BALTIC JOURNAL OF LAW & POLITICS
A Journal of Vytautas Magnus University
VOLUME 16, NUMBER 1 (2023)
ISSN 2029-0454

Cit.: *Baltic Journal of Law & Politics* 16:1 (2023): 24-41
https://content.sciendo.com/view/journals/bjlp/bjlp-overview.xml
DOI: 10.2478/bjlp-2023-0002

DISCRIMINATION ON THE BASIS OF PERSONAL DATA IN EMPLOYMENT: THE CASE STUDY OF LITHUANIA

Ingrida Mačernytė-Panomariovienė

Doctor, Senior Research Fellow
Institute of Law of the Lithuanian Centre for Social Sciences

Contact information:
Address: Ankštoji g./ Str. 1A, LT-01109, Vilnius (Lithuania)
Phone: Tel./Fax.: +3705 2497591
E-mail address: ingrida.macernyte@teise.org
ORCID https://orcid.org/0000-0003-0716-9354

Received: November 23, 2022; reviews: 2; accepted: March 6, 2023.

ABSTRACT

This article examines what kind of personal data disclosure may make it difficult to get employed and what kind of excessive (unlawful) data is collected when selecting candidates in Lithuania. The analysis reveals that there have been a number of justified complaints regarding the selection of employees via recruitment platforms and the provided application forms that specifically requested an excessive amount of information, or situations in which the conditions indicated in job listings were adapted to a specific circle of people, thus eliminating other potential candidates, such as persons of pre-retirement age, young families, persons with children, persons of a particular gender and similar groups of people. The purpose of this article is to identify methods of unlawful collection of personal data, as well as the types of requested personal data, the origin of which may lead to discrimination during the recruitment process in Lithuania. The article analyses the legality of documents requested from candidates, data collected from them by filling out application forms and providing preliminary or additional information during job interviews, or information gathered from former employers or social networks.

KEYWORDS

Personal data, discrimination, digital platforms, selection of candidates, equal opportunities, artificial intelligence (AI).

INTRODUCTION

Since the General Data Protection Regulation of the European Parliament and of the Council (hereinafter – GDPR) entered into force in May 2019[1], personal data and its protection have become a relevant topic not only in society, but also in science.

Individuals seeking employment must provide relevant data (documents) about their education, qualification, skills, work experience, etc. However, in some cases, the employer requests additional or even excessive data from the employee, and sometimes the employer collects such data about candidates independently (or through various online platforms, social networks or employment agencies that select candidates using IT apps, application forms and other tools). Is it always justified and permitted? What information can an employer collect about a potential employee and to what extent? These questions encourage us to find a balance between the employer's desire to select the best candidate and the individual's right to privacy.

Personal data (such as name, surname, personal identification number, age, gender, family or marital status, health condition, beliefs, hobbies, addictions, memberships, relationships with other persons, etc.) is closely related to personal privacy, which everyone (legally) must respect. Article 22 of the Constitution of the Republic of Lithuania states that "the private life of a human being shall be inviolable. <…> The law and the court shall protect everyone from arbitrary or unlawful interference in his private and family life, from encroachment upon his honour and dignity".[2] This principle also applies to employment relations. Article 88 of the GDPR obliges to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data and monitoring systems at the work place. In accordance with these principles, relevant laws have been adopted in Lithuania. Paragraphs 1 and 3 of Article 27 of the Labour Code of the Republic of Lithuania (hereinafter referred to as LC)[3] states that "the employer must respect the employee's right to private life and ensure the protection of the employee's personal data. <…>. The specifics of the implementation of the employee's right to private life may be established by laws and other labour law provisions." Accordingly, Law on Legal Protection of Personal Data of the Republic of Lithuania (hereinafter – LLPPD)[4] provides for certain restrictions (prohibitions and permissions) related to the collection and processing of personal data of a candidate applying to perform duties or conduct work functions.

A number of studies on various aspects of personal data protection, including labour relations, have been conducted. This topic was mainly described by the following foreign researchers: R. Sprague[5], who wrote about the social networks blurring the line between personal life and the employment relations; M.-A. Péano[6], who wrote about

1 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. OL L 119, 2016 5 4, p. 1—88.
2 Constitution of the Republic of Lithuania. 1992, *Official Journal*, 33-1014.
3 Republic of Lithuania Labour Code. 2016, *TAR,* 23709.
4 Law on the Legal Protection of Personal Data of the Republic of Lithuania amending Law No. I-1374 (2018) *TAR*, 117 33.
5 Robert Sprague, "Invasion of the Social Networks: Blurring the Line Between Personal Life and the Employment Relationship," *University of Louisville Law Review* 50 (2011): 1.
6 M.-A. Péano, "L'intuitus personae dans le contrat de travail," *Droit social* 2 (1995): 132-133.

personal data in the employment context, I. Byrnside[7], S. F. Befort[8], A. Bidet, and J. Porta[9], who all wrote about employee selection; as well as A. Lukács[10], who studied protection of employees' right to privacy and right to data protection on social network sites – with special regard to France and Hungary – in his dissertation, and other researchers. In Lithuania, R. Grigonienė[11] studied employees as a separate group of subjects related to personal data protection, while G. Tamašauskaitė-Janickė[12] and I. Petraitytė[13] analysed the principles of personal data protection in the context of employment relations, data arising from the employment contract, performance of the employee's functions, his or her salary, etc.; meanwhile, E. Štareikė[14] studied *the assurance of employees' rights to privacy and the protection of their personal data.*

The purpose of this article is to identify methods of unlawful collection of personal data, as well as the types of requested personal data, the origin of which may lead to discrimination during the recruitment process in Lithuania. The article analyses the legality of documents requested from candidates, data collected from them by filling out application forms and providing preliminary or additional information during job interviews, or information gathered from former employers or social networks.

During the research, methods of systematic analysis, document analysis, content analysis, as well as comparative and logical methods were used. The object of research is the randomly selected complaints about the discriminatory elements during the recruitment process that were examined by Office of the Equal Opportunities Ombudsperson of the Republic of Lithuania (hereinafter referred to as "the Office"), as well as Lithuanian and international case law, scientific doctrine and legislation of Lithuania and the European Union (hereinafter referred to as "EU").

1. COLLECTION OF PERSONAL DATA NECESSARY FOR EMPLOYMENT: CONCEPT AND LEGALITY

According to Article 4 of the GDPR, 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

---

7 Ian Byrnside, "Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants" *Vanderbilt Journal of Entertainment and Technology Law* Vol 10 No 2, (2008): 445-477.

8 Stephen F. Befort , "Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place" *Hofstra Labour and Employment Law Journal* Vol 14 No 2 (1997): 365-422.

9 Alexandra Bidet and Jerome Porta, "Le travail à l'épreuve du numérique," *Revue droit du travail* 5 (2016): 328.

10 Adrienn Lukács, "Protection of Employees' Right to Privacy and Right to Data Protection on Social Network Sites – With Special Regard to France and Hungary," (University Paris 1 Panthéon Sorbonne and University of Szeged Doctoral (PhD) dissertation 2020).

11 Rasa Grigonienė, "Legal Regulation Ensuring the Protection of Personal Data of Employees: a Critical Analysis," *Jurisprudence* Vol 27 No 2 (2020): 346–369.

12 Gintarė Tamašauskaitė-Janickė, "The Usage of Information and Communication Technologies at the Workplace in the Context of Labour Law" (Vilniaus university Doctoral (PhD) dissertation 2016), pp 82–83.

13 Ilona Petraitytė, "The Personal Data Protection Principles" (Vilniaus university Doctoral (PhD) dissertation 2013), p 186.

14 Eglė Štareikė and Sigita Kausteklytė-Tunkevičienė, "The main rights of the data subject and their enforcement in accordance with the EU General Data Protection Regulation," *Public Security and Public Order* 20 (2018); Eglė Štareikė, "Assurance of the Right to Privacy and the Protection of Personal Data in Labour Relations" *Public Security and Public Order* 26 (2021): 221-235.

In answering the question of what information constitutes personal data, it should be noted that there is no such information relating to a natural person that cannot be deemed personal data *a priori*. The information can take any form, come from any source, and have any other features characterising information; however, if such information can be linked to a specific natural person, it must be considered personal data.[15]

In accordance with the LLPPD, personal data is any information relating to a natural person who is known or can be identified, directly or indirectly, by reference to data such as an identification number, one or more factors specific to the physical, physiological, psychological, economic, cultural or social nature of the individual. Personal data can be described by many factors. Therefore, a person's name and surname[16] personal identification number[17] amount of personal income, information about the recipients of benefits paid by companies, the person's e-mail address associated with his or her surname, place of residence, phone number, information about the personal interests[18], and other information about the person, are unquestionably recognised as personal data.

Currently, the LC (2016) does not specify what types of personal data an employer may request. In individual cases, the mandatory provision of such data may be regulated by other laws or secondary legislation; however, it must be assessed by reference to each position, place of work or status of the applicant individually. Most personal data, such as name and surname, identity card number, personal identification number, place of residence, phone number and e-mail address are gathered by filling out the Template of Employment Contract[19], which was approved by Order No. A1-343 of the Minister of Social Security and Labour of the Republic of Lithuania of 29 June 2017. But is it really necessary to provide all of these details in order to be hired?

To collect data from a person applying for a specific position, it is necessary to determine what data can be collected and to what extent, because the employer's and employee's interests (objectives) may conflict. On the one hand, specific personal data may be important for an employer, in order to find a suitable candidate for a position based on special requirements (e.g. individuals can apply for certain positions only if they have the appropriate nationality (for example, a person is a citizen of a Member State of the European Union or of another party to the Agreement on the European Economic Area or of the Swiss Confederation; <…>[20]; a person may be appointed a bailiff if he is a national of the Republic of Lithuania and a person of high moral character <…>[21], etc.), age (for example, the office of notary may be held by a natural person, provided he is not more than 70 years of age[22]), place of residence (for example, "a permanent resident of the respective municipality may be elected as a member of the municipal council"[23]), knowledge of the national language (for example, "the office of notary may be held by a natural person, provided he: <..> 2) knows the official language[24] etc.) in order to protect the employer's assets and property (to ensure that equipment provided

15 Petraitytė, *supra note* 13, 54.
16 *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer*. CJEU (2009, No. C-553/07).
17 *UAB „Init" v. the State Data Protection Inspectorate.* Supreme Administrative Court of Lithuania. (2013, No. A822 -1173-2013).
18 *Criminal proceedings v. Bodil Lindqvist. CJEU* (2003, No C-101/01).
19 Order No. A1-343 of the Minister of Social Security and Labour of the Republic of Lithuania of 29 June 2017 "On Approval of Template of the Employment Contract". 2017, *TAR,* 11167.
20 Republic of Lithuania Law on the Notarial Profession. 1992, *Lietuvos aidas*, 192-0. Art. 3.
21 Republic of Lithuania Law on Bailiffs. 2002, *Official Journal,* 53-2042. Art. 4.
22 Republic of Lithuania Law on the Notarial Profession. 1992, *Lietuvos aidas*, 192-0. Art. 3.
23 See: Republic of Lithuania Law on Elections to Municipal Councils. 1994, *Official Journal,* 53-996.
24 Republic of Lithuania Law on the Notarial Profession. 1992, *Lietuvos aidas*, 192-0. Art. 3.

by the employer is used in accordance with its purpose at work), to protect his or her economic interests (e.g. to ensure productivity at work or to protect reputation) and to ensure the safety and health of other employees (such obligations on employers are imposed by the LC (2016) and the Law on Safety and Health at Work of the Republic of Lithuania[25]). From a legal perspective, the employment relationship is considered to be a personal, long-term legal relationship, where the identity of the parties plays an important role: performing work in person is one of the primary qualifying attributes of the employment relationship, having crucial importance[26]. The employer may involve either "screening in" applicants who possess desirable characteristics or "screening out" applicants who possess undesirable characteristics.[27] Pre-employment screening may contribute to higher productivity, increased quality, and lower employee turnover, as well as identifying whether an applicant has a criminal background.[28] On the other hand, the protection and privacy of personal data are important for a future employee, especially when they are published (on former/current workplace webpages, other websites or certain social networks (personal or professional pages, etc.) and have privacy features.

In order to protect the interests of the opposing party, data collection imposes certain constraints on both subjects of employment relationships. According to Article 22 of the Constitution of the Republic of Lithuania[29], only "the law and the court shall protect everyone from arbitrary or unlawful interference in his private and family life, from encroachment upon his honour and dignity". This means that prohibitions and restrictions on the collection, processing and storage of personal data can only be imposed by laws. The legal regulation establishes the scope of information that can be collected (e.g. rules related to the prohibition of discrimination or respect for personal or private life), considering certain subjective characteristics, such as the applicant's personality.[30] Article 5 of the LLPPD provides for certain restrictions on the collection and processing of personal data in relation to employment cases, including data of candidates applying to perform work functions. First of all, the employer must be aware of the applicant's qualifications, professional skills and professional qualities. The applicants usually provide this information to the employer at the time and in the manner indicated in the job listings. The term 'personal data' does not include information about a person's professional activities, and the requirement to provide information about the previous workplaces does not violate the LLPPD because the employer intended to learn about the applicant's professional qualities. Information about previous workplaces is also not considered part of the concept of inviolability of private life.[31] Information on previous workplaces is, first and foremost, information on the work experience of a candidate applying for the specific position. Because the plaintiff did not provide his driver's licence or any other identity documents during the selection procedure, the defendant was unable to fill out the application form and learn which lorries the plaintiff had driven or which countries he had worked in; therefore, the defendant suspected that the plaintiff had no work experience. According to the court, the fact that the plaintiff did

25 Law on the Legal Protection of Personal Data of the Republic of Lithuania amending Law No. I-1374. 2018, *TAR*, 117 33.
26 Lukács, *supra note* 10, 246.
27 Befort, *supra note* 8, 367-368.
28 Alan Kinsey, "The Benefits of Pre-employment Screening," James M. Sweeney and Associates, Inc. pp 2-3 (23 January 2022). // http://www.sweeneyinc.com/files/benefits_preemployment_screening.pdf.
29 Constitution of the Republic of Lithuania. 1992, *Official Journal,* 33-1014.
30 Péano, *supra note* 6, 132-133.
31 *A. K. v. UAB „Transkedavė"*. Kaunas Regional Court (2010, No. 2A-1749-390).

not meet the requirements of the defendant, such as having the driving experience, does not constitute discrimination.[32]

However, the employer wants to know not only about the candidate's education and work experience, but also about his personality and beliefs in order to determine whether the applicant can easily identify with the core values of the hiring company[33]. Therefore, the content of the information about the candidate's previous workplaces may differ from the clarification of his or her work experience. For example, his extensive work experience and personal characteristics such as accountability and reliability[34], or the fact that the employee has a conflict-free personality.

In some cases, the employer wants to know information about the applicant's criminal convictions, impeccable reputation (e.g. due to the state duties[35]), etc. The LLPPD prohibits processing personal data on convictions and criminal offences of a candidate for a position or a job function and an employee, except when such personal data are required to verify whether a person meets the requirements outlined in laws and implementing legislation for the performance of duties or job functions (Art. 5(1)). It means that if the law allows for the collection of personal data on convictions and criminal acts, it will be legal.

After studying Lithuanian laws, such as the Law on the Approval of the Statute of the Internal Service of the Republic of Lithuania, Aviation Law, Law on Banks, Law on Civil Service, Law on Education and others, applicants seeking to hold certain offices, such as a diplomat, director, civil servant, notary, official, judge, etc., must meet certain special requirements, such as having not only citizenship of the Republic of Lithuania, but also an impeccable reputation, no convictions and no unexpired (which means, for example, 3 years from the date) instances of dismissal or recognition of grave official misconduct[36] disciplinary penalties, etc. For example, the Law on Fundamentals of Protection of the Rights of the Child provides for the following restrictions on working with children: "persons found guilty by a final court conviction for crimes against a person's sexual selfdetermination and inviolability, child exploitation for pornography, profit from child prostitution, involvement of a child in prostitution or disposition of pornographic content depicting a child or presenting a person as a child, purchase or sale of a child, as well as other intentional serious or very serious crimes or analogous offences provided for in the criminal laws of other countries, regardless of whether or not the criminal record is expired or annulled."[37]

In some cases, the employer may ask for information about the applicant's health in order to assess his professional abilities (a medical certificate is usually requested at the time of recruiting). However, such a requirement cannot be applied automatically to every vacant position. In accordance with Articles 5 and 9 of "Recommendation of the Committee of Ministers to Member States on the Processing of Personal Data in the Context of Employment," health data may only be collected to fulfil legal obligations and in accordance with appropriate safeguards, complementing those set out in the present

---

32 *Ibid*.
33 Sprague, *supra note* 5, 6; Alan Finder, "For Some, Online Persona Undermines a Résumé," *The New York Times* (2006). // https://www.nytimes.com/2006/06/11/us/11recruit.html.
34 *D. P. v. Radviliškis district municipality Radviliškis district municipality administration.* Panevėžys Regional Court (2019, No. 2A-269-252).
35 *GC and Others v Commission nationale de l'informatique et des libertés (CNIL) CJEU* (2019, No C-136/17).
36 Republic of Lithuania Law on the Civil Service. 1999, *Official Journal*, 66-2130. Art. 4 (2, 5).
37 Republic of Lithuania Law on Fundamentals of Protection of the Rights of the Child. 1996, *Official Journal*, 33-807. Art. 30.

recommendation[38]. Article 18 of the Law on the Prevention and Control of Communicable Diseases in Humans of the Republic of Lithuania[39] provides that the Government shall establish the list, and procedure of the health examinations of the jobs and areas of activity in which employees are permitted to work only after prior health examination.

Information about health or addictions is considered confidential data; therefore, prospective employers could only ask for it if it is required by law. In accordance with the Law on Safety and Health at Work of the Republic of Lithuania[40] the compulsory health checks apply only to the groups associated with increased health risk, rather than all professions or positions and new employees.

Personal data of candidates or applicants may only be collected for recruitment purposes, which are indicated in law (in order to hold office) and on reasonable grounds, without discrimination against their family status, gender, age, or other factors.

2. METHODS FOR COLLECTING DATA FROM CANDIDATES APPLYING TO PERFORM DUTIES OR CONDUCT WORK FUNCTIONS

Data on candidates or job applicants can be collected using various methods through several stages, including application forms, interviews, social networks, interviews with former employers, etc. The primary data is collected by filling in an application form. Later, data may be collected during an interview or (oral) test – during the interview based on the submitted questionnaire; meanwhile, during the final selection stage, the selected candidates may be asked for additional information (e.g. about their health) or clarification of existing information (e.g. obtained from social networks, former employers and other sources).

An applicant must be properly informed about data processing prior to his or her participation in the recruitment process.[41] Article 5 of the GDPR provides a general rule permitting an employer to collect personal data directly from the corresponding data subject, *i.e. from the candidate or applicant; and,* legislation and job listings indicate to provide the relevant information and the supporting documentation.

To check the suitability of candidates, prospective employers frequently rely on the information provided by their former employers or current employer. For example, during the selection procedure for the position of an international truck driver-freight forwarder, the plaintiff was told during the interview that in order to participate in the further selection process, he had to produce written recommendations from former employers, as well as a copy of his driver's licence.[42]

It is especially important that when data is gathered from third parties on a legal basis, such as to seek professional advice, the data subject should be notified about it in advance. Article 5(2) of the LLPPD imposes restrictions regarding data collection by indicating sources from which information may be collected. According to the LLPPD, the prospective employer may collect personal data relating to qualifications, professional skills and qualities of a candidate from a former employer by informing the candidate

---

38 Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment, 5. p., CE. Adopted by the Committee of Ministers on 1 April 2015, at the 1224th meeting of the Ministers' Deputies.

39 Republic of Lithuania Law on the Prevention and Control of Communicable Diseases in Humans. 1996, *Official Journal,* 104-2363.

40 Republic of Lithuania Law on Safety and Health at Work. 2003, *Official Journal*, 70-3170. Art. 21.

41 Grigonienė, *supra note* 11, 359.

42 *A. K. v. UAB „Transkedavė*". Kaunas Regional Court (2010, No. 2A-1749-390).

in advance and from the existing employer – only with a consent of the candidate. Both information and consent must be given in writing (by electronic or other methods). Specific Lithuanian laws impose this obligation, for example, when a candidate for judicial office agrees in writing to have his candidacy checked[43].

In Lithuania, the employer also has the right to collect lawful information about the candidates applying for duties from other entities, such as:

a) Former employers, from whom an employer may request information regarding a person's unexpired disciplinary penalties. For example, the National Courts Administration may request information about candidates for judicial office or Special Investigation Service may request information about candidates for civil service;

b) Competent public authorities (such as Prosecutor General's Office of the Republic of Lithuania, Special Investigation Service or other institutions of pre-trial investigation), from which an employer, acting pursuant to the Law on Prevention of Corruption[44], may request information about a candidate[45] who won a competition and was selected for a position that was included in the list of positions subject to competition in accordance with Article 41(3) of the LC (2016);

c) State Security Department of Lithuania, which an employer may ask whether a candidate for judicial office meets the requirements necessary for the granting of a work permit or access to classified information in accordance with the procedure set out in the Law on State Secrets and Official Secrets of the Republic of Lithuania[46];

d) Register of Suspects, Accused and Convicts, checking whether a person has not been convicted of certain crimes[47];

e) A court where a judge is employed or is applying, by requesting the opinions of a group of judges[48];

f) Others.

The internet and social networks have dramatically increased the possibilities for finding information that can assist employers in finding qualified candidates. They became popular in recruitment methods and established themselves in the initial stage of selection process. Employers are increasingly using "Google," "Facebook," "Twitter," "LinkedIn," "ResearchGate" and other websites to find candidates, verify their information and learn about their personal characteristics, hobbies, and relationships. Therefore, it is critical to distinguish between professional (where individuals share facts about their professional lives, achievements, career, opportunities, etc.) and personal (where individuals interact with their friends and share impressive moments of their lives) social networks because screening of personal social networks may raise suspicions of collecting excessive information, unjustified data, as well as questions about personal privacy and data protection violations.[49] The legitimacy of such activities is frequently based on making information public, as though the person willingly gave his consent for everyone to see the information he shared. According to R. Grigonienė, it

43 Republic of Lithuania Amending the Law on Courts. 1994, *Official Journal,* 46-851. Art. 53-2.
44 Republic of Lithuania Law on Prevention of Corruption. 2021, *TAR*, No. 15850. Art. 17.
45 Resolution No. 496 of the Government of the Republic of Lithuania "On the Implementation of the Labour Code of the Republic of Lithuania." 2017, *TAR*, 10853.
46 Republic of Lithuania Law on State Secrets and Official Secrets. 1999, *Official Journal*, 105-3019.
47 Republic of Lithuania Law on Fundamentals of Protection of the Rights of the Child. 1996, *Official Journal,* 33-807. Art. 30.
48 Republic of Lithuania Amending the Law on Courts. 1994, *Official Journal,* 46-851. Art. 55-1 (7).
49 Byrnside, *supra note* 7, 457-458.

is difficult to assess such actions unambiguously.[50] Meanwhile, I. Petraitytė discovered that making personal data public does not imply that the published information is no longer classified as such.[51]

3. RESTRICTIONS ON THE COLLECTION OF PERSONAL DATA OF A CANDIDATE: WHAT KIND OF PERSONAL DATA SHOULD NOT BE COLLECTED?

Articles 2 and 26 of the LC (2016) prohibit employers from discriminating against employees due to circumstances unrelated to the employees' professional qualities. In other words, any direct or indirect discrimination, harassment, sexual harassment or instruction to discriminate on the grounds of gender, race, nationality, language, origin, social status, age, sexual orientation, disability, ethnic affiliation, political affiliation, religion, faith, convictions or views, except for cases concerning a person's professed religion, faith or convictions for those working in religious communities, societies or centres, provided that the requirement for the employee regarding his or her professed religion, faith or convictions, in view of the ethos of the religious community, society or centre, is normal, lawful and justifiable, or intention to have a child/children, or due to circumstances unrelated to the employees' professional qualities or on other grounds established by laws, shall be prohibited. For example, during the oral test, the applicant was asked questions that had nothing to do with her ability to perform the duties of head of a health care institution.[52] This means that any information that is not related to the candidate's future position or the professional qualities required to perform her duties shall be considered excessive or unlawful.

3.1. Excessive data

The right of an employer to collect excessive information that is not related to work is restricted in accordance with paragraphs 2 and 3 of Article 5 of the GDPR: personal data collected by employers for recruitment purposes must be relevant and not too broad, and should attend to the nature of the work and the changing information needs of the employer. Employers should refrain from demanding that an employee or job seeker provide them access to personal information that he or she posts to others online, especially through social networks. An employer has the right to collect an applicant's data independently, for example, both from former employers and other entities or even from a publicly accessible databases such as social networks, only if it is reasonable. The legal assessment of the collection of information on the candidate on social networks was provided by the Working Group[53], emphasising not only the validity of the purpose of information collection on social networks, but also the importance of properly informing employees about such actions, i.e. candidates should be properly informed (for example, in the text of job listing).

In accordance with the principle of data minimisation[54] set out in the Regulation, personal data shall be adequate, relevant and limited to what is necessary in relation

---

50 Grigonienė, *supra note* 11, 357.
51 Petraitytė, *supra note* 13.
52 *D. P. v. Radviliškis district municipality, Radviliškis district municipality administration.* Panevėžys Regional Court (2019, No. 2A-269-252).
53 "Opinion 2/2017 on data processing at work", 10, State Data Protection Inspectorate of the Republic of Lithuania. // https://vdai.lrv.lt/uploads/vdai/documents/files/Nuomonedelduomenutvarkymodrabe-20170608wp249lt(2).pdf.
54 Regulation (EU) 2016/679, *supra note* 1: article 5 para 1 (c).

to the purposes for which they are processed. A list of personal data to be provided should also be assessed by applying the principle of personal data minimisation. In legal doctrine, this principle is associated with the principle of proportionality. According to E. Leonaitė, the proportionality is defined as a balance between the restriction and the objective being pursued.[55]

In advertisements offering job, civil service or education opportunities, it shall be prohibited to specify requirements giving preference on grounds of sex, race, nationality, citizenship, language, origin, social status, belief, convictions or views, age, sexual orientation, disability, ethnic origin or religion.[56] It shall be prohibited in job advertisements to request information from job seekers about their family status, age, private life or family plans.[57]

When hiring an employee, it is obvious that the employer is legally obliged to identify him- or her-self (by providing personal identification number) and indicate the necessary contact information (postal address, phone number or e-mail address); however, it is not reasonable to include data collected from a passport or personal identity card in the Employment Contract, the template of which has been approved by the Minister for Social Security and Labour[58]. In addition, this data may change, requiring the employee to notify the employer of any changes. Meanwhile, as with any other data collection, the employer must explicitly declare the purpose of the collection, the location of storage, how the employee can request data changes, etc.[59]

The processing of personal data of a candidate applying for a position involves several problematic aspects that considerably increase the risk of violating the candidate's right to personal data protection. The collection of personal data on a candidate in order to gain as much information as possible about the potential employee can be distinguished separately.[60] For example, the court[61] noted that, in the examined case, a person's specific duties, even without providing any other data identifying a person, may be sufficient to identify a particular person of a social nature, and that if specific data about a person's remuneration is to be considered information of a private nature, it is necessary to assess whether such data can be disclosed. Because in accordance with Article 148(3) of the LC (2016) "information about an individual employee's remuneration may only be provided or published in the cases established by law or with the employee's consent." For example, the Court of Justice European Union (hereinafter – CJEU) has found that Articles of Directive do not preclude national legislation <…> the wide disclosure not merely of the amounts of the annual income above a certain threshold of persons employed <…> but also of the names of the recipients of that income is necessary for and appropriate to the objective of proper management of public funds pursued by the legislature.[62]

---

55 Erika Leonaitė, "The Principle of Proportionality and its Application by the ECHR in Art. 8 Cases Against Lithuania," *Teisė* Vol 77 No 116 (2010): 113-125.

56 see: Republic of Lithuania Law on Equal Treatment. 2003, *Official Journal*, 114-5115. Article 11.

57 See: Republic of Lithuania Law on Equal Opportunities for Women and Men. 2016, *TAR*, 26966. Article 16.

58 Order No. A1-343 of the Minister of Social Security and Labour of the Republic of Lithuania of 29 June 2017 "On Approval of Template of the Employment Contract". Register of Legal Acts. 2017, *TAR*, 11167.

59 Grigonienė, *supra note* 11, 359.

60 *Ibid,* 357.

61 *D. P. v. Kaunas Red Cross Clinical Hospital.* Supreme Administrative Court of Lithuania (2011, No. A492 -2809).

62 *Rechnungshof v Österreichischer Rundfunk and Others* (C-465/00) and *Christa Neukomm v Österreichischer Rundfunk* (C-138/01) and *Joseph Lauermann v Österreichischer Rundfunk* (C-139/01) CJEU (2003, Joined Case No C-138/01,C-465/00,C-139/01).

Candidates are frequently asked about their work experience in applications or during interviews, including requests to list all previous workplaces, employment lengths and roles. This information is related to the verification of competences and skills needed to perform the duties. On the one hand, this information could be used against an employee who regularly changes jobs or does not complete a probationary period because the frequency of changing jobs may have an impact on the candidate's (in)capacity to work. On the other hand, such data does not allow employers to gain complete information on the quality of the candidate's performance of such duties, as well as any existing additional competencies or skills that a company requires but were not required by the candidate's past employers.

In Lithuania, instances where a candidate may be forced to disclose excessive information can be distinguished. Candidates are sometimes asked (in job listing, application or during an interview) to provide other information that is not related to their work or duties, such as whether they have a tendency to get sick, whether they own a car or have any financial obligations, whether they have a family or children and how old they are, what their hobbies are, whether they have a conflict-free personality or whether they had friendly relations with former colleagues, etc.

Special data (e.g. used by taking management positions, particularly at enterprises or facilities of strategic importance to national security, or by taking other positions in the public service) may be requested from a candidate only if the laws or other legislation impose an unambiguous obligation on the employer to appoint persons to positions indicated in the List of Positions or to check the appointed persons in accordance with the procedure established by the Government to see if they meet the established criteria or cannot be appointed to or hold the positions referred to in the List of Positions.[63] It was also demonstrated by the European Court of Human Rights (hereinafter – ECHR) in one of the cases where it was sought to determine whether the applicant could be subject to a specific law: "The scheme did not provide for an individual assessment of the evidence on each person featuring in the security services' surviving records. The statute only affects those who have taken up posts of special importance since the fall of the regime."[64] Although the employment of former secret agents is prohibited by law, it only applies to the selection of candidates applying for a specific position.

Since the employer is required to justify why certain information about the candidate is collected and processed, the fact that the employer has reviewed a publicly available candidate's account created for professional purposes would make the necessity for such a review easier to justify. However, it is critical to ensure that the determination of the scope of personal surveillance is not arbitrary or discriminatory.

Not only should excessive personal data not be collected, but also personal data should not be kept for longer than necessary. For example, information should not be collected solely to supplement an employer's database with potential candidates in the hope that this information will be needed someday without the intention of recruiting a new person at that time. Therefore, employers should not keep CVs and other data of potential candidates even if they believe they may need such an employee in the future. Such data may be reasonably stored for as long as the period for appealing an unlawful refusal to hire a person is valid.

---

[63] Law No. IX-1132 of the Republic of Lithuania amending Law on Enterprises and Facilities of Strategic Importance for National Security and Other Undertakings Important for National Security No. IX-1132. 2018, TAR, 1004. Art. 17 (2).

[64] *Anchev v. Bulgaria* ECHR (2018, No. 38334/08 and 68242/16).

Another point is the prohibition on disclosing personal data to third parties by providing excessive information. The provision of personal data to third parties without specifying such a purpose prior to data collection may be difficult to justify. Vilnius Regional Administrative Court decided in the hearing[65] held in 2019 that the State Data Protection Inspectorate legitimately imposed a reprimand on a company that, while in litigation with its former employee over the allegedly unlawful dismissal, contacted the recruitment agency, which offered this candidate, and asked it to provide data about the employee to the court. The mere act of requesting data from third parties to the court is not considered a violation in itself. The company was fined because, by requesting data, it revealed to the recruitment agency that the employee in question had been fired for serious breach of labour discipline. According to the Inspectorate, disclosing such excessive data to a third party for the achievement of a specific purpose was unnecessary, and the employee was not properly informed about such use of his data.

Therefore, the collection of personal data in each specific case must be linked to the purposes and legal grounds set out in the GDPR. The collection of information on social networks can reveal a lot of excessive information about the habits of a potential employee, as well as his views, interests, financial situation, etc. If the collection of such data is not related to professional duties, then such actions violate the employee's right to privacy and set the foundation for discrimination against him.

3.2. Personal data, the collection of which may result in discrimination during the recruitment process

Employers frequently fail to realise that certain questions they ask a candidate during an interview may be interpreted as unethical or discriminatory instruction communicated through an intermediary regarding the candidate's preferred qualities, such as specific gender, age or other features, because discrimination may also be indirect and covert. For example, collecting information, even of a personal nature, such as name, surname, date of birth, personal identification number, etc., may also serve to identify other information about applicants.

One point of personal data that is frequently requested in recruitment applications is the personal identification number. Processing a personal identification number may be reasonable; therefore, it is not considered a violation of the GDPR in itself; however, the Supreme Administrative Court of Lithuania already noted in 2013 that when a person can be unambiguously identified from the entirety of personal data, there is no need to use a personal identification number for that purpose.[66] However, personal identification number provided for a person's identification in Lithuania was developed in accordance with the standard of the Republic of Lithuania RST 1185-91 "Personal Identification Number. Composition and Structure," which entered into force on 1 December 1991. It is a unique sequence of eleven decimal numbers that identifies a person and is used to process data about him or her in databases processed by the state. Accordingly, the employer can instantly identify the applicant's gender by knowing his or her personal identification number because the first number encodes the person's century of birth and gender (1 means a male born in the 19th century, 2 means a female born in the 19th century, 3 means a male born in the 20th century, 4 means a female born in the 20th century,

[65] *A. D. v. the State Data Protection Inspectorate.* Vilnius Regional Administrative Court (2019, No. I-822-643).
[66] *UAB „Init" v the State Data Protection Inspectorate.* Supreme Administrative Court of Lithuania (2013, No. A822 -1173-2013].

5 means a male born in the 21st century and 6 means a female born in the 21st century), as well as his or her age because the following six numbers refer to the date of birth: the two last digits of the year, two digits of the month and two digits of the day.

When recruitment platforms require a person to fill out forms with personal information, they get an opportunity to filter preferred candidates based on their personal identification number (both when applications are reviewed by individuals and artificial intelligence). For example, after investigating the complaint, the Office of the Equal Opportunities Ombudsperson discovered that the company automatically limited the number of job offers for women in its electronic system "workis.online". It hid offers from natural persons on the platform based on their personal identification number (3 and 5 meaning males, 4 and 6 meaning females) and did not display women's job offers where cargo loads exceeded 10 kilograms, despite the fact that some women with suitable physical build were able to do those jobs. The Company provided its services (via "workis.online" platform) to its clients (job seekers) differently, depending on their gender: certain job offers were hidden from women.[67]

In accordance with Article 3(2) of the Law on the Spelling of a Person's Name and Surname in Documents of the Republic of Lithuania[68], unlike the citizens of the Republic of Lithuania who are of non-Lithuanian nationality, the surname given by the spouse to the other spouse or to the child of parents or either parent shall be written in Lithuanian characters in the documents confirming the identity of the citizen of the Republic of Lithuania and in the entries of the civil status registers by taking into account differences in the surname form according to a person's gender. However, in the issued passports of citizens of the Republic of Lithuania, the names and family names of individuals of non-Lithuanian nationality shall be written in Lithuanian characters. Under a citizen's written request of an established form, his name and family name shall be written according to the pronunciation and without conforming to the grammatical rules (without Lithuanian inflexions).[69] Accordingly, differences regarding Lithuanian inflexions in names and surnames (as noted by the Constitutional Court regarding the preservation of national identity) occur due to the preservation of the identity of the nation, i.e. when applicants of Lithuanian origin provide their name and surname, the employer gets information not only about their gender, but also about their marital/non-marital status. Of course, the employer should only use such information to identify a person and not consider it critical data when selecting candidates for a position.

Investigation of complaints conducted by the Office of the Equal Opportunities Ombudsperson[70] has revealed a lot of cases in which employers collected excessive data of a discriminatory nature about the candidates. The review of a lot of complaints has confirmed that many job offers (most of which was published on www.cvbankas.lt), interviews or individual inquiries of applicants about their future position or job were subject to discriminatory content with regard to candidates because they were asked to provide general personal data that was not directly related to their future duties,

67 Decision No. (21)SN-140) SP-56 of the Office of 27 October 2021. (20 May 2022).// https://www.lygybe.lt/data/public/uploads/2021/10/21sn-140sp-56.pdf.

68 Law on the Spelling of a Person's Name and Surname in Documents of the Republic of Lithuania. Register of Legal Acts. 2022, *TAR*, 1142.

69 Ruling of the Constitutional Court of the Republic of Lithuania of 21 October 1999 on the compliance of the Resolution of the Supreme Council of the Republic of Lithuania "On Writing Names and Family Names in Passports of Citizens of the Republic of Lithuania" of 31 January 1991 with the Constitution of the Republic of Lithuania, 1999.

70 Investigations of complaints conducted by the Office of the Equal Opportunities Ombudsperson can be found on the following website: Available at:< https://lygybe.lt/lt/kontrolieriaus-priimti-sprendimai >(accessed 20 May 2022).

for example, the employer wanted to know their gender[71],[72],[73], age[74],[75], nationality or citizenship[76], family status[77],[78], social status[79], sexual orientation[80] rather than their experience, education and competences. The request for such information concerns not only discrimination but also the exclusion of potential employees, who do not meet the employer's selection criteria based on age and other factors. It may prevent the applicant from being hired if, for example, the company is looking for a young person (under 50[81] or 53 years of age[82], preferring a female over male[83] or vice versa.[84]

By requesting information about income from a candidate, it is also clear that the aim is to discriminate against the applicant based on his or her sociability, the ability to meet (or adapt to) the representativeness of the company (whether a person will arrive to work by car, what kind of car, what clothes he or she will wear, etc.). However, the provision of information about income may be justifiable, for example, if it is needed for reasons of public interest.[85] The collection of information about a person's membership in the organisation, affiliation with it or links to it must also be assessed cautiously (here, one can see the possibility of discrimination when a person becomes aware that another person is linked to persona non grata due to differences in the party's interests, friendship with representatives of certain minority groups, etc.).

The Office also discovered cases of violations on the grounds of citizenship, nationality and origin, such as when a company decided that the applicant was not Lithuanian and blocked her account after seeing her "foreign" name and surname. Despite the fact that the applicant was a citizen of the Russian Federation and a member of the family of a citizen of a Member State of the European Union (the Republic of Lithuania), the company has not requested to disclose the citizenship and status. Therefore, employers had no right to inquire about her citizenship, nationality and other personal data[86] and had no reason to restrict her ability to participate in the selection process.

---

71 Decision No. (21)SN-140)SP-56 of the Office of 27 October 2021. Available at:< https://www.lygybe.lt/data/public/uploads/2021/10/21sn-140sp-56.pdf

72 Decision No. (20)SN-148)SP-84 of the Office of 28 October 2020. Available at:< https://www.lygybe.lt/data/public/uploads/2020/11/20sn-148sp-84-.pdf

73 Decision No. (19)SN-41)SP-38 of the Office of 21 April 2019. Available at:< https://www.lygybe.lt/data/public/uploads/2020/04/sprendimas-20-38.pdf

74 Decision No. (19)SN-35)SP-36 of the Office of 12 March 2019. Available at:< https://www.lygybe.lt/data/public/uploads/2019/03/19sn-35sp-36.pdf

75 Decision No. (16)SN-179)SP-129 of the Office of 17 November 2016. Available at:< https://www.lygybe.lt/data/public/uploads/2016/11/pazyma-tamosiuno-129.pdf

76 Decision No. (21)SN-119)SP-33 of the Office of 29 July 2021. Available at:< https://www.lygybe.lt/data/public/uploads/2020/02/sprendimas-nr.-19sn-9sp-33.pdf

77 Decision No. (20)SN-148)SP-84 of the Office of 28 October 2020. Available at:< https://www.lygybe.lt/data/public/uploads/2020/11/20sn-148sp-84-.pdf

78 Decision No. (19)SN-41)SP-38 of the Office of 21 April 2019. Available at:< https://www.lygybe.lt/data/public/uploads/2020/04/sprendimas-20-38.pdf

79 Decision No. (20)SN-148)SP-84 of the Office of 28 October 2020. Available at:< https://www.lygybe.lt/data/public/uploads/2020/11/20sn-148sp-84-.pdf

80 Decision No. (19)SN-213)SP-10 of the Office of 3 February 2020. Available at:< https://www.lygybe.lt/data/public/uploads/2020/02/19sn-213sp-10.pdf

81 Decision No. (16)SN-179)SP-129 of the Office of 17 November 2016. Available at:< https://www.lygybe.lt/data/public/uploads/2016/11/pazyma-tamosiuno-129.pdf

82 Decision No. (19)SN-35)SP-36 of the Office of 12 March 2019. Available at:< https://www.lygybe.lt/data/public/uploads/2019/03/19sn-35sp-36.pdf

83 Decision No. (19)SN-9)SP-33 of the Office 1 March 2019. Available at:< https://www.lygybe.lt/data/public/uploads/2020/02/sprendimas-nr.-19sn-9sp-33.pdf.

84 Decision No. (21)SN-216)SP-3 of the Office of 8 February 2022. Available at:< https://lygybe.lt/data/public/uploads/2022/02/nr.-21sn-216sp-3.pdf.

85 *Rechnungshof v Österreichischer Rundfunk and Others* (C-465/00) and *Christa Neukomm v Österreichischer Rundfunk* (C-138/01) and *Joseph Lauermann v Österreichischer Rundfunk* (C-139/01) CJEU (2003, Joined Case No C-138/01,C-465/00,C-139/01).

86 Decision No. (21)SN-119)SP-33 of the Office of 29 July 2021. Available at:< https://www.lygybe.lt/data/public/uploads/2020/02/sprendimas-nr.-19sn-9sp-33.pdf

A similar situation exists in terms of knowledge of the Lithuanian language, which is frequently unreasonably required everywhere. Such a requirement unlawfully restricts the rejection of national minorities and foreigners and impedes free movement of persons. For example, the Office found that the company unlawfully refused to provide access to taxi services or employment services to the applicant with a self-service certificate because the latter allegedly lacked skills of Lithuanian language and was unable to communicate with the customers. The applicant stated that he had lived in Lithuania since 2014, so he was familiar with the rules of passenger transportation and spoke Lithuanian well. Therefore, the applicant believed that he had faced discrimination based on his origin, language and citizenship.[87] Accordingly, the employer could not make any assumptions about his level of language knowledge based on his surname.

In summary, employers discriminate against applicants and misuse personal data to find a suitable candidate for a position by drawing unjustified conclusions about a candidate based on certain data. Therefore, an option to submit additional data should be provided.

CONCLUSIONS

The decision on the specific documents to be submitted for employment in Lithuania depends on the employer's discretion. However, the applicants are still required to provide excessive data in the Template of Employment Contract.

Data on candidates or job applicants can be collected using various methods through several stages, including application forms, interviews, social networks, interviews with former employers, etc. The primary data is collected by filling in an application form. Later, data may be collected during the interview based on the submitted questionnaire; meanwhile, during the final selection stage, the selected candidates may be asked for additional information (e.g. about their health) or clarification of existing information (e.g. obtained from social networks, former employers and other sources).

Any information related to a specific natural person shall be considered personal data; therefore, before collecting it, an employer must complete a specific task – not to cross the boundaries of data collection for purposes other than those intended. In other words, personal data may only be collected for recruitment purposes, some of which are provided for by law, only on reasonable grounds and without discrimination against family status, gender, age or other factors.

The investigation of complaints conducted by the Office of the Equal Opportunities Ombudsperson in Lithuania revealed that a personal identification number, which also shows a person's gender and age, may have an impact on successful employment; meanwhile, name and surname may lead to assumptions about the applicant's knowledge of the Lithuanian language; and that employers unlawfully prevent applicants from getting a job and discriminate against them by finding out their gender, age, nationality or citizenship, family or social status, sexual orientation and other factors.

The legislator should regulate the limits of the use of artificial intelligence for the selection of employees, associated with the protection of personal data and non-discrimination of individuals.

[87] Decision No. (18)SN-129)SP-77 of the Office of 10 August 2018. Available at:< https://lygybe.lt/data/public/uploads/2018/08/sprendimas-nr.-77.pdf

BIBLIOGRAPHY

1. Befort, Stephen F. "Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place." *Hofstra Labour and Employment Law Journal* Vol. 14, No 2 (1997): 365–422.
2. Bidet, Alexandra, and Porta, Jerome. "Le travail à l'épreuve du numérique." *Revue droit du travail* 5 (2016): 328.
3. Byrnside, Ian. "Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants." *Vanderbilt Journal of Entertainment and Technology Law* 10:2 (2008): 445–477.
4. Finder, Alan. "For Some, Online Persona Undermines a Résumé." *The New York Times* (2006) // https://www.nytimes.com/2006/06/11/us/11recruit.html.
5. Grigonienė, Rasa. "Legal Regulation Ensuring the Protection of Personal Data of Employees: a Critical Analysis." *Jurisprudence* Vol. 27, No.2 (2020): 346–369.
6. Kinsey, Alan. "The Benefits of Pre-employment Screening," James M. Sweeney and Associates, Inc. Available at: http://www.sweeneyinc.com/files/benefits_pre-employment_screening.pdf (23 January 2022).
7. Leonaitė, Erika. "The Principle of Proportionality and its Application by the ECHR in Art. 8 Cases Against Lithuania." *Teisė* 77 (2010): 113–125.
8. Lukács, Adrienn. "Protection of Employees' Right to Privacy and Right to Data Protection on Social Network Sites – With Special Regard to France and Hungary", (University Paris 1 Panthéon Sorbonne and University of Szeged Doctoral (PhD) dissertation 2020).
9. Péano, M.-A. "L'intuitus personae dans le contrat de travail." *Droit social* 2(1995): 132–133.
10. Petraitytė, Ilona. "The Personal Data Protection Principles` (Vilniaus university Doctoral (PhD) dissertation 2013), p 186.
11. Sprague, Robert ."Invasion of the Social Networks: Blurring the Line Between Personal Life and the Employment Relationship." *University of Louisville Law Review* 50 (2011): 1.
12. Štareikė, Eglė, and Kausteklytė-Tunkevičienė, Sigita. "The main rights of the data subject and their enforcement in accordance with the EU General Data Protection Regulatio." *Public Security and Public Order 20* (2018);
13. Štareikė, Eglė. "Assurance of the Right to Privacy and the Protection of Personal Data in Labour Relations." *Public Security and Public Order* 26 (2021): 221-235.
14. Tamašauskaitė-Janickė, Gintarė. "The Usage of Information and Communication Technologies at the Workplace in the Context of Labour Law" (Vilniaus university Doctoral (PhD) dissertation 2016), pp 82–83.

LEGAL REFERNECES

1. *A. D. v. the State Data Protection Inspectorate.* Vilnius Regional Administrative Court, 2019, No. I-822-643.
2. *A. K. v. UAB „Transkedavė*". Kaunas Regional Court, 2010, No. 2A-1749-390.
3. Anchev v. Bulgaria App, ECHR, 2018, No. 38334/08 and 68242/16.
4. *College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer,* CJEU, 2009, C-553/07.
5. Constitution of the Republic of Lithuania. 1992, *Official Journal,* 33-1014.
6. *Criminal proceedings v. Bodil Lindqvist.* CJEU, 2003, No C-101/01.

7. *D. P. v. Radviliškis district municipality Radviliškis district municipality administration.* Panevėžys Regional Court, 2019, No. 2A-269-252.
8. *D. P. v. Kaunas Red Cross Clinical Hospital.* Supreme Administrative Court of Lithuania, 2011, No. A492 -2809.
9. Decision No. (16)SN-179)SP-129 of the Office of 17 November 2016. Available at: <https://www.lygybe.lt/data/public/uploads/2016/11/pazyma-tamosiuno-129.pdf
10. Decision No. (18)SN-129)SP-77 of the Office of 10 August 2018. Available at: <https://lygybe.lt/data/public/uploads/2018/08/sprendimas-nr.-77.pdf
11. Decision No. (19)SN-213)SP-10 of the Office of 3 February 2020. Available at: <https://www.lygybe.lt/data/public/uploads/2020/02/19sn-213sp-10.pdf
12. Decision No. (19)SN-35)SP-36 of the Office of 12 March 2019. Available at: <https://www.lygybe.lt/data/public/uploads/2019/03/19sn-35sp-36.pdf
13. Decision No. (19)SN-41)SP-38 of the Office of 21 April 2019. Available at: <https://www.lygybe.lt/data/public/uploads/2020/04/sprendimas-20-38.pdf
14. Decision No. (19)SN-9)SP-33 of the Office 1 March 2019. Available at:<https://www.lygybe.lt/data/public/uploads/2020/02/sprendimas-nr.-19sn-9sp-33.pdf.
15. Decision No. (20)SN-148)SP-84 of the Office of 28 October 2020. Available at: <https://www.lygybe.lt/data/public/uploads/2020/11/20sn-148sp-84-.pdf
16. Decision No. (21)SN-119)SP-33 of the Office of 29 July 2021. Available at: <https://www.lygybe.lt/data/public/uploads/2020/02/sprendimas-nr.-19sn-9sp-33.pdf
17. Decision No. (21)SN-140) SP-56 of the Office of 27 October 2021. Available at: <https://www.lygybe.lt/data/public/uploads/2021/10/21sn-140sp-56.pdf> (accessed 20 May 2022).
18. Decision No. (21)SN-140)SP-56 of the Office of 27 October 2021. Available at: <https://www.lygybe.lt/data/public/uploads/2021/10/21sn-140sp-56.pdf
19. Decision No. (21)SN-216)SP-3 of the Office of 8 February 2022. Available at: <https://lygybe.lt/data/public/uploads/2022/02/nr.-21sn-216sp-3.pdf.
20. *GC and Others v Commission nationale de l'informatique et des libertés (CNIL).* CJEU, 2019, No C-136/17.
21. Law of the Republic of Lithuania amending Law on Enterprises and Facilities of Strategic Importance for National Security and Other Undertakings Important for National Security No. IX-1132. 2018, *TAR*, 1004.
22. Law on the Legal Protection of Personal Data of the Republic of Lithuania amending Law No. I-1374 (2018) *TAR*, 117 33.
23. Law on the Spelling of a Person's Name and Surname in Documents of the Republic of Lithuania. Register of Legal Acts. 2022, *TAR*, 1142.
24. Opinion 2/2017 on data processing at work, 10, State Data Protection Inspectorate of the Republic of Lithuania, available at: https://vdai.lrv.lt/uploads/vdai/documents/files/Nuomonedelduomenutvarkymodrabe20170608wp249lt(2).pdf.
25. Order No. A1-343 of the Minister of Social Security and Labour of the Republic of Lithuania of 29 June 2017 "On Approval of Template of the Employment Contract". Register of Legal Acts. 2017, *TAR*, 11167.
26. *Rechnungshof v Österreichischer Rundfunk and Others* (C-465/00) and *Christa Neukomm v Österreichischer Rundfunk* (C-138/01) and *Joseph Lauermann v Österreichischer Rundfunk* (C-139/01). CJEU, 2003 Joined Case No C-138/01, C-465/00, C-139/01.

27. Recommendation CM/Rec(2015)5 of the Committee of Ministers to member States on the processing of personal data in the context of employment, 5. p., CE. *Adopted by the Committee of Ministers on 1 April 2015, at the 1224th meeting of the Ministers' Deputies*.
28. 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. OL L 119, 2016 5 4, p. 1—88.
29. Republic of Lithuania Amending the Law on Courts. 1994, *Official Journal,* 46–851.
30. Republic of Lithuania Labour Code. 2016, *TAR,* 23709.
31. Republic of Lithuania Law on Bailiffs. 2002, *Official Journal,* 53-2042.
32. Republic of Lithuania Law on Elections to Municipal Councils. 1994, *Official Journal,* 53-996.
33. Republic of Lithuania Law on Equal Opportunities for Women and Men. 2016, *TAR*, 26966.
34. Republic of Lithuania Law on Equal Treatment. 2003, *Official Journal*, 114-5115.
35. Republic of Lithuania Law on Fundamentals of Protection of the Rights of the Child. 1996, *Official Journal*, 33-807.
36. Republic of Lithuania Law on Prevention of Corruption. 2021, *TAR*, No. 15850.
37. Republic of Lithuania Law on Safety and Health at Work. 2003, *Official Journal*, 70-3170.
38. Republic of Lithuania Law on State Secrets and Official Secrets. 1999, *Official Journal*, 105-3019.
39. Republic of Lithuania Law on the Civil Service. 1999, *Official Journal*, 66–2130.
40. Republic of Lithuania Law on the Notarial Profession. 1992, *Lietuvos aidas*, 192-0.
41. Republic of Lithuania Law on the Prevention and Control of Communicable Diseases in Humans. 1996, *Official Journal,* 104-2363.
42. Resolution No. 496 of the Government of the Republic of Lithuania "On the Implementation of the Labour Code of the Republic of Lithuania." 2017, *TAR*, 10853.
43. Ruling of the Constitutional Court of the Republic of Lithuania of 21 October 1999 on the compliance of the Resolution of the Supreme Council of the Republic of Lithuania "On Writing Names and Family Names in Passports of Citizens of the Republic of Lithuania" of 31 January 1991 with the Constitution of the Republic of Lithuania, 1999.
44. *UAB „Init" v the State Data Protection Inspectorate.* Supreme Administrative Court of Lithuania, 2013, No. A822-1173-2013.