eISSN 2938-1487
https://doi.org/10.5565/rev/jhsgl.39

Data Retention in Labour Law

Retención de datos en el derecho laboral

Lela Janashvili
PhD. Professor of Tbilisi State University
President of the Georgian Personal Data Protection Service

Reception: 11/10/2023
Acceptance: 28/10/2023

Abstract

The age of information has a massive impact on society. New possibilities including search engines, sensor networks, security agencies, marketers and highly accessible databases require multiple and careful legal frameworks that will help to protect personal data on an advanced level. Its protection is a subject of comprehensive analysis that requires the assessment of multiple international or domestic legislation. Multiple perspectives regarding the protection of personal data in the employment context make the subject more important as it's crucial to make a proper assessment in order to determine the differences in between the visions of legislators as all of them are trying to do their best in order to protect the personal data but they still have many dissimilarities. This paper analyses the differences in European and Georgian Legislation and determines the main aspects of data retention in labour law. European treaties, directives and domestic law of Georgia might carry certain similarities and values but every aspect carries lots of important outcomes from the perspective of data protection that needs to be properly addressed.

Keywords: Personal Data Protection; Employment regulations; European Directives; General Data Protection Regulation; Georgian Legislation; Law of Georgia on Personal Data Protection of Georgia

Resumen

La era de la información tiene un impacto masivo en la sociedad. Nuevas posibilidades, incluyendo motores de búsqueda, redes de sensores, agencias de seguridad, profesionales del marketing y bases de datos altamente accesibles, requieren múltiples y cuidadosos marcos legales que ayuden a proteger los datos personales a un nivel avanzado. Su protección es un tema de análisis integral que requiere la evaluación de numerosas leyes internacionales o nacionales. Las diversas perspectivas sobre la pro-

tección de datos personales en el contexto laboral hacen que el tema sea aún más importante, ya que es crucial realizar una evaluación adecuada para determinar las diferencias entre las visiones de los legisladores, puesto que todos están haciendo un gran esfuerzo para proteger los datos personales, pero aún existen muchas discrepancias. Este artículo analiza las diferencias entre la legislación europea y la georgiana y determina los principales aspectos de la retención de datos en el derecho laboral. Los tratados, directivas y leyes nacionales europeas y de Georgia pueden tener ciertas similitudes y valores, pero cada aspecto conlleva muchas consecuencias importantes desde la perspectiva de la protección de datos que deben abordarse adecuadamente.

Palabras clave: protección de datos personales; regulaciones laborales; directivas europeas; Reglamento General de Protección de Datos; legislación georgiana; ley de Georgia sobre la protección de datos personales

1. Introduction

A variety of challenges that come with the process of digital transformation have brought into sharper focus the modern institutional role of data protection authorities in relation to the right to privacy and personal data protection. Although numerous scientific studies (Tikkinen-Piri and Rohunen, 2018; Fuster, 2014; European Union Agency for Fundamental Rights and Council of Europe, 2018; Safari, 2016) and regulations[1] have been published in recent years regarding the importance of personal data protection, this protection cannot be perceived separately from other legal institutions, as they are interconnected and work together to create a greater legal climate. It is also important to note that the legal frameworks of certain topics tend to change over time, under the influence of various key factors: culture, economics, politics, religion, etc. (Khubua, 2015). A different arrangement of a certain issue is often based on the relevant standard in a particular country, which in turn is formed according to the existing challenges.

It would therefore be reasonable to undertake comparative-legal research into employment relationship policies and their legal framework, as well as into data retention, based on the comprehensive analysis and assessment of European and Georgian legal systems.

1. Data Protection Act 2018, c. 12. Available at: <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted> (Accessed: 4 July 2023); Convention 108 +, Convention for the protection of individuals with regard to the processing of personal data. Available at: <https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2018/09-10/Convention_108_EN.pdf> (Accessed: 13 August 2023); Data Protection Act 2018, c. 12. Available at: https://www.legislation.gov.uk/ukpga/2018/12/introduction/enacted (Accessed: 5 July 2023); California Consumer Privacy Act of 2018. Available at: <https://oag.ca.gov/privacy/ccpa> (Accessed: 10 August 2023).

As Georgia is not a part of the European Union (EU), there are obviously multiple differences in legal provisions. Thus, it requires a discreet assessment to clarify different positive and negative tendencies.

Although the EU is an alliance, when regulating employment-related legal matters, it does not prescribe specific laws that must be followed by its members. Rather, it defines various directives that set the minimum standards for member states of the Union to meet in their national legislation.[2] When regulating a similar subject, as an independent state, Georgia issues a special organic law that must be taken into account and has a mandatory character. For instance, an organic law – the Labour Code of Georgia – governs labour relations in Georgia.[3]

In the EU, personal data protection is primarily governed by the General Data Protection Regulation (GDPR),[4] whereas in Georgia the Law of Georgia on Personal Data Protection is the main legally binding document regulating these matters.[5, 6]

Georgia is striving to obtain candidate country status to the European Union, and while there are lots of differences even between the laws of the member countries, Georgian legislation still carries many similarities to its European counterparts in terms of core values, especially when it comes to recognising and protecting human rights. These values are the main driving factor that helps and encourages a non-member country such as Georgia to precisely identify existing problems and find rationally correct legal solutions. This goal has more or less been achieved, and along with these values, there are currently a number of concrete similarities at the legislative level. An excellent example of

2. Treaty on European Union and the Treaty on the Functioning of the European Union. Articles (288; 289; 290; 291). Available at: <https://eur-lex.europa.eu/EN/legal-content/summary/the-european-union-s-secondary-law.html> (Accessed: 10 August: 2023).
3. Organic Law of Georgia. Available at: <https://matsne.gov.ge/en/document/view/1155567?publication=23> (Accessed: 11 August: 2023).
4. Data Protection Act 2018, c. 12. Available at: <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted> (Accessed: 4 July 2023). The Act makes provision for the processing of personal data and was enacted in 2018.
5. Law of Georgia on Personal Data Protection. Available at: <https://matsne.gov.ge/en/document/view/1561437?publication=23> (Accessed: 7 August: 2023). In Georgia, personal data protection is regulated by an overarching legislative act, the Law of Georgia on Personal Data Protection, which was enacted in 2011. The Law regulates the processing of personal data by public and private institutions and law enforcement bodies. In general, the Georgian model of personal data protection legislation is similar to the European one, where domestic and international regulations envisage the functioning of the law applicable to all sectors under the so-called "umbrella" legislation. Furthermore, Georgia is a party to the Council of Europe's "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data", and to an "Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows".
6. It is important to note that we find entries regarding the issue of personal protection in a number of regulatory acts of Georgia. For instance: The Code on the Rights of the Child; and the Law of Georgia On the Protection of Consumer Rights.

this is the recently adopted Law of Georgia on Protection of Personal Data,[7] which, almost equally, provides all the significant mechanisms for the protection of human rights defined by the General Data Protection Regulation. The phrase "almost equally" should not be considered to suggest a legislative weakness, as this is a comprehensive continuous process similar to the European Union's own legal drafting.[8]

Considering this change, it will be appropriate to assess the subject under discussion.[9]

2. Lawfulness of Data Processing in Labour Law

The General Data Protection Regulation applies to organisations that are established in the EU as well as organisations that operate outside the EU but offer goods or other services to, or monitor the behaviour of, individuals in the EU.[10] Article 6 of the GDPR identifies six grounds for lawful processing of personal data. If none of them apply to a particular processing activity, there will simply be no acceptable justification for a person to process the data of others (Gonzalez and de Hert, 2019).

It is clear that these requirements apply to the relationships that are formed within the scope of labour law,[11] during pre-contractual, contractual or even post-contractual relationships between employers and employees.

Data processing begins at the very first moment of communication between an employer and an employee who wishes to apply for a vacant position. Any kind of information that is mentioned by applicants about themselves in any application that is sent is considered to be their personal data.[12] Article 4(1) states that: "Any information relating to an

7. The new Law of Georgia was adopted on the third reading by the Parliament of Georgia on 14 June 2023. Available at: <https://parliament.ge/legislation/18184>. Law of Georgia on Personal Data protection. Available at: <https://matsne.gov.ge/ka/document/view/5827307?publication=0> (Accessed: 19 August: 2023).
8. "Working Party was aware of the need to conduct a deep analysis of the concept of personal data. Information about current practice in EU Member States suggests that there is some uncertainty and some diversity in practice among member states as to important aspects of this concept, which may affect the proper functioning of the existing data protection framework in different contexts." Opinion 4/2007 on the concept of personal data, Article 29, Data protection working party, 01248/07/EN WP 136. Available at: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf>.
9. New Law of Georgia on Personal Data Protection. Available at: <https://matsne.gov.ge/ka/document/view/5827307?publication=0> (Accessed: 19 August: 2023).
10. Data Protection Act 2018, c. 12. Available at: <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted> (Accessed: 4 July 2023). Article 2. Material scope.
11. In the case of Georgian legislation – The Labour Code of Georgia.
12. Data Protection Act 2018, c. 12. Available at: <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted> (Accessed: 4 July 2023). Article 4.(1). Definitions. New Law of Georgia on Personal Data Protection. Available at: <https://matsne.gov.ge/ka/document/view/5827307?publication=0> (Accessed: 19 August: 2023). Article 3.a. Definitions.

identified or identifiable natural person" should be considered to be personal information.[13] The commentary on the same Article 4(1) states that if data are not personal, their processing is not subject to data protection law (Kuner, Bygrave and Docksey, 2021). Both of these statements shall be taken into account simultaneously to correctly understand the scope of the law to be applied to the situation.

According to the General Data Protection Regulation, the six legal grounds for processing data are:

1. Consent of the data subject;[14]
2. The necessity for the performance of a contract;[15]
3. The necessity for compliance with a legal obligation of the controller;[16]
4. The necessity for protecting vital interests of the data subject or other persons;[17]
5. The necessity for performing a task carried out in the public interest or in the exercise of official authority;[18]
6. The necessity for the legitimate interest of the controller or other third party.[19]

These six legal grounds are not just requirements set by the General Data Protection Regulation, but they serve as a legal basis by enumerating six possible grounds for processing activities (Gonzalez and de Hert, 2019).

Similar legal grounds are also stipulated in the Law of Georgia on Personal Data Protection.[20] In addition to these requirements, it is important to pay attention to the data processing itself. From the perspective of the model of human activities, particular authors mention the importance of modelling the workflows as a sequence of steps that uses certain resources in input and produces corresponding outcomes. It is clarified that such workflows consist of two parts: (i) the plan to do something; (ii) the concrete sequence of actions that were actually performed (Palmirani et al., 2016).

13. Data Protection Act 2018, c. 12. Available at: <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted> (Accessed: 4 July 2023). Article 4.(1). Definitions.
14. Data Protection Act 2018, c. 12. article 6(1(a)).
15. Data Protection Act 2018, c. 12. Article 6(1(b)).
16. Data Protection Act 2018, c. 12. Article 6(1(c)).
17. Data Protection Act 2018, c. 12. Article 6(1(d)).
18. Data Protection Act 2018, c. 12. Article 6(1(e)).
19. Data Protection Act 2018, c. 12. Article 6(1)(f)).
20. Law of Georgia on Personal Data protection. Available at: <https://matsne.gov.ge/ka/document/view/5827307?publication=0> (Accessed: 19 August: 2023). Article 5.a. Grounds for data processing.

Such an approach helps to distinguish the plan from the actual execution, which helps to ensure a better approach from the perspective of the general principles of General Data Protection Regulation.

3. Key Principles of European Data Protection Law

The General Data Protection Regulation sets out the following principles governing the processing of personal data:

1. Lawfulness, fairness and transparency;
2. Purpose limitation;
3. Data minimisation;
4. Data accuracy;
5. Storage limitation;
6. Integrity and confidentiality.[21]

The first time similar principles were introduced for EU states was in 1995, in the Data Protection Directive, also known as DPD.[22]

These principles provide multiple positive outcomes that are worth noting. They help define important rights relating to data protection, including the individual's right to know and acknowledge how their data is being used. They also enable individuals to access their data and even request that any existing inaccuracies are corrected.[23]

They are also the main safeguard for the individual's right to privacy, as they establish a strong legal framework to ensure that personal data is handled in a respectful way. It is essential for organisations to abide by these principles as this greatly helps to build trust with customers, partners and organisations, because they have more possibilities to avoid legal issues, extra fines and reputational damage. It also has a huge positive impact on innovation since it encourages sharing and spreading ideas and starting new businesses, as they are aware of the strong legal mechanism that helps to protect their data during the development process. The existence of such principles is directly related

21. Data Protection Act 2018, c. 12. Available at: <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted> (Accessed: 4 July 2023). Article 4.(1). Principles relating to processing of personal data.
22. 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, *Official Journal of the European Communities*, No. L 281/31. Article 6. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046> (Accessed: 21 August: 2023).
23. This statement relates to the right to be forgotten. This is a very important and comprehensive model which has also been taken by courts at the national level – including in Germany. Fabbrini F. and Celeste E. (2020).

to building trust and confidence as they play a crucial role in the digital era. Civil relationships would not have evolved over time if they did not have reliable legislation to support this process.

The importance of such a requirement is not a novelty for the EU member states. The Data Protection Act 1998 implemented Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and also on the free movement of such data (Middleton and Smith, 2003). Section 4(4) of the 1998 Data Protection Act states similar principles that were mentioned earlier, including the security measures, which is also significantly important in employment relationships.

Labour law is not separated from other legal branches from the perspective of technological development, and the same principles that govern other fields are also relevant here. For example, it is essential to actively apply the same principles in the case of employment relationships. But time after time, it becomes more advanced as technological development isn't only used by citizens, but also by entities that have been authorised by public authorities and which are responsible for monitoring and recording communication. It is therefore important to systematically develop and improve different methods that have been used previously in order to achieve the goal (Zubik, Podkowik and Rybski, 2021). This topic has been a massive subject of review for decades, and generates concern for a similar reason – new information and communication technologies that establish new possibilities for data collection (Blanchette and Johnson, 2011).

Employers must determine the scope of processing of personal data in advance, and the processing must always have a legitimate purpose. According to the principles of personal data protection, after collecting the data, employers are obliged to ensure its security and confidentiality. It must be noted that employers often process sensitive types of information, such as special category data relating to criminal records, health conditions, race or ethnicity. Therefore, it is always important that they carry out all the necessary measures to make sure that the information obtained from such data processing remains secure and confidential. The protection of personal data is important in labour relations so as not to deter the legal balance between employees and employers. Personal data should not be collected from third parties unless there is an appropriate legal basis and, where required by the law, employees must be duly informed. The law establishes specific rules, principles, frameworks and security measures that must be observed when processing personal data. Collection, storage, use and distribution of data in violation of these rules constitutes a violation of the law and may become the basis for administrative liability. One of the basic prin-

ciples of data processing is proportionality and adequacy, which implies that data should be processed to the minimum extent necessary for achieving a specific legitimate purpose. The processed data must always be relevant for a specific purpose.[24] During every operation of processing, it is important to carefully determine the storage period for personal data. Personal data must be stored only for the period necessary for the purpose for which it was collected/processed.[25] Accordingly, employers must only store the information which is necessary within the context of the relevant labour relations.

4. Data Processing in Labour Relations

Article 8 of the Charter of Fundamental Rights of the European Union[26] not only establishes the right to the protection of personal data, but also defines the core values associated with it. According to the charter, the processing of personal data must be fair, carried out for specific purposes, with the consent of the person concerned or on legitimate grounds established by the law. "People should have access to and the ability to correct their personal data, and the right to personal data protection should be monitored by an independent body."[27]

The importance of personal data protection in labour relations is certainly high, so as not to deter the balance between the rights of employees and those of employers. Data protection governs the processing operations affecting the personal data of employees, as well as of candidates for employment starting from the very beginning of their pre-contractual relationships. Both the European and the Georgian legislations establish specific rules, principles, frameworks and security measures that must be observed when processing personal data. Collection, storage, use and distribution of data in contravention of these rules may constitute a violation of the law and become the basis for administrative liability.

> Data retention, or record retention, is exactly what it sounds like — the practice of storing and managing data and records for a designated period of time.

24. Law of Georgia on Personal Data Protection. Available at: <https://matsne.gov.ge/ka/document/view/5827307?publication=0> (Accessed: 19 August: 2023). Article 4.
25. Law of Georgia on Personal Data Protection. Available at: <https://matsne.gov.ge/ka/document/view/5827307?publication=0> (Accessed: 19 August: 2023). Article 4.
26. Convention for the protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg 28.1.1981. Available at: <https://rm.coe.int/1680078b37> (Accessed: August 1: 2023).
Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&rid=5> (Accessed: August 1: 2023).
27. Charter of Fundamental Rights of the European Union, Article 8.

> There are any number of reasons why a business might need to retain data: to maintain accurate financial records, to abide by local, state and federal laws, to comply with industry regulations, to ensure that information is easily accessible for eDiscovery and litigation purposes, and so on. To fulfill these and other business requirements, it is imperative that every organisation develop and implement data retention policies.[28]

Given the subordinate nature of the employee-employer relationship, the employee is economically dependent on the employer and is the so-called "weaker party". This relationship between the parties is reflected in personal data processing by employers. In particular, in some cases the employee agrees against their will to provide the employer with information about themselves that may not be relevant to the employment relationship between parties at all. And this is in direct proportion to the shortcomings of the employer's legitimate purpose in the course of data processing, and implies an abuse of their position. Protecting the confidentiality and security of personal data gained about an employee and processing the data only for lawful purposes in full compliance with the principle of proportionality and legal requirements represents the basic prerequisite for a bona fide employment relationship. Thus, all employers at any stage of the employment relationship must strike a fair balance between the employee's right to privacy and the legitimate interests of the employer in processing their data.[29]

Given the volume of personal data processed by the employer, there are usually several people involved in the data processing. They use the information obtained by the employer for the purposes of employment relationships within the scope of their duties. In addition, employers often process personal data through various electronic systems.[30] It should be noted that more than one person may have access to electronic systems. Consequently, if adequate organisational and technical measures are not taken to protect data confidentiality, there may be an increased risk of inadvertent or improper personal data processing.

Thus, the protection of personal data within the employment relationship is a particular priority for the Georgian data protection supervisory authority – the Personal Data Protection Service of Georgia.[31] This is why the Personal Data Protection Service has implemented a number of activities that have contributed to providing employees with

28. <https://www.intradyn.com/data-retention-policy/> (Data Retention Policy 101: Best Practices, Examples & More).
29. Case of Barbulescu v. Romania GC, [2017] ECHR App. No. 61496/08, §§ 116-123.
30. Article 29 Data Protection Working Party, WP 249 Opinion 2/2017 on Data Processing at Work, 2017.
31. For further information about the powers, values and missions of the Personal Data Protection Service of Georgia, see the official web-page: <https://personaldata.ge/en>.

information about the legal requirements for processing employees' personal data and to raising public awareness.

4.1. Types of Data

In the course of an employment relationship employers may collect various types of personal data for contractual, security, professional development or other legitimate purposes. Labour relations are regulated by specific legislation, which may sometimes oblige the applicants to provide certain requested documents containing their personal data. However, there may be cases where only the consent of the data subject is used as a basis for data processing.

Collecting personal data from employees may include obtaining any document or information sufficient for identifying a person, or which relates to them. For example, employers may collect a copy of an ID card, an autobiography, an email address, a phone number, a photograph, information about previous work experience, bank account details and various other types of information relating to their present or future employees.

Information is usually requested directly from the employees themselves, but it may also be obtained from third parties. There may be occasions when a person voluntarily provides the employer with their personal data, such as when adding extra information or documents to their CV.

4.2. Georgian Perspective

There may be certain labour relationships where collecting special categories of data is also deemed to be legitimate. The Law of Georgia on Personal Data Protection includes a list of special categories of data.[32] The content of this list is identical to Directive 95/46/EC of the European Parliament and Council.[33] According to Georgian law, special categories of data refer to information about a person's racial or ethnic origin, political opinions, religious or philosophical beliefs, membership of professional associations, health and sex life, information relating to a criminal conviction, administrative imprisonment, application of a pre-

32. Law of Georgia on Personal Data Protection, Article 2(b).
33. 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, Official Journal of the European Communities, No. L 281/31. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046>. (Accessed: 21 August: 2023).

ventive measure to a person, the conclusion of a settlement agreement with a person, diversion, and recognition as a victim of a crime, as well as biometric and genetic data that allows identification of an individual based on the listed characteristics. Before signing an employment contract, employers often require a potential employee to present a certificate of their criminal record and a health certificate, both of which contain special categories of data about the person. As for the European legislation, Article 9(1) of the General Data Protection Regulation defines special categories of personal data as personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation. The health-related data may be collected later during the employment period as well, for example when certain health conditions interfere with employees performing their obligations.

5. Storage of Personal Data by the Employer

Storage of personal data may serve the purpose of effective performance of legal and contractual obligations. It is important that information is collected in accordance with the principles of reasonableness, legality and legitimacy. In an employment relationship, the processing of personal data is carried out for the purposes of concluding contracts, providing services, paying compensation, fulfilling contractual obligations, reviewing reports, carrying out various contractual relationships, employment, and direct marketing, as well as fulfilling obligations determined by the legislation governing the company's operation.

During the period of employment, employers generally have the right to collect and process certain personal data of their employees for lawful purposes. This may include information such as contact information, salary information, etc. The specific retention period for the collected data may vary from country to country due to national legislation, but it is generally considered acceptable to retain such data for as long as necessary for the employment relationship. Following the termination of an employment relationship, there are often legal requirements regarding how long certain work-related data must be retained. For example, documents relating to financial matters may need to be retained for a certain number of years to comply with tax laws. As already mentioned, the duration may vary depending on the law.

Special categories of data, such as medical records or criminal records, should have stricter retention obligations. Employers may need to delete

or securely archive such data after a certain period of time, or when it is no longer needed. The retention period will depend on the purpose for which the data was collected and often also on whether the employee has consented to the processing and to what extent. If data is collected with the employee's consent for a specific purpose, it should not be retained beyond the purpose for which it is needed. The introduction of data protection regulations such as the General Data Protection Regulation in the European Union has had a significant impact on data protection in employment relationships. Under the General Data Protection Regulation, employers are required to process the personal data of employees lawfully, fairly and transparently, as well as to have a legal basis for processing. They must also adhere to the principles of data minimisation and purpose limitation, which means that data should be retained no longer than necessary for the purposes for which it was collected.[34] It is also important to note that employees have the right to demand correction or deletion of information and data stored about them.

5.1. Personal Data Protection in Employment Relationships – Analysis of Georgian Practice

Violations of the requirements of the Law of Georgia on Personal Data Protection have been identified in personal data processing within the scope of employment relationships, in both the public and the private sector. Given the variety of ways and forms of data processing that are possible, processing of employees' personal data by employers remains one of the key challenges. In most instances, the data processing violations relate to a conflict between the legitimate interests of employers and that of employees. Thus it is important to strike a fair balance between the right to privacy of employees and the legitimate interests of employers. The cases examined by the Personal Data Protection Service clarify that there have been certain irregularities and shortcomings in data processing in the area of employment relations. and in order to eradicate them, it is expedient to consider the following recommendations:

— Cases were identified in which employers obtained and disclosed data, including the special categories of data, to a greater extent than necessary to fulfil legitimate purposes. Data controllers must act on the principle of minimising the amount of data processed, and must maintain a fair balance between the legitimate purpose of data processing, the privacy of the data subject and

34. Data Protection Act 2018, c. 12. Available at: <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted> (Accessed: 4 July 2023).

the right to protection of personal data in the course of personal data processing. This means that the form of data processing chosen by the data controller must be adequate, necessary and effective to achieve the legitimate purpose of data processing. At the same time, the data must only be processed to the minimum extent possible that will enable the data controller to achieve the relevant legitimate purpose;

— Cases were revealed in which an employer processed the employee's personal email without a proper legal basis. Communicating with others is a guaranteed human right that allows the individual to determine the time, content and addressee of the communication, and to expect that this communication will be protected against interference from outsiders. Data processing during private communication is a gross intrusion into the privacy of the data subject. Thus, in each case, in order to process data in accordance with the requirements of the law, the data controller must clearly define the legal basis provided by the Law of Georgia on Personal Data Protection, and follow the principles enshrined in the same law with absolute precision. This will ensure a fair balance between the employee's right to privacy and the legitimate interests of the employer;
— The processing of biometric data (fingerprints) of employees without any legitimate purpose was found to have taken place during personal data processing within employment relationships. It is crucial to highlight that the law imposes high standards for the processing of biometric data, allowing such processing only when it is necessary to achieve the purpose(s) specified by the law. This necessity must arise when other means or methods are inadequate, or when a disproportionate effort would be required to achieve the same objective.
— An employer was found to have processed the special categories of data of current or former employees for a longer period of time than was necessary to achieve the purpose of data processing. When processing data, institutions are obliged to clearly establish the legal purpose and specific timeframe required to achieve the designated legal objective. Once the specified timeframe has elapsed and the objective has been attained, the data must be deleted in accordance with the legal requirements.
— In specific instances, video surveillance was found to have taken place in locker rooms and hygiene areas, and thus the processing of the personal data of employees by the institutions involved. Locker rooms and hygiene areas, depending on their function, should be considered to be particularly private spaces. Thus, monitoring the

data subject in such a space is unreasonable for any purpose. In addition, when introducing video surveillance in workplaces, it is essential for institutions to implement the surveillance only in exceptional cases, and after informing all employees in writing;

— In the course of personal data processing within the framework of employment relations, data controllers were found to have failed to take the appropriate organisational and technical measures for the prevention of unauthorised access to personal data. This failure exposes the risk of unlawful disclosure of personal data pertaining to job applicants, current employees and former employees. In order to ensure data security, data controllers must urgently take appropriate organisational and technical measures that will limit to a maximum the possibility of access to data;
— As part of the inspections and investigations of the Personal Data Protection Service of Georgia, it was singled out that in a number of cases the electronic systems through which the personal data of job applicants and current and former employees were processed did not record all the actions carried out on the data.[35]

6. Conclusion

Ensuring the lawfulness of personal data processing in labour relations is one of the most difficult tasks that employer organisations are faced with. For this reason, it is important that employers establish specific internal policies and regulations that promote good practice of data processing. Any person within the organisation who has access to the personal data of employees is obliged to protect its confidentiality. Effective internal control mechanisms must be created to detect violations of legislation on the protection of personal data (European Union Agency for Fundamental Rights and Council of Europe, 2018).

Even in the context of employment, an employee retains the right to privacy,[36] which places an obligation on the employer to undertake all requisite measures for safeguarding the employee's private life. In addition, in order to raise the standard of data processing in the employment relationship, it is important for the employer to effectively manage each instance of processing of an employee's data and protect the confidentiality and security of the information obtained, as well as ensuring a fair balance between the employer's legitimate interest and the employee's right to privacy.[37]

35. Personal Data Protection Service of Georgia, 2022. 2022 Activity Report of the Personal Data Protection Service of Georgia, 48-60.
36. Case of Antovic and Mirkovic v. Montenegro, [2017] ECHR App. No. 70838/13, §§ 40-43.
37. Case of Lopez Ribalda and others v. Spain GC, [2019] ECHR App. Nos. 1874/13, 8567/13, § 116.

It is worth noting that the processing of data in employment relations is governed by the general legislation of the European Union on the protection of personal data. It should also be noted that there is a regulation[38] that regulates the processing of personal data by European institutions specifically in the context of employment. The General Data Protection Regulation refers to employment relationships in Article 9(2), according to which the processing of personal data is permitted in the performance of the duties of a data processor or data subject or in the exercise of specific rights in the field of employment. In accordance with the General Data Protection Regulation, employees must be given an opportunity to clearly inspect the data which they voluntarily consent to be processed and/or stored, as well as the purposes for such storage. Before requesting consent, employers should inform employees about their rights and the retention period for the data. If a violation of the security of personal data of employees creates an increased risk for human rights and freedoms, employers are obliged to notify the employees whom it may concern. According to Article 88 of the Regulation, EU member states have the right to lay down specific rules to protect the rights and freedoms of individuals in the context of employment in relation to personal data.[39]

A good example is the Worten case,[40] which concerns the recording of daily earned time and rest periods, which are personal data. National legislation obliged the employer to disclose this information to government agencies that monitored working conditions. As a result, these agencies gained access to the relevant personal data of an employee.

However, on the other hand, access to the data was necessary for the relevant control and/or supervisory authority to monitor the legality of working conditions. The processing of personal data for employment purposes must be subject to certain principles and restrictions both in the public and private sectors. Adhering to these principles includes, for example, ensuring transparency and consultation with employees before installing workplace monitoring systems.[41]

38. Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data. Available at: <https://op.europa.eu/en/publication-detail/-/publication/0177e751-7cb7-404b-98d8-79a564ddc629/language-en> (Accessed: August 2: 2023).
39. Data Protection Act 2018, c. 12. Available at: <https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted> (Accessed: 4 July 2023). Article 89.
40. *Copland v. the United Kingdom,* No. 62617/00, 2007. *Worten – Equipamentos para o Lar SA v. Autoridade para as Condições de Trabalho (ACT).* Available at: <https://hudoc.echr.coe.int/app/conversion/docx/?library=ECHR&id=001-79996&filename=CASE%20OF%20COPLAND%20v.%20THE%20UNITED%20KINGDOM.docx&logEvent=False> (Accessed: 3 August: 2023).
41. European Commission, Recommendation CM/Rec(2015)5 of the Committee of Ministers to member states on the processing of personal data in the context of employment.

Bibliographical references

Blanchette, J. and Johnson, D. (2011). "Data Retention and Panoptic Society: The Social Benefits of Forgetfulness". *The Information Society: An International Journal*, 18, 7.

European Union Agency for Fundamental Rights and Council of Europe (2018). *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union. Available at: <https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition> (Accessed: August 1: 2023).

Fabbrini, F. and Celeste, E. (2020). "The Right to be Forgotten in the Digital Age: The Challenges of Data Protection Beyond Borders". *German Law Journal*, 21(1), 55-65.
<https://doi.org/10.1017/glj.2020.14>

Fuster, G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Brussels: Springer Science & Business.

Gonzalez, E. and de Hert, P. (2019). "Understanding the legal provisions that allow processing and profiling of personal data—an analysis of GDPR provisions and principles". *ERA Forum*, 19, 597-621.
<https://doi.org/10.1007/s12027-018-0546-z>

Greenleaf, G. (2018). "'Modernised' Data Protection Convention 108 and the GDPR". *UNSW Law Research Paper*, 19(3).

Khubua, G. (2015). *Theory of Law*. Tbilisi: Meridiani.

Kuner, C., Bygrave L. and Docksey C. (2021). *The EU General Data Protection Regulation: A Commentary. Update of Selected Articles*. In: Article 4(1): 22-27. Brussels and Oslo: Oxford University Press.

Middleton, R. and Smith, H. (2003). "Data retention policies – data protection considerations". *Computer Law & Security Report*, 19, 216.

Palmirani, M., Martoni, M., Rossi, A., Bartolini, C. and Robaldo, L. (2016). "PrOnto: Privacy Ontology for Legal Reasoning, conference paper". *International Conference on Electronic Government and the Informational Systems Perspective*, p. 6.

Safari, B. (2016). "Intangible privacy rights: How Europe's GDPR will set a new global standard for personal data protection". *Seton Hall L. Rev.*, 47, 809.

Tikkinen-Piri, C. and Rohunen, A. (2018). "EU General Data Protection Regulation: Changes and implications for personal data collecting companies". *Computer Law & Security Review*, 34(1), 134-153.

Zubik, M., Podkowik J. and Rybski R. (2021). "European Constitutional Courts towards Data Retention Laws". *Law Governance and Technology Series. Issues in Privacy and Data Protection*, 45, 28.