of Cloud Computing Services by the European Institutions and Bodies, 2018.

3. Legal Status of Subjects

Data processing through cloud systems is a highly complex topic involving multiple parties. In many cases, due to the imbalance of resources and the dominant position of certain entities, it can be challenging to determine which party is responsible for data processing and which is authorized to process it. In this context, it is crucial to assess, on one hand, the role and responsibilities of the cloud service provider, and on the other hand, the responsibilities of the user of its services.

According to Article 3, subsection “o” of the Law of Georgia “On Personal Data Protection” data controller is the “natural person, a legal person, or a public institution, who individually or in collaboration with others determines the purposes and means of the processing of data, and who directly or through a processor processes data”, according to subsection "j" of the same article, data processor is “a natural person, a legal person, or a public institution, which processes data for or on behalf of the controller. A natural person who is in labour relations with the controller shall not be considered a processor”.

When utilizing cloud systems, the user determines the purposes and means of data processing, making them the data controller responsible for the processing. In contrast, the cloud service provider does not have a personal interest in processing user data and acts solely on behalf of the data controller. As such, the provider functions as the data processor**,** authorized to process data only in accordance with the instructions of the data controller[6].

It is important to note that, typically, in the data processing relationship, the data controller sets the "rules of the game," and the data processor follows them. However, when using cloud systems, the dominant role and resources of the service provider often mean that the data controller must accept the terms and conditions set by the provider. For instance, when a user opts to use Google Cloud Platform, they cannot dictate the terms for such a large-scale company. Nevertheless, the user still determines the purposes and means of data processing, which remains the key factor in determining their legal status as the data controller[7].

[6] The Data Protection Commission of Ireland: Guidance for Organisations Engaging Cloud Service Providers, 2019.

[7] Information Commissioner's Office (ICO), Guidance on the Use of Cloud Computing, 18, <https://ico.org.uk/> [10.03.2025].

4. Processing of Personal Data in Cloud Systems

Due to the efficiency of data processing, cloud systems are widely adopted by both businesses and government agencies. Additionally, cloud systems enable users to reduce costs and enhance service delivery.

Data processing through cloud systems can be broken down into several key stages. First and foremost, it is important to note that the data controller has the discretion to decide how, in what format, and to what extent data is uploaded to the cloud system.

The most common form of data processing in cloud systems is data storage ("Data at Rest"), where it is crucial to consider the security measures outlined in Article 27 of the Law of Georgia “On Personal Data Protection”. These measures must be implemented by both the cloud service provider and the data controller to ensure compliance and safeguard personal data.

In addition to storage, cloud systems are also utilized for various other types of data processing ("Data in Use"), such as downloading, sharing, analytics, and training artificial intelligence, among others. In these cases, the data controller must be aware that using a cloud system does not absolve them of the obligations set forth in the Law of Georgia “On Personal Data Protection”. This includes the duty to comply with both technical and organizational security measures, as well as, most importantly, to process data in accordance with the relevant legal basis and principles.

5. Challenges and Opportunities

It has been widely acknowledged that cloud systems enable companies and governments to process data efficiently and with flexibility. However, they also introduce several complex issues related to the legality of personal data processing. Among the most critical challenges are those concerning data security and the location of the systems.

5.1. The Location of Cloud Systems and the Aspect of International Data Transfer

A key distinguishing feature of cloud systems is that users can access the service provider's infrastructure and process data from anywhere in the world via the Internet. As such, when a data controller utilizes cloud systems, data may be stored or processed outside Georgia, as most cloud service providers,

including Google, Amazon, and Microsoft, operate databases and infrastructure in various countries[8]. In these cases, it is crucial to consider Article 37 of the Law of Georgia “On Personal Data Protection”, which allows the transfer of data to another country or international organization if certain conditions are met. Specifically, the transfer is permissible if the relevant jurisdiction or international organization provides adequate safeguards for data protection and the rights of the data subject, in accordance with the requirements outlined in the law.[9]

It is also important to note that Order No. 23 of the President of the Personal Data Protection Service, dated February 29, 2024, titled "On Approval of the List of Countries with Adequate Guarantees for the Protection of Personal Data,"[10] is currently in effect. This Order outlines a list of countries where data transfers are permitted without the need for additional justification.

In accordance with this legal framework, the data controller must first thoroughly investigate the country or countries where the data is being stored before proceeding with any data processing or transfer[11].

After obtaining the relevant information, if it is determined that data transfer occurs outside Georgia to a country not listed in the adequate guarantees list, the data controller is required to apply to the Personal Data Protection Service for authorization to transfer the data internationally[12]. Alternatively, the data controller must obtain written consent from the data subjects for the transfer.[13]

Regarding the international transfer of data through cloud systems, the decision of the European Data Protection Supervisor (EDPS) on March 8, 2024[14], is particularly noteworthy. In this decision, it was determined that the European Commission used the Microsoft 365 program, processing data through a cloud system, with servers located in the United States. As a result, international data transfers occurred without an appropriate legal basis.

[8] European Data Protection Supervisor, Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", 2012, 16.
[9] Law of Georgia “On Personal Data Protection”, 3144-XIMs-XMP, 14/06/2023, article 37.
[10] Order No. 23 of the President of the Personal Data Protection Service, dated February 29, 2024 “On Approval of the List of Countries with Adequate Guarantees for the Protection of Personal Data”
[11] Information Commissioner's Office (ICO) - Guidance on the use of cloud computing, version: 1.1, 18.
[12] It is important to note that international data transfer, upon obtaining permission, is one of the permissible grounds. Alternatively, depending on the specifics of data processing, other grounds may apply as outlined in Article 37, Paragraph 2 of the Law of Georgia on Personal Data Protection.
[13] It is mandatory that the written consent complies with the requirements set forth in Article 32 and Article 37, Paragraph 2, Subparagraph "d" of the Law of Georgia on Personal Data Protection.
[14] EDPS Investigation into Use of Microsoft 365 by the European Commission, Decision №2021-0518, 08/03/2024.

5.2. Data Security

According to Article 4 of the Law of Georgia "On Personal Data Protection", security constitutes one of the fundamental principles of data processing. Also, according to Article 27, „A controller and a processor are obliged to take organisational and technical measures that are adequate for the possible and associated risks of data processing (including data pseudonymisation, registration of the access to data, information security mechanisms (confidentiality, integrity, accessibility), etc.), which will ensure the protection of the data against loss or unlawful processing, including destruction, deletion, alteration, disclosure or use".

Based on the aforementioned provision, ensuring data security is the responsibility of both the processor — the cloud system provider — and the controller — the system user.

Given the specifics of the system, the primary responsibility for ensuring technical security lies with the service provider, i.e., the processor. Specifically, the provider must first ensure that the system is designed in a manner that prevents users from accessing each other's data. Additionally, the system must implement encryption technology utilizing a "Public Key" and "Private Key" mechanism, ensuring that the provider itself cannot access either stored data ("Data at Rest") or data in transit ("Data in Use")[15].

In practice, Georgian legislation primarily applies to cloud service users, i.e., controllers, as the operations of leading cloud service providers fall outside Georgia's jurisdiction.

Accordingly, it is crucial to determine the security-related obligations of controllers when utilizing cloud systems. First and foremost, controllers must thoroughly investigate and assess the security mechanisms of various cloud systems before selecting a reliable and secure provider[16].

Additionally, the cloud system user must implement organizational security standards and grant access to relevant data only to individuals who have the necessary authorization, legitimate grounds, and a justified need[17]. Furthermore, appropriate measures must be taken to prevent, detect, and mitigate unlawful data processing by employees, including ensuring that employees are adequately informed about data security matters.[18]

[15] CNIL, Recommendations for Companies planning to Use Cloud Computing Services, 2012, 10.

[16] Information Commissioner's Office (ICO), Guidance on the Use of Cloud Computing, 13-14, <https://ico.org.uk/> [10.03.2025].

[17] EU Data Protection Code of Conduct for Cloud Service Providers, 2020, 17-20.

[18] Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023, Article 27 (6).

In accordance with Article 27(4) of the Law of Georgia "On Personal Data Protection", a controller is obliged to ensure that all operations performed in relation to electronic data (including information on incidents, data collection, data alteration, data access, data disclosure (transfer), data links and data deletion) are registered. In the vast majority of cases, cloud systems include a "logging" function; however, the controller is obligated to create multiple individual user accounts to ensure that, if necessary, it is possible to determine who specifically edited, deleted, added, or performed other actions on the data[19].

6. Conclusion

In conclusion, the increasing popularity of cloud systems is inevitable, as they represent one of the most advanced technologies for fast and flexible data processing, enabling companies, states, and individuals to reduce costs, enhance efficiency, and access data from anywhere in the world across various devices.

However, the capabilities of cloud systems are accompanied by significant challenges, particularly concerning the legal and ethical aspects of personal data processing.

To address these challenges, it is essential for both data controllers and authorized data processors to adhere to strict security measures. Specifically, the cloud service provider must implement robust data encryption technologies, while the user must ensure that access to data is granted only to authorized individuals and that all relevant organizational security standards are followed.

Furthermore, data controllers must determine the location of data storage and, if necessary, establish an appropriate legal basis for international data transfers.

Additionally, it is crucial to raise awareness of the intersection between cloud systems and data protection legislation, ensuring that data controllers fully understand both the advantages of cloud systems and the legal obligations they entail. Ultimately, personal data protection is not merely a technical legal requirement but a fundamental responsibility of any data processor.

[19] Information Commissioner's Office (ICO) - Guidance on the use of cloud computing, version: 1.1, 14 - 15.

Bibliography:

1. Law of Georgia "On Personal Data Protection", 3144-XIMs-XMP, 14/06/2023.
2. Order No. 23 of the President of the Personal Data Protection Service, dated February 29, 2024 “On Approval of the List of Countries with Adequate Guarantees for the Protection of Personal Data.
3. CNIL, Recommendations for Companies planning to Use Cloud Computing Services, 2012.
4. EDPS, Guidelines on the Use of Cloud Computing Services by the European Institutions and Bodies, 2018.
5. EDPS Investigation into Use of Microsoft 365 by the European Commission, Decision №2021-0518, 08/03/2024.
6. EU Data Protection Code of Conduct for Cloud Service Providers, 2020.
7. EDPS, Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the potential of Cloud Computing in Europe", 2012.
8. Information Commissioner's Office (ICO), Guidance on the Use of Cloud Computing, 18, <https://ico.org.uk/> [10.03.2025].
9. National Institute of Standards and Technology (NIST) - Cloud Computing Synopsis and Recommendations, Special Publication, 2012.
10. Public cloud services end-user spending worldwide from 2017 to 2024 <https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/> [21.02.2025].
11. The Data Protection Commission of Ireland: Guidance for Organisations Engaging Cloud Service Providers, 2019.