ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 2 (December)
http://doi.org/10.9770/jesi.2022.10.2(39)

Publisher
http://jssidoi.org/esc/home

EMPLOYEE DATA RETENTION PERIODS IN IMPLEMENTING THE RIGHT TO BE FORGOTTEN: THE SITUATION IN LITHUANIA

Andrejus Novikovas [1]*, Rasa Grigonienė [2]

[1,2] Mykolas Romeris University, Ateities str. 20, 08303, Vilnius, Lithuania

E-mails: [1] andrejus@mruni.eu *(Corresponding author); [2]* rasa.grigoniene@gmail.com

Received 11 October 2022, accepted 21 December 2022, 30 December 2022

Abstract. The General Data Protection Regulation (Regulation, 2016) (hereinafter – the GDPR, Regulation) establishes the basic principles of personal data protection and the data subject's rights. The right to be forgotten is established in Article 17 of the GDPR. It allows the data subject, under certain conditions, to obtain from the controller the erasure of personal data concerning him or her upon the termination of the employment relationship. The study was conducted mainly in the context of labour law, i.e. the actions of the employer (as the data controller) and the employee (as the data subject) in processing (protecting) personal data and implementing the right to be forgotten are analysed. However, the public sector was assessed and compared for a more objective and detailed disclosure of the situation in the subject's data retention activities. In the relationship between employers and employees, there are discussions about how long the employer must store the employee's personal data, as well as disputes regarding the period after which the data subject acquires the right to obtain from the controller the erasure of personal data concerning him or her. The GDPR does not provide personal data retention periods – these periods are established in the national legislation of the European Union (EU) Member States. It should be noted that after the provisions of the GDPR came into force, the national legislation regulating personal data retention periods were not changed. This leads to possible non-compliance with the provisions of the GDPR stipulating that the periods for which personal data are stored must be optimal and not too long and must not violate the interests of the data subject. During the study, by analysing case law as well as legal regulation in the Republic of Lithuania and other EU countries, the content of the right to be forgotten is revealed, and optimal personal data retention periods that allow a sustainable relationship between the data subject and the data controller to be maintained are proposed.

Keywords: rights of data subjects; right to be forgotten; employee data retention periods; obligations of employers

Reference to this paper should be made as follows: Novikovas, A., Grigonienė, R. 2022. Employee data retention periods in implementing the right to be forgotten: the situation in Lithuania. *Entrepreneurship and Sustainability Issues*, 10(2), 623-634. http://doi.org/10.9770/jesi.2022.10.2(39)

JEL Classifications: J53, J58

Additional disciplines: law

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 2 (December)
http://doi.org/10.9770/jesi.2022.10.2(39)

1. Introduction

Document retention periods and compliance with them affect the sustainability of employment relations and assurance of employees' rights and legitimate interests. Compliance with the retention periods for employee documents is inextricably linked to the implementation of the right to be forgotten, as whether or not the person acquires the right to exercise it depends on the period for which the data will be stored. If the right to be forgotten is infringed, so is not only the GDPR, but also the rights enshrined in Article 8 of the European Convention on Human Rights (Convention, 1950) (hereinafter - ECHR) and Article 8 of the Charter of Fundamental Rights of the European Union (Charter, 2016) (hereinafter - Charter). On the other hand, data about employees must be stored to ensure the rights and legitimate interests (guarantees) of the very employees, e.g. proving their length of employment, entitlement to a longer holiday, disability guarantees and guarantees for raising children, or occupational health-related and subsequent benefits. Employee data are thus a unique group of data, the preservation of which requires a precise legal regulation that justifies the need for specific data while assessing the risks that may arise from their loss. However, the still widespread practice among employers in Lithuania of keeping everything about employees almost forever by creating personal files for them should not be continued. The main problem raised in this study is the excessive accumulation of personal data in workplaces, primarily out of fear and not knowing what specific personal data must or may be retained about the employee and for how long. The objective of the study is to analyse court practice and legal regulation in the Republic of Lithuania and other EU countries to reveal the content of the right to be forgotten and propose optimal personal data retention periods that allow a sustainable relationship between the data subject and the data controller to be maintained. Several tasks have been formed to achieve this objective: reveal the concept and content of the right to be forgotten; investigate the circumstances when the employer (the data controller) must store the personal data of the employee (data subject), and the employee cannot demand the erasure of personal data concerning him or her; analyse the practical specifics of realising the data subject's right to be forgotten, and propose optimal personal data retention periods. During the study, the document analysis method was used to analyse legislation, court practice and scientific sources revealing the content of the right to be forgotten and the specifics of its implementation. Based on the comparison method, the (procedural) document retention periods established in various pieces of legislation were compared. Using the generalisation method, the authors made substantiated and reasoned conclusions and generalisations. The article was written with references to other work on the topic by (Erdos, 2021), (Moore, 2017) (Petraitytė, 2013), (Grigonienė2020) and other sources.

2. The essence and content of the right to be forgotten

The right to be forgotten was formulated and developed by the Court of Justice of the European Union in the 2014 case of *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD)* (Case No. C 131/12, 2014). In this case, the court found that the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (Charter, 2016), request that the information in question no longer be made available to the general public by its inclusion in such a list of results. These rights override, as a rule, not only the economic interest of the operator of the search engine but also the general public's interest in finding that information upon a search relating to the data subject's name. It should be noted that the right to be forgotten is not absolute – it can only be exercised when the information is excessive, irrelevant, inadequate or inaccurate. The public interest and the public's right to receive information have a higher priority in some instances than the individual's right to respect one's private and family life under Article 8 of the ECHR or under the regulation.

As Erdos D. notes, the “right to be forgotten” is clearly imperative. There is an understanding that data protection can and should enable individuals, especially in the context of online dissemination, to restrict access or otherwise exercise at least *ex post* control over personal data (to prevent actual or potential harm), provided that there are no

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 2 (December)
http://doi.org/10.9770/jesi.2022.10.2(39)

legitimate and overriding reasons to oppose such restriction or control (Erdos, 2021). The CJEU has stressed that "the right to the protection of personal data is not an absolute right, but must be considered in relation to its function in society and be balanced against other fundamental rights, following the principle of proportionality."(Case No 3C-507/17, 2019). That the right to the protection of personal data is not absolute is also emphasised in Recital 4 of the GDPR, which states: "The processing of personal data should be designed to serve humanity. The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality."(Regulation, 2016).

To ascertain the essence of the employee's right to be forgotten in the context of the right to the protection of personal data, the reasons for the implementation of the data subject's right to be forgotten and the content of the information that employees could demand the deletion of must be analysed. The right to obtain the erasure of personal data only arises where one of the grounds listed in Article 17(1) of the GDPR applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing. It should be noted that in employment relationships, consent is a relatively rare legal basis for processing personal data, because only in rare cases can such consent be considered freely given (due to the power imbalance between the employee and the employer). This is therefore an extremely rare reason to obtain the erasure of personal data;

(c) the data subject objects to the processing pursuant to Article 21(1), and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

According to the Information Commissioner's Office (ICO), individuals have the right to have their personal data erased if:

- the personal data is no longer necessary for the purpose which you originally collected or processed it for;
- you are relying on consent as your lawful basis for holding the data, and the individual withdraws their consent;
- you are relying on legitimate interests as your basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- you are processing the personal data for direct marketing purposes, and the individual objects to that processing;
- you have processed the personal data unlawfully (i.e. in breach of the lawfulness requirement of the 1st principle);
- you have to do it to comply with a legal obligation; or
- you have processed the personal data to offer information society services to a child (ICO, 2022)

Depending on the grounds given, a person can acquire the "right to be forgotten" and the information used in real-time. For example, data subjects have the right to withdraw their consent at any time, either if they believe that the data controller no longer needs their personal data, or when it becomes clear that the personal data has been processed unlawfully, and so on. In this context, the right to be forgotten can be considered as an element of informational self-determination, since the right to be forgotten is not conditioned by the criterion of the elapsing of time (de Terwangne, 2013). In the context of personal data protection, the right to be forgotten is not only the duty of the data controller to constantly assess the expediency of the processing of personal data (in terms of scope, purpose and time) – it is also the ability of the data subjects to control how and where their personal data is

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 2 (December)
http://doi.org/10.9770/jesi.2022.10.2(39)

processed. One of the purposes of this right is to protect the individual against potentially negative consequences that may arise when certain information is too readily available.

Suzanne Moore, a columnist for *The Guardian*, called the right to be forgotten "the right to have an imperfect past" (Moore, 2017). An imperfect past in an employment relationship could be associated with violations of job duties (or what was previously called "employee discipline"), the employee's negative or satisfactory work performance evaluations, or other data (telephone call recordings, video material, electronic correspondence, etc.) that could allow inappropriate (imperfect) employee conduct to be established. And even if such data were collected legally and transparently (after properly informing the employee), it is worth coming back to justify the necessity and proportionality of such data and the retention periods set by the state or the data controller.

As stated in Recital 39 of the GDPR, personal data should be processed only when the purpose of the processing of personal data cannot reasonably be achieved by other means. To ensure that personal data are kept only as long as necessary, the controller should establish time limits for the erasure or periodic review of the data. The cases provided for in the regulation when the right to be forgotten cannot be exercised are:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims (Regulation, 2016)

Even considering the reasonable interest of the public or law enforcement authorities to know, in the 2020 case *Gaughran v. the United Kingdom* (Case No. 45245/15, 2022) the European Court of Human Rights established a violation of Article 8 of the ECHR due to the procedure in force in Northern Ireland, where the private data (DNA profile, fingerprints, photographs) of previously convicted persons were stored indefinitely in the databases of law enforcement authorities. So according to the GDPR, even criminals have the right to be forgotten, thus begging the question: Is the employee's right to be forgotten really properly implemented in Lithuanian legislation?

3. Employee data retention periods

As previously mentioned, the right to be forgotten is not absolute. Article 17(3) of the GDPR provides exceptions where, rather than being obliged to delete personal data without undue delay, the data controller must store the data for a certain period. One of the conditions obliging the data controller not to delete data is for compliance with a legal obligation which requires processing by Member State law to which the controller is subject (Article 17(3)(b) of the GDPR). The general obligation to store documents arises from the Civil Code of the Republic of Lithuania (Official Gazette, No 74-2262, 2000)[*]. Laws and other legislation also set specific document retention periods. According to the provisions of the Republic of Lithuania Law on Documents and Archives (Official Gazette, No 57-1982, 2004),"retention period" means the length of time that documents must be retained (Article 2(20)); state and municipal institutions, agencies and enterprises, persons authorised by the state, non-governmental organisations, and private legal persons must retain their activity documents for the period necessary to ensure evidence of the activities and protect the rights of natural and legal persons related to the said

[*] For example, Article 2.4(3) of the Civil Code of the Republic of Lithuania stipulates that “all persons engaged in business or professional activities must manage their property and everything else related to their business or professional activities, and store documents and other information about their property, business or professional activities, in such a way that every person who has a legal interest can at any time receive comprehensive information about the property rights and obligations of the person in question.”

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 2 (December)
http://doi.org/10.9770/jesi.2022.10.2(39)

activities, and must also retain for the required period the activity documents of other natural and legal persons that were taken over in accordance with the procedure established by this law and other regulations (Article 12(1)(2) and (3)); and it is the head of the state or municipal institution, agency or enterprise, non-governmental organisation, or private legal person who is responsible for retaining the activity documents for the period necessary (Article 12(2)). Accordingly, the Code of Administrative Offences (Official Gazette, 2015-11216, 2015) provides for liability for document management violations. For example, Article 522(1) of the Code of Administrative Offences foresees liability for infringement or non-execution of the regulatory acts governing the management and/or use of documents from the National Document Fund. In contrast, Article 505(1) foresees liability for obstructing officials authorised by law to exercise their rights or to perform their duties and for not complying with their lawful requirements or instructions or the decisions of collegial institutions or public officials. Consequently, the head of the agency is responsible for retaining the agency's documents for the required period.

The 15 December 2021 ruling of the Supreme Administrative Court of Lithuania stated that the data controller must not only store documents for a certain period of time, but also set clear document retention periods. The data controller must distinctly define the period for which the personal data will be stored, and legal regulation or assessment of the need of the circumstances cannot be considered sufficient and transparent criteria that can help define the duration of the retention period for personal data that is available for the purposes of processing. The court agrees with the court's assessment of the first instance that the period for which the personal data will be stored is not clearly defined in the response (Case No eA-2108-822/2021, 2021). It should be emphasised that the data subject (employee) must be informed about the data retention period (Guidelines, 2017).

From the above information, it follows that a person's right to obtain the erasure of personal data – or right to be forgotten – is directly related to the principle of limiting the duration of the retention period for personal data. The personal data of current or former employees must be kept and stored for a certain period of time. In view of this, the employer is obliged to ensure the storage of personal data for a certain period of time, and to assume all of the risks related to storage, and the employee/former employee cannot demand the erasure/deletion of personal data concerning him or her. The principle of limiting the period for which the personal data are stored is related to two important criteria: the purpose of storage (the question must be raised as to whether storing the data is necessary at all and why) and the duration of storage (there must be a clear justification as to why specific data need to be stored for the set period of time).[†] According to Petraitytė, I. storage is one of the actions of processing personal data, so if personal data is stored, it cannot be said that these data are no longer being processed (Petraitytė, 2013). The GDPR establishes that personal data must be "kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed." The regulation's preamble also talks about the need to carefully assess the goals and periods of data retention, and to set the shortest ones possible: The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum." (Regulation, 2016).

During this study, the aim was to analyse the main pieces of legislation regulating the duration of the retention period for the personal data of employees in Lithuania. The Index of General Document Retention Periods (Official Gazette, No. 32-1534, 2011) (hereinafter - Index) approved by order of the Chief Archivist of Lithuania establishes the general main retention periods for the personal data of employees, while the retention periods for the personal data of individual categories of employees or specific personal data are established by the legislation of individual ministries or other institutions. Under Law on Documents and Archives of the Republic of Lithuania (Official Gazette, No 57-1982, 2004), if the data retention periods are not officially established, the obligation to

[†] In this case, a distinction should be made between the purpose of collecting personal data and the purpose of storing such data. Even with the legitimate purpose of collecting personal data, storing personal data is only sometimes justified.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 2 (December)
http://doi.org/10.9770/jesi.2022.10.2(39)

establish the data retention period rests with the head of the institution or company: "State and municipal institutions, agencies and enterprises, non-governmental organisations and private legal persons shall establish the retention periods for activity documents in compliance with the requirements of laws and other regulatory acts. If these requirements are not set out, the document retention period is to be established taking into account the obligations and legitimate interests of the state and municipal institutions, agencies and enterprises, non-governmental organisations, private legal persons and other persons concerned." It should be noted that the personal data retention periods set out in the Index were not changed after the regulation entered into force. They are mandatory for documents of state and municipal institutions, agencies and enterprises and persons authorised by the state, which are drawn up during internal administration and other general functions. Furthermore, the minimum retention periods established in the Index also apply to the activity documents of non-governmental organisations and private legal entities that are prepared in accordance with regulatory acts.

The justification for the purpose and duration of storage of the listed personal data is not separately stated in the legislation. In other words, legislation only provides for a data retention period without discussing other circumstances (purpose, categories of personal data, etc.), so it is more difficult to assess which period applies to a specific document or personal data processing operation. The more abstract the provision, the greater the responsibility of the data controller is to justify the personal data retention period chosen. It is logical to assume that these periods must be associated with periods already established in legislation, such as limitation periods, procedural terms, or other juridical facts and circumstances. However, the links could be more apparent, more understandable and more pronounced, as required by the principle of transparency enshrined in the regulation. According to the Labour Code of the Republic of Lithuania (Official Gazette, No. 2016-23709, 2016) the general limitation period is three years, while according to the Civil Code of the Republic of Lithuania (Official Gazette, No 74-2262, 2000) it is 10 years, so in the opinion of the authors, the key personal data retention periods should also be linked to these terms. Since the basis and subject of labour disputes are often relationships, objects and values regulated by civil law, priority should reasonably be given to the regulation provided for in the Civil Code. According to Grigonienė, R., the 50-year retention period established for employment contracts (which begins to be calculated after the contract expires) was previously associated with human lifespan, and the employer's obligation to store the specified documents was based on important purposes such as calculating the person's length of employment and pension. Currently, the electronic notifications about employment relations in the Sodra database eliminate the validity of the previously set purposes (Grigonienė, 2020). The same can be said about the retention periods for personal payroll records at the workplace. Storing this kind of personal data for 50 years increases the risk of unauthorised disclosure of personal data. It creates a substantial bureaucratic burden for employers who must retain these documents for the specified period.

Another group of personal data – employee job duty violation and misconduct investigation documents – also requires clearer substantiation of the storage duration and purpose. These documents must be stored for five years (Official Gazette, No. 32-1534, 2011). The choice of this data retention period takes on special importance, since the employee's statement on the alleged violation of job duties (as well as the accompanying supporting documents and the decision of the data controller) may mention information concerning the employee's health, family circumstances, children and so on, so their storage may pose additional risks. The Labour Code stipulates that an employment contract may be terminated due to either a gross violation of the employee's job duties or a second instance of the employee committing the same job duty violation over the past 12 months (Official Gazette No. 2016-23709, 2016). In this case, it would be sufficient to store these documents for 12 months to prove the repetition of the violation and the legal grounds for dismissal. Taking into account the limitation period for labour disputes, the storage period for these documents could be extended to three years. However, longer periods (like personal files – 10 years) raise reasonable doubts about the necessity, proportionality and assurance of adequate protection of employees' personal data in general. Specific data retention periods not provided for in legislation prevent data controllers from even considering the assumptions of the need for such data. According to Petraitytė, I. the fact that the permitted duration of the processing of personal data must correspond to the purposes of

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 2 (December)
http://doi.org/10.9770/jesi.2022.10.2(39)

processing means that only the data controller can determine the optimal period for the processing of personal data that is compatible with the adequacy aspect of the principle under consideration (Petraitytė, 2013). The narrowing of this right, and at the same time, the duty of the data controller by establishing the period of personal data processing in legislation, can only be justified in exceptional cases, taking into account the specifics of the personal data and the possible impact on the person, and after assessing the threat that the data controllers will not act fairly and diligently in establishing the period of personal data processing. The period of personal data processing established in legislation must unconditionally comply with the principle of data minimisation.

In the above-mentioned Index, a 50-year retention period is established for internal legislation regarding the employee's hiring, dismissal and so on generally referred to as "personnel orders". As a rule, the manager writes an order to give an employee (civil servant) a penalty. The Labour Code was amended as of 1 July 2017, and now penalties have been cancelled for employees (except civil servants), but job duty violations are also recorded by order. The question arises as to whether, in cases like these, an employee can exercise the right to be forgotten in one, three, five or ten years if legislation requires them to be retained for 50 years. From a legal point of view, the employer cannot question the periods specified in legislation. Legislators should decide the question of time periods. Given that in some instances, the duration of personal data retention could be linked to the general limitation period, it can be assumed that a retention period of 10 years would be enough for internal legislation regarding the employee's hiring, dismissal and so on.

Depending on their type, the purpose of processing and other circumstances, the retention periods for some personal data should be less than 10 years. The State Data Protection Inspectorate (hereinafter - SDPI) has repeatedly spoken about the proportionality of the personal data retention period after performing inspections of data controllers. According to the SDPI, the data retention period must be specific and substantiated. It must be determined by assessing the need to process the personal data taking into account the purposes of data processing (Article 5(1)(e) of the GDPR) (Summary, 2018). After carrying out inspections, the SDPI established that some companies either do not have specific personal data retention periods, or have unreasonably long personal data retention periods, specifying that personal data will be stored “as long as you have a valid customer card and 10 years after its last use” or “ for 10 years after the end of participation in the loyalty programme”, and that “the data will be deleted once and for all five years after the transfer to the archive” or will be “stored for the duration of the Company’s activities” and so on. These companies were given instructions to eliminate the violations identified by the SDPI.

Another "potentially forgotten" group of employee personal data is performance evaluation documents, which are stored for 10 years, even if the information is not relevant to anyone after one year and does not create legal effects. The authors believe that the optimal retention period for such documents would be three years.

The question of the validity of the retention period's duration for employees' personal data also arises when analysing employee leave data. Until the Labour Code in force until 2017, annual leave was accumulated, and the employee had the opportunity to use it for the entire working period, even if it was for 10 years. Article 127(5) of the current version of the Labour Code establishes that "the right to take one's entire annual leave or part thereof (or to receive monetary compensation therefor in the case established by this Code) shall be lost three years after the end of the calendar year during which the right to full annual leave was acquired, except for cases when the employee was, in actuality, unable to take it." This means that data on accrued leave days are not relevant after three years, except in rare, isolated cases, like if the labour inspectorate conducts an investigation into the granting of leave after a period of more than three years. The practice of not accumulating leave days is rapidly forming, where employers are obliged, and it is in the interest of employees to use annual leave during the same year. However, item 7.12 of the Index obliges employers to store leave data for 10 years. It is proposed that a three-year retention period be set for documents concerning annual, unpaid, educational and other leave, and a 10-year retention period can only be provided for if the employee has unused leave for more than three years. This

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 2 (December)
http://doi.org/10.9770/jesi.2022.10.2(39)

proposal also correlates with the latest practice of the Court of Justice of the European Union, in which it is interpreted that the employee's right to paid annual leave that is time-barred and conditional under national legislation cannot, in certain cases, be lost upon expiry of the three-year time limit for exercising this right – for a specific period of work (Case C-120/21, 2022). In the Index, personal account cards are also meant to be stored for a long time – 50 years. Currently, when all financial documents are submitted to state institutions electronically into databases, and wages are paid directly to the employees' bank accounts, obliging the employer to additionally store employee account cards or payroll records for 50 years is an excessive requirement. All the more so when the Index of General Document Retention Periods does not regulate the storage of personal data in special state databases but provides storage requirements for agencies and enterprises. Suppose the longer storage of such data at the state level can be legally justified. In that case, this regulation imposes too much of an administrative burden on the employer and does not ensure the employee's right to be forgotten. In summary, information about changing the retention periods for individual documents could be presented in Table 1 below.

Table 1. Retention periods

Numbering in the Index	Document	Periods provided for in the Index	Proposed periods
7.1.1.	Regarding hiring, transfer, substitution, dismissal, salary, child care leave, paternity leave;	50	10 years. This period is linked to the general limitation period provided for in the Civil Code of 10 years (after the contract expires).
7.3.	Employment contracts and appendices (agreements on supplementary employment contract terms and so on)	50 (after the contract expires)	This period is linked to the general limitation period provided for in the Civil Code of 10 years. A more extended period entails a high risk of data disclosure and is a vast bureaucratic burden for employers and archives.
10.20.1.	Personal account cards	50	It is suggested not to save as it is an redundant requirement
7.2.	Personal file documents (documents related to the beginning, course and end of service/work at the workplace or copies thereof)	10 (after the termination of the service/employment relationship)	12 months to 3 years (after the termination of the service/employment relationship). More extended periods raise reasonable doubts about the necessity, proportionality and assurance of adequate protection of employees' personal data.
7.14.	Employee job duty violation and misconduct investigation documents	5 years	3 years This is a sufficient period for proving the repetition of the violation.
7.9.2.	Direct line manager conclusions, civil servant qualification evaluation questionnaires, evaluation commission conclusions, documents confirming an employee's refusal to sign an evaluation conclusion	10 years	3 years The subsequent information is not relevant to anyone and does not create legal effects.
7.1.2	Concerning annual, unpaid, educational and other leave;	10 years	3 years, and a 10-year retention period can only be included if the employee has unused leave for more than 3 years.
10.20.1	Personal account cards	50 years	No retention period since this is an excess requirement.

Source: Compiled by the authors

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 2 (December)
http://doi.org/10.9770/jesi.2022.10.2(39)

4. Specifics of processing data subject requests related to the right to be forgotten

Even though the data controller (employer) must store the data subject's data for a certain period of time, this does not exempt the data controller from the duty to comply with the requirements set out in the GDPR, including those related to the realisation of the data subject's rights, including those related to the right to be forgotten. The GDPR provides for the duty of the data controller to assess the data subject's request to delete data. Article 12(3) of the GDPR establishes that "the controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. That period may be extended by two months where necessary, considering the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay." Article 12(4) of the GDPR stipulates that "if the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy." Hence, by not providing any information regarding a request received on the right to erasure (implemented/partially implemented/not implemented), i.e. by not responding to an applicant's request, the data controller is not properly implementing the requirements of Article 12 of the GDPR (transparent information, communication and modalities for the exercise of the rights of the data subject) and is violating the rights of the data subject.

Accordingly, to realise the right to be forgotten, the employee does not have to comply with the formal requirements for such a request or specifically indicate the documents the employer must delete. In administrative case No eA-2108-822/2021, it is specified that it would be wrong for a data subject's request for the exercise of his or her rights to be disregarded simply because the request is not of the format and content expected by the data controller. The GDPR does not provide requirements for the specific content of the request that the data subject must submit to the data controller. Furthermore, individuals may simply request that their personal data be deleted without explicitly naming them, and the requirement to specifically call them disproportionately limits the exercise of their right to the "right to be forgotten" (Case No. eA-2108-822/2021, 2021).

The legal regulation of the duration of storage of job candidate data is unique in its own right. The report of the Committee of Ministers to Member States on the processing of personal data during recruitment states that "personal data submitted in support of a job application should normally be deleted as soon as it becomes clear that an offer of employment will not be made or is not accepted by the job applicant." (Recommendation, 2015). When such data is stored to provide more employment opportunities, the data controller must base such processing on at least one condition for the lawful processing of personal data (Article 6 and, where applicable, 9 or 10 of the GDPR). The data subject must be informed accordingly regarding for what purpose, on what legal basis, and how the personal data will be processed. If the legal basis is the consent of the individual, the data subject should make a decision of his or her own free will as to whether to give such consent (in this case, in the absence of consent, the personal data could not be further processed when inviting to new interviews). Furthermore, even after giving consent, the data subject can withdraw it at any time and request that the personal data be deleted.

It should be noted that even if the person does not request it, the data controller still has to regularly assess the erasure of personal data and decide whether circumstances that make it necessary to delete the personal data have arisen. This is required by the accountability principle enshrined in Article 5(2) of the GDPR, i.e. the employer must ensure compliance with the principles related to the processing of personal data, such as the principle of data minimisation and the principle of storage limitation.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 2 (December)
http://doi.org/10.9770/jesi.2022.10.2(39)

It should be noted that before a person starts participating in a recruitment process, he or she must be properly informed about data processing. In Lithuania, the by-laws still in force limit the ability of a candidate who has not been selected for a job to obtain the erasure of personal data concerning him or her without undue delay. At present, the legislation does not allow the documents of unsuccessful candidates to be stored for less than one year: "Applications and other documents submitted by applicants for a job competition are to be stored for one year (after the hiring deadline)." (Official Gazette, 2011). Analysing the provisions of the Index, this requirement cannot be applied to private data controllers. Pursuant to Article 17(1)(a) of the GDPR, at the end of the selection period, the personal data should be deleted because they are "no longer necessary in relation to the purposes for which they were collected or otherwise processed." Taking this into account, it can be concluded that the private and public sectors are subject to different requirements for storing the data obtained during a recruitment process. It was mentioned that in the public sector, data must be stored for another year after the selection process, but they cannot be used, for example, to invite the data subject to a selection. Meanwhile, there is no such imperative in the private sector, which means that the same purpose is not relevant in the private sector. It is proposed that the same requirements for storing data obtained in the recruitment process be applied in the public sector as in the private sector, i.e. that, pursuant to Article 17(1)(a) of the GDPR, the personal data be deleted at the end of the selection period because they are no longer necessary in relation to the purposes for which they were collected or otherwise processed, except if the further processing of the personal data is based on another condition of lawful data processing.

Conclusions

The right to be forgotten is not absolute – it can only be exercised when the information is excessive, irrelevant, inadequate or inaccurate. The public interest and the public's right to receive information have a higher priority in some instances than the individual's right to respect one's private and family life. In the context of personal data protection, the right to be forgotten is not only the duty of the data controller to constantly assess the expediency of the processing of personal data (in terms of scope, purpose and time) – it is also the ability of the data subjects to control how and where their personal data is processed.

Rather than being obliged to delete personal data without undue delay, the data controller must store the data for a certain period of time. One of the conditions obliging the data controller not to delete data is for compliance with a legal obligation which requires processing by Member State law to which the controller is subject. A person's right to obtain the erasure of personal data – or right to be forgotten – is directly related to the principle of limiting the duration of the retention period for personal data. If the data retention periods are not officially established, the obligation to establish the data retention period rests with the head of the agency or enterprise.

The personal data retention periods set out in national legislation were not changed after the regulation entered into force. Legislation usually only provides for a data retention period, without discussing other circumstances (purpose, categories of personal data, etc.), so it is more difficult to assess which period applies to a specific document or personal data processing operation. The more abstract the provision, the greater the responsibility of the data controller is to justify the personal data retention period chosen. Personal data retention periods must be associated with periods already established in legislation, such as limitation periods, procedural terms, or other juridical facts and circumstances.

Even though the data controller (employer) must store the data subject's data for a certain period of time, this does not release the data controller from the obligation to respond to the data subject's requests, including requests to be forgotten. Personal data submitted in support of a job application should normally be deleted as soon as it becomes clear that an offer of employment will not be made or is not accepted by the job applicant. It is proposed that the exact requirements for storing data obtained in the recruitment process be applied in the public sector as in the private sector, i.e., the personal data be deleted at the end of the selection period.

ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2022 Volume 10 Number 2 (December)
http://doi.org/10.9770/jesi.2022.10.2(39)

References:

Article 29 Data Protection Working Party: Guidelines on Transparency under Regulation 2016/679 (wp260rev.01), adopted on 29 November 2017, Retrieved July 15, 2022, from file:///C:/Users/User/Downloads/20180413_article_29_wp_transparency_guidelines_7B894B16-B8B9-B044-ED400A6DBAA4FA60_51025.pdf

Civil Code of the Republic of Lithuania. Book Two. Persons (*Official Gazette*, 2000, No 74-2262).

Code of Administrative Offenses of the Republic of Lithuania (*Official Gazette*, 10-07-2015, No. 2015-11216)

Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and 14 Rome, 4.XI.1950 (*Official Gazette*, 1995, No 40-987).

Charter of Fundamental Rights of the European Union (2016/C 202/02), Retrieved July 9, 2022, from https://eur-lex.europa.eu/legal-content/LT/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN.

Decision of the Supreme Administrative Court of Lithuania of 15 December 2021 in administrative case No eA-2108-822/2021

De Terwangne, C. (2013). The Right to be Forgotten and the Informational Autonomy in the Digital Environment, Luxembourg: *Publications Office of the European Union*, EUR 26434 EN, p 2, Retrieved July 12, 2022, file:///C:/Users/User/Downloads/jrc86750_cecile_fv.pdf

Erdos, D. (2021). The 'right to be forgotten' beyond the EU: an analysis of wider G20 regulatory action and potential next steps. *Journal of Media Law*, 13(1), 1-35. http://doi.org/10.1080/17577632.2021.1884947

Grigonienė, R. (2020). Legal Regulation Ensuring the Protection of Personal Data of Employees: A Critical Analysis. *Jurisprudence*, 27(2), 346-369. http://doi.org/10.13165/JUR-20-27-2-06

Judgment of the Court of Justice of the European Union (Grand Chamber) of 24 September 2019 in Case C-507/17 Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL). ECLI Retrieved July 10, 2022 https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CJ0507

Judgment of the Court of Justice of the European Union (Grand Chamber) of 13 May 2014 in Case C-131/12— Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González, EUR-Lex, Retrieved July 10, 2022 from https://eur-lex.europa.eu/legal-content/LT/TXT/HTML/?uri=CELEX:62012CJ0131&from=EN,

Judgment of the Court of Justice of the European Union (Sixth Chamber) of 22 September 2022 in Case C-120/21, LB v TO, request from the Bundesarbeitsgericht for a preliminary ruling, EUR-Lex, Retrieved July 20, 2022 from https://eur-lex.europa.eu/legal-content/lt/TXT/?uri=CELEX:62021CJ0120.

Judgment of European Court of Human Rights of 13 February 2020 in case Gaughran v. the United Kingdom (No 45245/15), ECHR, Retrieved July 20, 2022 from https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-200817%22]}, date of access: 18 June 2020.

Labor Code of the Republic of Lithuania (*Official Gazette*, 19-09-2016, No. 2016-23709).

Law on Documents and Archives of the Republic of Lithuania (*Official Gazette*, 1995, No 107-2389; 2004, No 57-1982).

Moore, S. (2017). The right to be forgotten is the right to have an imperfect past, *The Guardian*, 7 August 2017, Retrieved July 10, 2022, from https://www.theguardian.com/commentisfree/2017/aug/07/right-to-be-forgotten-data-protection-bill-ownership-identity-facebook-google

Order of the Chief Archivist of Lithuania adopted in 2011 March 9 No. V-100 "On Approval of the Index of General Document Storage Terms" (*Official Gazette*, 2011, No. 32-1534).

Petraitytė, I. (2013). Asmens duomenų teisinės apsaugos principai (Principles of legal protection of personal data; doctoral dissertation, Vilnius University, 2013), p 186, Retrieved July 10, 2022, from http://www.tf.vu.lt/wp-content/uploads/2016/08/Ilona-Petraityt%C4% 97_Personal-data%C5%B3-teisin%C4%97s-protection-principles-.pdf.

Recommendation CM/Rec(2015)5 of the Committee of Ministers to Member States on the processing of personal data in the context of employment, item 13.2, *CE*, Retrieved July 22, 2022 https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805c3f7a,

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Retrieved July 9, 2022, from https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32016R0679

Right to erasure. (2022). Information Commissioner's Office (ICO), Retrieved July 11, 2022, from https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/#ib1.

Summary of the results of lawfulness checks on the processing of personal data for the purposes of direct marketing and loyalty programmes (2018)(Asmens duomenų tvarkymo tiesioginės rinkodaros ir lojalumo programos tikslais teisėtumo patikrinimų rezultatų apibendrinimas), State Data Protection Inspectorate, Retrieved July 15, 2022 https://vdai.lrv.lt/uploads/vdai/documents/files/Apibendrinimasdeltiesioginesrinkodarosirlojalumo20180926.pdf .

Author Contributions: The authors contributed equally; they have read and agreed to the published version of the manuscript.

Andrejus NOVIKOVAS, Institute of Public Law at the Law School at Mykolas Romeris University. Research interests: administrative law, administrative procedure law, public security, public administration.
ORCID ID: https://orcid.org/0000-0002-2715-1402

Rasa GRIGONIENĖ, Institute of Private Law at the Law School at Mykolas Romeris University. Research interests: application of information technologies for protecting employee rights, telework, protection of the personal data of employees, labour disputes.
ORCID ID: https://orcid.org/0000-0002-2398-2639

.