INTERNATIONAL
HELLENIC
UNIVERSITY

Data protection issues of employee monitoring

Serasidis Ioannis

UNIVERSITY CENTER OF INTERNATIONAL PROGRAMMES OF STUDIES
SCHOOL OF HUMANITIES, SOCIAL SCIENCES AND ECONOMICS

A thesis submitted for the degree of
LLM in Transnational and European Commercial Law, Banking Law, Arbitration/Mediation

February 2022
Thessaloniki – Greece

Student Name: Ioannis Serasidis

SID: 1104200024

Supervisor: Prof. Komnios Komninos

I hereby declare that the work submitted is mine and that where I have made use of another's work, I have attributed the source(s) according to the Regulations set in the Student's Handbook.

February 2022
Thessaloniki - Greece

Abstract

This dissertation was written as part of the LLM in Transnational and European Commercial Law, Banking Law, Arbitration/Mediation at the International Hellenic University. The radical technological progress has given employers the opportunity to use a wide variety of monitoring methods. Aim of this thesis is to demonstrate the legal framework surrounding the protection of employees' rights from the monitoring from employers and analyse the balancing between employers' legitimate interests and employees' rights.

The first Chapter is an introduction to the topic. The second Chapter describes the legal framework surrounding the protection of the rights to data protection and privacy. The third chapter specifically regards the General Data Protection Regulation and how this regulation applies in the context of employment relationships, while the fourth Chapter analyses methods of monitoring used by employers and specifically video surveillance, access to electronic devices and communications, social media monitoring, Global Pointing Systems and Biometric methods. Finally, the last Chapter draws a conclusion to the study.

I would like to thank my supervisor, Mr. Komninos Komnios, for his valuable guidance and support during the writing of this dissertation and throughout my studies at the International Hellenic University, as well as my family and friends for their relentless support.

Keywords: General Data Protection Regulation, Right to data protection, Privacy, Employee Monitoring, Data processing

Ioannis Serasidis
February 2022

Contents

Introduction

The present study is focused on the personal data protection of employees and particularly attempts to highlight the issues arising from the monitoring of employees' personal data by their employers. It is undeniable that employers have been traditionally the stronger part in a labour contract compared to their employees. Actually, the issue whether an employee is dependent to his/her employer is used by scholars in legal theory as the main criterion to determine whether a working relationship is indeed a labour contract, in which Labour Law applies, or another relative type of contract, which might be dictated by another sector of Law (e.g., a contract for the supply of services is dictated by Civil Law)[1]. This criterion was defined by German legal scholars as the criterion of "personal dependence" due to the fact that the influence an employer has on an employee by exercising his/her managerial prerogative is not restricted to a professional level, but it also exceeds to the personal sphere of the employee. Even though this dependence criterion is established as "legal", instead of "personal", in the French legal theory, it actually sets the same requirements in order to apply. More specifically, a working relationship is considered as employment when someone is obliged to: a) provide his/her services at a time and place set by the other party, b) follow instructions regarding the way the service is provided and accept to be supervised, c) provide services within an organized framework managed by the employer and d) provide his/her services in person[2].

Taking into consideration the above mentioned, an employee is by definition dependent to his/her employer, thus in most cases clearly in a weaker position with less bargaining power. This fact is noticeable in pretty much every single aspect of the labour relationship with the issue of data collection and processing, making no exception. Actually, employers are the only contracting party in a labour relationship that collect and process personal data of the other party, i.e., employees, and there are many instances where the collection of employees' data is mandatory by law in order to ensure that the labour relationship is functional and lawful (for instance data that are necessary to complete social security and tax obligations)[3]. Even before the beginning of a labour relationship an employee is forced at a pre-contractual phase to disclose personal information to the potential employer as, for instance, the job application is followed by a CV, which includes a wide variety of personal data vital in order for employer to hire the most suitable candidate. In addition to the previous, the employer has also the opportunity to dig deeper into an employees' private sphere during the job interview. Afterwards, when the labour contract is already completed and functioning, the employer continues to have access to employees' personal data or take further cognizance while exercising his/her managerial prerogative to safeguard his/her interests (for example invigilate whether the working schedule is followed, assess

[1] Zerdelis, Εργατικό Δίκαιο, Ατομικές Εργασιακές Σχέσεις (Labour Law, Individual Employment Relationships), 2014, p. 6

[2] ibid p. 7, 8

[3] Douka, Προσωπικά δεδομένα και εργασιακές σχέσεις: προστασία σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων (Personal Data and Employment Relationships: protection according to General Data Protection Regulation), 2018, p. 645

employees' productivity etc.) or even to serve employees' rights[4] (for instance grant leave of absence or pay salaries etc.). Last but not least, there are cases in which employers still process personal data of former employees, when for example the labour contract includes a confidentiality or non-compete clause.

It has already been said that employers collect and process a vast amount of their employees' personal data, but an issue that needs to be further discussed is how this data come into employers' knowledge. First of all, an employee might directly divulge personal information to the employer voluntarily, for example, as mentioned previously, by sending a CV when applying for a job. However, it is of common knowledge that many times employers actually collect personal data by monitoring employees[5], while in many instances they do not even know that they are being monitored[6]. The monitoring of employees has always been existent in labour relationship via the physical presence of a supervisor or even the employer himself/herself, whose presence safeguards the efficient and coordinated working environment. Nevertheless, nowadays the breakthroughs in the sector of technology provoked swift changes to the landscape of employee monitoring, providing employers with several cheaper, less time-consuming, and simpler means than the traditional monitoring[7], which actually enable a much more intrusive interference to employees' personal sphere (e.g., video surveillance systems, Global Positioning System, biometric finger scanning systems etc.). Except for the previous, this digital revolution, which has started since the 90s, also led to a transformation to the traditional way of working and created new types of working, which were promoted by EU as, on the one hand, they were beneficial for the enterprises by offering flexibility, reduction of expenses and enhanced competitiveness in the market, while on the other hand they also introduced benefits for employees, offering more flexible working schedules and reducing unemployment rates[8]. One of these transformations was the growth of tele-working into an efficient, productive and common way of providing work. Especially in today's era, the outburst of the Covid-19 pandemic has led to a massive increase in the number of employees working remotely, as the current emergency situation demands social distancing and avoiding crowd gathering in workplace. Notwithstanding the aforementioned benefits for both employers and employees, working from home poses many risks regarding the protection of employees' personal data and privacy. In fact, working from home makes the limits between personal and working life blurry, allowing the employer to monitor employees' behavior and habits completely irrelevant to work issues.

According to the previously mentioned, it is clear that employers collect personal data of their employees by monitoring their activity either offline or online. These data,

---

[4] Liksouriotis, Ατομικές εργασιακές σχέσεις (Individual Employment Relationships), 2017 p. 586

[5] Kizza, Ethical and Social Issues in the Information Age, 2017, p. 154

[6] In fact, as it will be later discussed, their knowledge, or even consensus would not be considered in most of the cases a lawful ground for the collection and processing of personal data, according to articles 6 and 7 of the GDPR.

[7] Michos, Η επιτήρηση των τηλεπικοινωνιών μέσω ίντερνετ στον χώρο εργασίας (The monitoring of telecommunications via Internet in the workplace), 2007, p. 13

[8] Malgardi, Νέες τεχνολογίες, προσωπικά δεδομένα και εργατικό δίκαιο (New technologies, personal data and labour law), 2010, p. 9

with the assistance of new technologies, can be stored and processed with ease at an ample amount, enabling employers to use them whenever they wish, individually or combined, even if the purpose of their processing is totally different from the one they had initially been collected[9]. This practice, which actually is incompatible with the finality principle, is often utilized by employers in order not only to assess the quality and quantity of work that the employee provides, but further to evaluate the personality of the employee[10]. Under these circumstances, employees often act in a way not representative of their character and follow a pattern of behavior that is supposedly more likeable to their employers, knowing or suspecting that they are being monitored even unlawfully and resulting into psychological distress and anxiety[11].

Yet one should acknowledge that there are instances where the monitoring of employees is required so as the rights of employers to be protected, such as the legitimate interest to construct an enterprise in the most efficient possible way in order to achieve its productivity goal, translated into economic benefits[12]. Hence, the legal framework surrounding the processing of employees' personal data via monitoring by their employers should be primarily oriented around the protection of employees from unlawful processing of their data, since employees are in a weakened factual and contractual position in comparison to employers, but should also be flexible enough in order to allow the appropriate balance with employers rights and legitimate interests.

[9] Simitis, Reconsidering the Premises of Labour Law: Prolegomena to an EU Regulation on the Protection of Employees 'Personal Data, 1999, p 56

[10] Crysogonos, Vlachopoulos, Ατομικά και Κοινωνικά Δικαιώματα (Individual and Social Rights), 2017, p. 49

[11] ibid 10, p. 59

[12] Ladas, Το δικαίωμα της προσωπικότητας του εργαζομένου (The personality right of employee), p. 264

The Legal Framework surrounding the protection of employees from employer monitoring

The distinction between right privacy and right to data protection

The unlawful employee monitoring by employers infringes both the right to privacy and the right to data protection, which could be used as legal basis to employees' legal actions in such case. These two rights are related to each other, however they are not identical, as there are cases in which only one of the two is violated.

The concept of privacy, which is, in fact, by far the older of the two, exists since the ancient human societies, nevertheless it was not actually recognized as a human right until the late 19th century. The trigger of the legal conceptualization of privacy as a human right was the well-known article of Warren and Brandeis with the title "The Right to Privacy", which was published back in 1980 to the Harvard Law Review, defining privacy as "the right to be let alone"[13]. Despite the fact that over a century has passed and a multitude of scholars attempted to define privacy, to this date there is not a generally accepted definition of privacy[14]. Among others, the notion of privacy has been described as "the withholding or concealment of information", "the claim of an individual to determine what information about himself or herself should be known to others", "the control we have over information about ourselves" and "the right of the individual to decide about himself/herself"[15], yet the task of a universally accepted context around privacy remains incomplete. In fact, big part of the American legal theory considers privacy being extremely vague and conceptually inadequate, based on contradictions[16]. Moreover, privacy is often accused in American fora for being old-fashioned and outdated, also creating obstacles to other urgent issues, such as national security and promotion of entrepreneurship[17]. Probably this is the reason that in particular regarding employees' privacy the majority of the legal scholars in the U.S.A. support the opinion that employees do not have a legitimate expectation of privacy in the workplace since providing work is not a private matter[18].

Nonetheless, the truth is that privacy is actually an important modern era issue, even concerning employment relationships[19], taking into consideration factors like the progress in the technological sector, the extent use of social media in everyday life and

---

[13] Warren and Brandeis, The Right to Privacy, 1890, p. 193, [https://www.jstor.org/stable/1321160seq=1#metadata_info_tab_contents], accessed 13 October 2021

[14] Adrienn Lukacs, To post or not to post-that is the question: Employee monitoring and employees' right to data protection, 2017, p. 190, [https://heinonline.org/HOL/Page?collection=journals&handle=hein.journals/mujlt11&id=188&men_tab=srchresults], access 15 October 2021

[15] ibid

[16] Julie Cohen, Turning Privacy Inside Out, 2019, p. 3, [https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3162178], accessed 12 November 2021

[17] Julie Cohen, What Privacy Is For, 2013, p. 1906, [https://cdn.harvardlawreview.org/wp-content/uploads/pdfs/vol126_cohen.pdf], accessed 12 November 2021

[18] Mitrou, Ιδιωτικότητα, προσωπικά δεδομένα και εργασιακές σχέσεις (Privacy, personal data and employment relationships), 2017, p. 140

[19] see below Halford v UK and Barbulescu v Romania cases, p. 29

the raise of tele working, and, in spite of the previous arguments, privacy has been recognized as a fundamental right and has been mentioned by many international legal documents. For example, according to article 12 of the Universal Declaration of Human Rights (U.N., 1948) "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks"[20]. Article 17 of the International Covenant on Civil and Political Rights (U.N., 1966) states that "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation"[21], while according to Article 8 of European Convention of Human Rights (Council of Europe, 1950) "Everyone has the right to respect for his private and family life, his home and his correspondence"[22].

On the other hand, the right to data protection is a younger legal concept. An indication that safely leads towards this conclusion is the fact that the right to data protection appeared in international documents later than the right to privacy. Examples of such documents are the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (September, 1980)[23], the Convention for the Protection of Individuals with Regard to Automatic Processing of personal Data[24] (Council of Europe, 1981) and the Guidelines for the Regulation of Computerized Personal Data file (U.N., 1990). Even though the right to data protection is closely related to privacy, it has a different scope and formulation.

The right to Data Protection applies when personal data are processed, regardless of the kind of data that are processed and the kind of the processing itself. Thus, there are instances in which data processing has zero impact to the data subject's privacy since the processed data are completely irrelevant to privacy in general. Taking into consideration an example from the employee monitoring context, on the one hand the unlawful video surveillance of employees in a workplace infringes both the right to data protection and privacy, however on the other hand the recording of data by an employer regarding the names and remuneration paid to an employee is not harmful towards the employee's private life.

Moreover, the distinction between these rights is visible in international documents that have separate provisions and articles for each of them. For example, the Charter of Fundamental rights of the EU acknowledges both rights, providing different articles for each one. More specifically, according to article 7 "Everyone has the right to respect for his or her private and family life, home and communications", while according to article 8 "Everyone has the right to the protection of personal data concerning him or her"[25]. In conclusion, even though the right to privacy and the right to data protection are related, they actually are two distinct fundamental human rights

[20] Access at https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf
[21] Access at https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx
[22] Access at https://www.echr.coe.int/documents/convention_eng.pdf
[23] https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm. They were revised in 2013.
[24] Access at https://rm.coe.int/1680078b37
[25] Access at https://fra.europa.eu/en/eu-charter/article/7-respect-private-and-family-life regarding right to privacy and https://fra.europa.eu/en/eu-charter/article/8-protection-personal-data regarding data protection.

with different scope and formulation, that may often, and not always, be infringed at the same time.

The sources of protection

The protection of employees against unlawful data processing in general, but also in concreto against monitoring from employers, is achieved, as mentioned above, with the acknowledgment and safeguard of the right to privacy and data protection. Before proceeding forward, it would be meaningful to briefly summarize the different legal sources of protection.

International Legal Documents

As it has already been said, there are several international legal documents dedicated to the protection of the right to privacy and the right to data protection. Legal documents, which are binding for the contracting States, like the aforementioned Convention for the Protection of Individuals with Regard to Automatic Processing of personal Data[26] regarding data protection, and Article 8 of the European Convention of Human Rights) regarding privacy, have played decisive role in the protection of employees, even though there is not a direct reference to the application of them during the performance of a labour contract. This conclusion has its origin to jurisprudence, especially of the European Court of Human Rights (*EctHR)*, based in Strasbourg. Article 8 of ECHR, in specific, has become subject of discussion in several important judgments of the Strasbourg Court, which clarified the way article 8 should be interpreted. Such court decisions, like the ones on the cases Barbulescu v. Romania, Halford v. UK and Amann v. Switzerland[27], played a decisive role in the acknowledgement of the right privacy in workplace, expanding the content of the notion of private life in employment relationships and enhancing the protection of employees' personal data.

Beside the existence of binding rules, a lending hand to the shielding of the right to privacy and data protection of employees (and data subjects in general) is offered by non-binding legal texts. Binding rules often leave regulatory ambiguities or even gaps, which cannot be covered by the existing legal framework. Under these circumstances, in many cases, legal initiatives with no mandatory character may be used as guides pointing out the need of legislative act or providing with instructions regarding the application and interpretation of legislative acts. As an example of an international non-binding legal document relative to the protection of employees' right to data protection, one could mention the Recommendation No. R (89) 2 of the Committee of Ministers to Member States of the Council of Europe on the Protection of Personal Data used for Employment Purposes[28].

Legislative acts of the EU

On a European Union level, as already mentioned previously, both the right to privacy and the right to data protection are protected by the Charter of Fundamental rights of

[26] In fact, this is the only legally binding international (non-EU) instrument regarding data protection.

[27] Access at https://hudoc.echr.coe.int/eng?i=001-58497

[28] Access at https://www.coe.int/t/dg3/healthbioethic/texts_and_documents/Rec(89)2E.pdf

the EU, on article 7 and 8 respectively. Furthermore, the issue of data protection is also mentioned on article 16 of the Treaty for the Functioning of the EU (ex-article 286 TEC). According to the first paragraph "Everyone has the right to the protection of personal data concerning them", while on the second paragraph TFEU sets the regulatory framework concerning the legislative procedure[29]. Moving a step forward towards achieving the goal of a unanimous legal framework among Member States in order to facilitate free flow of data, while the data subjects are also protected from unlawful processing, as set in the preamble, the European Parliament and the Council put into effect the Directive 95/46/EC of 24 October 1995 "on the protection of individuals with regard to the processing of personal data and on the free movement of such data"[30]. The Directive was in effect for more than two decades and played a big role to the configuration of the legal framework around data protection not only among the EU Member States, but also to non-Member States[31]. However, it was eventually repealed by the General Data Protection Regulation and one of the main reasons was its failure to prevent fragmentation in the implementation of data protection across the Union, leading into obstacles to the free flow of data due to the differences in implementation and application of the Directive from State to State[32].

Regulation 2016/679 of the European Parliament and of the Council on "the protection of natural persons with regard to the processing of personal data and on the free movement of such data"[33], also known as GDPR, was voted on 27 of April 2016 and started being applying on 18 May 2018. The GDPR actually maintained the goals and principles of the Data Protection Directive[34], adding some new rights for natural persons, obligations for enterprises and sanctions against those violating the provisions of the regulation. In fact, the GDPR has evolved into the main weapon supporting data subjects from unlawful processing of personal data not only in Europe, since GDPR has an extra-territorial effect. According to article 3, the GDPR provisions also apply to data controllers and processors established outside EU, provided that they are offering goods or services to individuals in the EU, or they are monitoring their behaviour. This second requirement is really important for the protection of personal data of employees working to multinational enterprises registered outside EU, which will need to obey to both their national law and the GDPR[35]. Regarding data protection of employees, the GDPR does not provide any specific provisions, making just brief references (e.g., article 9, 88). Nevertheless, it is a regulation that is of general application, consequently it could

[29] Access at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN

[30] Access at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=el

[31] Igglezakis, Ο Γενικός Κανονισμός προστασίας Προσωπικών Δεδομένων - Εισαγωγή στο νέο νομικό πλαίσιο προστασίας προσωπικών δεδομένων (The General Data Protection Regulation-Introduction to the new legal framework of personal data protection, 2018, p. 15

[32] Rectial 9 of GDPR

[33] Access at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e2001-1-1

[34] Recital 9

[35] Tikkinen-Piri, Rohunen, Markkula, EU General Data Protection Regulation: Changes and implications for personal data collecting companies, 2018, p. 135 [https://www.sciencedirect.com/science/article/abs/pii/S0267364917301966], accessed 8 September 2021

be used in order to safeguard employees' rights from monitoring by employers. Given that the GDPR is the main legislative act regarding data protection within the EU Member States, the next chapter is dedicated on the analysis of its provisions and how they can be adapted so as to protect employers from unlawful monitoring.

National legislation

Last but not least, every sovereign state has the power to enact its own general or specific rules, following the constitutionally established legislative procedure. Regarding the data protection of employees, most of the countries omit to mention any specific provision. For instance, France constitution does not make any specific reference on this kind of employees' rights and depends their protection on other national, international and EU legislative acts and jurisprudence of Courts[36], while US constitution fails to mention privacy and data protection in abstracto. In order for a state to sufficiently protect employees from unlawful data processing from employers, it is vital that data protection law efficiently interacts with labour law, since only one of them solely cannot provide employees with full protection[37]. In Italy, the start had already been made with the Statuto Dei lavoratori in 1970[38], while another example of an early try to solve employees' data protection issue was the Act no. 78-17 of January 6, 1978, on Information Technology, Data files and Civil Liberties, followed later by Act no. 92-1446 of December 31,1992, which was specified on employee's rights, unlike the former act, which was general[39].

Having already made a reference to the GDPR, it is interesting to notice that even though GDPR is a Regulation, which unlike directives, is strict and binding, it actually gives EU Member States the flexibility, on many occasions, to regulate some more specific issues at will. This divergence to the rigid character of Regulations is the reason that often enough the GDPR is called a "DiRegulation", since it is considered as a hybrid between a directive and a regulation[40]. As a quite characteristic example, one could mention the provision of article 88, which is relative to the protection of employees. According to this article, national laws or collective agreements could regulate more specific issues that were not included in the provisions of GDPR, in order to safeguard employees' data. Furthermore, another example is article 80 which could also be utilized for the protection of employees. Based on this article, Member States have the freedom to assign a non-for-profit body, organization or association, lawfully constituted, to lodge complaints, exercise the rights of articles 77,78 and 79 and receive compensation on behalf of the data subjects. Such an organization could without a doubt be a Union

[36] Pogace, Employees' Data Protection in the Workplace and its Legal Implications, A Comparative Overview of EU's Legal Framework, 2016, p. 2, [https://heinonline.org/HOL/Page?handle=hein.journals/iihcj10&collection=journals&id=63&startid=&endid=72], accessed 15 October 2021

[37] Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, page 4

[38] Simitis, 1999, p. 45

[39] Pogace, 2016, p. 3

[40] Lempesi, Γενικός Ευρωπαϊκός Κανονισμός για την προστασία των προσωπικών δεδομένων 679/2016/ΕΕ- Κατάργηση της Οδηγίας 95/46/ΕΚ – Συγκριτική μελέτη (General European Regulation for the protection of personal data 679/2016/EU-Repeal of Directive 95/46/EC – Comparison study, 2017, p. 498

Body that serves employees' rights. Thus, even though GDPR is a regulation, the participation of national implementing laws is vital to the formation of the legal framework surrounding the protection of personal data.

Employee Protection under the General Data Protection Regulation

As mentioned previously, the GDPR is a vital legal instrument for the protection of personal data. Despite the fact that its provisions do not set explicitly a legal framework for the protection of employees, the fact that the GDPR is of general application means that personal data in the employment context are also protected.

Definitions

Before proceeding to a more in-depth analysis of the way employees' data are protected by the GDPR, it is important first, for the better understanding of its provisions, to explain some key definitions.

First of all, speaking of personal data protection, it is important to define the notion of personal data itself. According to article 4 paragraph 1 of 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"*. In other words, personal data could literally constitute any information regarding a natural person that could lead to the identification of that person, indinidually or along with other information. Thus, information about employees that every single employer collects throughout an employment relationship (e.g., name, social security number, phone number, photographs, e-mails etc.) are considered "personal data" and fall under the protection of the GDPR. Actually, employers have also knowledge of employees' information that are considered "special categories of personal data". According to article 9 of the GDPR such special categories of data are *"data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation"*. These types of data, also called "sensitive", are so closely related to the privacy of the data subject, that there is the need for further protection.

The aforementioned article also includes the definition of the "data subject", who is the natural person identified or identifiable by a set of information ("personal data"). In the frame of a labour relationship, one who provides work is considered an employee concerning Labour Law and a data subject according to the GDPR. Consequently, an employee enjoys a combined protection from the two different sectors of law, as already mentioned[41]. Moreover, the notion of employer should not be restrictively interpreted. This means that the combined data protection offered by the GDPR along with labour law should not be restricted only to the employers with an active labour contract, but also cover prospective and former employees, since their data are collected by employers as well. Furthermore, according to opinion 2/2017 on

[41] Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, p. 4

data processing at work of the article 29 Data Protection Working Party, the notion of employees also includes not only the traditional employment contracts, but also new types of labour relationships, like employment on a freelance basis[42]. Last but not least, it is interesting to notice that the word employee also includes public servants. As the ECtHR ruled on the Buivids Case[43], which was about the video recording of a police officer. The police officers cannot be excluded from the protection of their data just because they are performing their duties and moreover, the Directive 95/46, which applied then, did not contain any provision excluding public officials from its scope[44], something that also stands for the GDPR.

According to article 4 of the GDPR, " *'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data"*. As mentioned above regarding employees, in the context of an employment relationship, employers have also a double role. From the one side they are "employers", having the rights and obligations that Labour Law dictates, while on the other side they operate as data controllers. What was mentioned before regarding the interpretation notion of employee, applies equally regarding the notion of employer. In other words, the potential or former employers are considered as data controllers[45], as well as public authorities, agencies or other bodies. In accordance with the same article, *"'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"*. This distinction serves the allocation of responsibility, in regard to data processing, to those who actually control the purpose and means of processing and those who just act on behalf of them[46]. In fact, in the relationship between data controller and data processor the provisions of vicarious agent liability could apply[47]. Examples of data processors that process employees' data on behalf of employers are book-keeping offices, companies occupied with the security of workplaces, companies undertaking the payment of salaries, etc.

Having cited the definitions of the main participants to a processing procedure, it is time to define what exactly the "processing of data" is. The GDPR defines processing as *"any operation or set of operations which is performed on personal data or on sets of personal data, either by automated means or not, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"*. It is obvious that the definition is rather broad and the list of examples is non-restrictive, providing a field for the protection against a wide variety of data controllers' actions. Interpreting the definition according to the context of the current study, monitoring of employees by their

[42] Article 29 Data Protection Working Party, Opinion 2/2017 on data processing at work, p. 4
[43] Access at https://curia.europa.eu/juris/document/document.jsf?docid=210766&doclang=EN
[44] Ibid, paragraphs 44,45
[45] Ibid
[46] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and processor", page 5
[47] Koukiadis, Εργατικό Δίκαιο: ατομικές εργασιακές σχέσεις και το δίκαιο της ευελιξίας της εργασίας (Labour Law: individual employment relationships and the law of the flexibility of work), 2017, p. 51

employers constitutes processing of data, as a way of collecting and recording employees' data. Hence, employees unlawfully monitored, irrespective of the form of the monitoring, are protected by the GDPR provisions. In addition, article 4 also includes a definition of "personal data breach" according to which *" 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed"*.

Principles

Besides the detailed list of definitions given by article 4, the GDPR also includes an article dedicated to the principles that data processing should follow. Hence, the principles laying on article 5 also bind employer monitoring, as a form of processing. These principles are the following:

Lawfulness, fairness and transparency

According to GDPR [article 5(a)] *"personal data shall be lawfully, fairly and in a transparent manner in relation to the data subject"*. A reference regarding this principle is also found on paragraph Recital 39 of the GDPR. According to it, an aspect of this principle is the access of the data subject to any information concerning the processing in a concrete manner. This applies in particular to information in regard to the identity of the data controller, the purposes (which should be legitimate and explicit at the time of collecting) and risks of the processing, the rights of the data subject, the storage of data and its duration. As examples in the context of employment relationships, one could mention the a priori briefing of employees by the employers and the in abstracto transparency and legitimacy regarding the processing of employees' data collected according to the provisions of article 13 and 14 of GDPR[48].

Purpose limitation

As article 5 par. 1 (b) of the GDPR dictates *"personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes"*. As mentioned above, the purposes of the data processing should be a priori communicated to the data subject and be legitimate. As a result, the use of personal data for different purposes from those that they were initially collected for is illegitimate, exempt from the exceptions set at article 23 of the GDPR. Concerning the legitimacy of the purpose, it is heavily dependent on the requirements set by the provisions of article 6 of GDPR, under the title "lawfulness of processing"[49] (and article 9 regarding special categories of data). For instance, an employer may lawfully collect information regarding the participation of an employee to trade union acts, which is actually considered as data of special category under article 9, in order to grant a special purpose leave of absence to the employee so as to exercise his/her

[48] Donos, Mitrou, Middleton, Papakonstantinou, Η αρχή προστασίας των προσωπικών δεδομένων και η επαύξηση της προστασίας των δικαιωμάτων (The principle of protection of personal data and the increase of the right protection, 2002, p. 218

[49] See below, chapter "The Lawfulness of the Processing", p. 16

collective rights[50]. However further usage of these data, in order for example to assess the compatibility of the union activity and the enterprises' interests and afterwards create a profile regarding the employee, is unlawful.

Data Minimisation

Under article 5 par. 1 (c) the processed personal data shall be *"adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed"*. This principle is in fact a more specific aspect of the proportionality principle. From the perspective of an employee, his/her data are being collected and processed, as already mentioned, on a pre contractual basis, during the performance of the labour contract and also after the end of the labour relationship. The data minimisation principle shall apply to all the aforementioned stages. During the interview or generally the examination of CVs regarding the hiring of an employee, the data collected should be restricted only to the necessary information to judge whether a candidate is qualified or not. For instance, questioning or monitoring prospective employees concerning past violations of the law, is generally considered incompatible with this principle, however if the nature of the violation is closely related to the available job, collecting such data might be justified. Hence, it is justified for an employer to monitor whether or not a job applicant for a position of professional driver has been convicted for violation of traffic laws or for a position of cashier if the applicant has been convicted for embezzlement[51]. In cases though that such questions are unlawfully posed, employees have the right to deny answering, without this denial lawfully harming their chances to be hired, or even to exercise the so called "right to lie"[52] [53]. The aforementioned also apply regarding data related to health conditions. In conclusion, the personal data collected shall be limited up to the necessary extent and be appropriate in order to fulfill the purpose of the processing.

Accuracy

According to article 5 par. 1 (d) personal data shall be *"accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay"*. In other wards, in order to comply with this principle, employers, as data controllers, are obliged initially to collect personal data with accuracy and in case of any mistake, rectify or delete them. In addition to the previous, in case the data are modified, even if they were initially accurate, data controllers ought to keep them updated. This obligation actually allows employers to monitor employees and collect data that in other cases it would be unlawful to. For example, if an employer initially collected information of an employee with his/her consent that was later found incorrect or outdated, the monitoring by the employer would be legitimate in order to rectify them.

[50] Zerdelis, Συλλογικό Εργατικό Δίκαιο (Collective Labour Law), 2016, p. 76
[51] Zerdelis, 2014, p. 255
[52] Zerdelis, 2014, p. 258
[53] Simitis, 1999, p. 49

Storage limitation

Article 5 par. 1 (e) institutes the principle of storage limitation, according to which *"personal data shall 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject"*. The provisions of article 13 par. 2(a) and 14 par 2 (a), which are relevant to this principle, oblige the data controller to provide the data subject with information regarding the exact period of time that the data will be stored, and if not possible, the criteria used to define this period. An example related to this principle is the Directive 1/2011 of the Hellenic Data Protection Authority, according to which personal data collected via monitoring through video surveillance in private places where public has access, for example a store, which also happens to be a workplace, shall be deleted regularly at most 15 days after the recording, or ultimately 30 days, if a violation of law occurred against the controller and 3 months if the violation occurred against a third person.

Integrity and Confidentiality

According to article 5 par. 1 (f) personal data shall be *"processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures"*. An aspect of this principle is the provision of article 32, which mentions that, in order to protect natural persons from potential risks, both data controllers and processors shall implement appropriate measures, suggesting indicatively: *"a) the pseudonymisation*[54] *and encryption of personal data, b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services, c) the ability to restore the availability and access to personal data in timely manner in the event of a physical or technical incident and d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing"*. Furthermore, the provisions of articles 33 and 34 are related to the above mentioned, concerning the obligation of the data controller to inform the supervisory authority and the data subject regarding a potential personal data breach.

Accountability

Paragraph 2 of Article 5 introduces the accountability principle, according to which *"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1"*. An employer, such as every data controller, is forced not only to comply with the above principles of the GDPR, but also carries the burden to prove it. Therefore, employers need to keep track of the evidence proving the legitimacy of the processing, take the appropriate technical and organisational measures, like implementing data

[54] Recital 23 of the GDPR

protection policies or maintain documentation of processing activities, and keep those measures up to date.

Besides the principles included in Article 5 of the GDPR, article 29 WP had also set some principles that shall be followed during the processing of data in the frame of a labour contract in specific, with the Opinion 8/2001 on the processing of personal data in the employment context. These principles, which are actually relative to the one set by the GDPR, are: finality, transparency, legitimacy, proportionality, accuracy and retention of the data, security and awareness of the staff[55].

The Lawfulness of the Processing

After citing definitions and principles, the GDPR sets the requirements for the legitimate processing of personal data. According to the GDPR the processing of personal data is unlawful, unless there is a lawful basis allowing it. Looking at article 6 entitled "Lawfulness of processing" one could notice that paragraph 1 (a) mentions the consent of the data subject as justifying reason for the processing of data, while paragraphs 1 (b-f) are justifying reasons that do not require data subjects' consent in order to justify the processing. Employers, as data controllers, have to ground the processing (consequently the monitoring as well) of the employees' data on a lawful basis, otherwise the processing is unlawful. However, In the context of a labour relationship, the legal framework around the lawful basis of the processing is a little peculiar, especially when it comes to consent.

Consent as a lawful basis

In general

According to article 4 par. 11 of the GDPR "consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". As follows, in order for consent to be considered valid, article 4 sets some requirements, that need to be met.

First of all, consent must be "freely given". More specifically the data subject needs to have real choice and control while giving consent to data processing, otherwise the consent is invalid[56]. Furthermore, a decisive role regarding the evaluation of the consent as "freely given" is played by the bargaining power the data subject possesses in comparison with the data controller. If there is a significant imbalance of power consent is again considered invalid. Moreover, article 7 par. 4 of the GDPR suggests that an important parameter, among others, to assess if consent is freely given, is whether the data subject is asked to consent to the processing of the data subject that are not necessary for the performance of the contract. According to Opinion 06/2014 of WP29, the term "necessary for the performance of a contract" should be interpreted narrowly. In addition to the previous, Recital 43 of the GDPR is referred to the need of freely given consent. On the one side it mentions that there shall not be imbalance of power

[55] For more information: Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, p. 19

[56] Article 29 Data Protection Working Party, Guideline on Consent under Regulation 2016/679, wp279 rev. 01, p. 5

between data subject and data controller, while further it underlines that the consent is considered to be freely given only if the data subject is allowed to give separate consent for each data processing operation. Accordingly, Recital 32 states that" Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them"[57]. Concerning the "free" element, it should be ultimately mentioned that Recital 42 underlines that besides the free choice to consent or not, data subject shall also be able not only to refuse, but also to withdraw consent without any detriment.

In accordance with the requirements set by article 4, the consent of the data subject must also be "specific". Furthermore, pursuant to article 6 par. 1(a) *"the data subject has given consent to the processing of his or her personal data for one or more specific purposes"*, while the requirement for specific consent is also related closely to the principles of Lawfulness, fairness and transparency and Purpose limitation, as set at article 5 par. 1 (a) and 5 par. 1 (b) respectively, since this requirement aims to accomplish on the one hand an efficient level of transparency regarding each and every processing purpose and on the other hand clarification on the different consent requests. Relevant to this requirement is also the requirement for "informed" consent, since they are both linked with the principles of lawfulness, fairness and transparency and purpose limitation. For the consent to be informed, hence valid, the Article 29 Working Party requires data subjects to have in advance access at least to the following information: a) data controller's identity, b) the purpose of each of the processing operations for which consent is sought, c) what (type of) data will be collected and used, d) the existence of the right to withdraw consent, e) information about the use of the data for automated decision-making in accordance with article 22 (2)(c) where relevant, and f) on the possible risks of data transfers due to absence of an adequacy decision and of appropriate safeguards as described in Article 46[58]. At this point, it important to mention that the consent must be given in advance, before that initiation of the data processing, while the a posteriori permission is not considered a legitimate lawful basis[59].

Regarding the last requirement dictated by article 4, consent must be unambiguous. This means that consent cannot be given tacitly, but only explicitly with an active motion or declaration. Recital 32 sets the means available in order for the consent to be unambiguous, stating that consent could be given either written or orally, even by electronic means, excluding silent means.

In the context of employment relationships

According to the aforementioned in the previous chapters, an employer in the frame of a labour contract is also a data controller, while an employee is simultaneously a data subject. Therefore, the requirements set in the previous paragraph shall also apply for

[57] ibid, p. 10

[58] ibid, p. 13

[59] Aleksandropoulou-Aigiptiadou, Προσωπικά Δεδομένα: βασικές έννοιες και αρχές επεξεργασίας, υποχρεώσεις υπέυθυνου επεξεργασίας, δικαιώματα υποκειμένου, κυρώσεις, διασύνδεση αρχείων και διασυνοριακή ροή δεδομένων, ηλεκτρονικές επικοινωνίες, κωδικοποιημένη νομοθεσία (Personal Data: basic notions and processing principles, data controller obligations, data subjects' rights, sanctions, connection of files and transborder flow of data, electronic communications, codified legislation), 2016, p. 88

the lawful processing (hence monitoring as well) of employees' data by employers based on the consent of the employee.

However, the consent giving procedure demonstrates further differentiations in the context of employment relationships regarding the "free" element. The obstacle preventing the freely given consent of an employee is the position of weakness in comparison to the employer. As mentioned above, the consent is not considered freely given in case there is an imbalance of power between data controller and data subject. Such an imbalance of power occurs in the employment context, since an employee, so as a prospective employee, is highly dependent on the employer, hence it is unlikely that he/she will refuse to grant consent under the fear of unfavorable consequences as a result of the refusal. Therefore, the consent of an employee regarding his/her monitoring via video surveillance is unlikely to be considered freely given[60]. This conclusion was made long before the GDPR applied. According to the Opinion 8/2001 on the processing of personal data in the employment context of the article 29 Data Protection Working Party should be seen as a last resort in case other lawful basis does not apply[61] and only when there will be no adverse consequences, irrespective of whether they gave consent or not[62].

Notwithstanding the aforementioned, the GDPR allows under certain circumstances Member States to provide for specific rules on the processing of employees' personal data in the employment context. This possibility comes from the combination of article 88 and Recital 155 and can only be applied if the employee has provided genuinely free consent with the option to withdraw it without any detriment[63].

Non-consent-based lawful basis

Consent is not the only lawful basis mentioned on article 6. According to article 6 par. 1 (b) the necessity of the processing for the performance of a contract or in order to take steps as per request of the data subject prior to entering into the contract, is also a lawful basis. An employer, for example, concerning the pre contractual stage, could lawfully monitor the behaviour of a prospective employee via a questionnaire in order to proceed to the appointment, or assess the quantity of work by checking an employees' time of arrival, in regard to the performance of the contract[64]. Under article 6 par. 1 (c) the processing is also lawful, if it is necessary for the employer /controller in order to comply with legal obligations, as for instance tax payment. Pursuant to par. 1 (d), employer is able to lawfully process employees' personal data so as to protect the vital interests of the employee or of another natural person. For instance, in case of an accident at workplace, the employer could lawfully monitor employees' data in order to disclose them to a doctor if the employee is unable to. Furthermore, processing by data

[60] Article 29 Data Protection Working Party, Guideline on Consent under Regulation 2016/679, wp279 rev. 01, p. 7

[61] Article 29 Data Protection Working Party, Opinion 8/2001 on the processing of personal data in the employment context, p. 23

[62] Article 29 Data Protection Working Party, Guideline on Consent under Regulation 2016/679, wp279 rev. 01, p. 7

[63] Lempesi, 2017, p. 522

[64] Douka, Η προστασία των προσωπικών δεδομένων στη σχέση εργασίας (The protection of personal data in the employment relationship), 2011, p. 216

controller is lawful, if it is dictated by public interest purposes [article 6 par. 1 (e)], while last but not least an employer could legitimately process employees' data in order to protect his/her own- or third person's interest except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data [par. 1 (d)]. As an example one could mention that employers could legitimately present employees' personal data in front of a court in order to protect their interests[65].

Lawful basis on the processing of special categories of personal data

Employers as data controllers, process employees' personal data, which in many occasions belong to the special categories, such as health related data and information regarding the participation in trade union acts. Therefore, before proceeding forward it is useful to spare a few words regarding the lawful basis on the processing of special categories of personal data.

First of all, article 9, besides the exhaustive list of the data considered "special", states that their processing shall be prohibited. Nevertheless, paragraph 2 introduces some exceptions to this prohibition. To begin with, paragraph 2 (a) establishes consent as a lawful basis. The previous analysis regarding consent applies regarding special categories of personal data as well. This provision also allows Member States to introduce national laws preventing the possibility that consent is considered lawful basis for the processing of special categories of personal data in particular.

Pursuant to paragraph 2 (b), processing of special categories of personal data is also lawful as long as *"processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject"*. This provision is directly applicable in the field of employment relationships and is actually similar to the provisions of article 6, regarding personal data in general. However, in regard to special categories of personal data, the processing shall not only be necessary, but there is also the requirement that there is a Member State law providing safeguards for the fundamental rights and interests of data subjects, allowing the processing[66].

The rest of the exceptions to the prohibition of processing of special categories of personal data are introduced on article 9 par. 2 (c-j). Even though there is not an explicit reference to the context of labour relationships, they could also apply occasionally on employment relationships.

Employee's Rights as data subjects

The provisions of the GDPR provide a number of rights to data subjects in order to protect their personal data. These provisions are neither applicable to a specific field of personal data nor protect a particular category of data subjects. Hence, the rights provided for data subjects in regard to the processing of their data, as already

[65] Ibid, p. 224
[66] Koukiadis, 2017, p. 104

mentioned, also protect employees from the processing of data by employers (e.g., unlawful monitoring). These rights are the following:

The right to be informed

To begin with, an employee has the right to be informed regarding the processing of his/her data, which is actually a corollary of the "lawfulness, fairness and transparency" principle[67]. According to articles 13, when the data are collected from the employee directly, the employee has the right to be informed regarding the identity of the data controller or his/her representative, the contact details of the data protection officer, if applicable, the purposes and the legal basis of the processing, the recipients of the personal data and information regarding the availability of personal data in case the data controller transfers them to a third country. Furthermore, employees shall be provided with information regarding: i) the period of storage of data, ii) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability, iii) the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal, iv) the right to lodge a complaint with a supervisory authority, v) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data and vi) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. Moreover, in case the employer wishes to process personal data for purposes different than the ones that the personal data were initially collected form, the employer ought to provide a priori further information in regard to the new purposes.

Article 14 is also dedicated to the right of the data subjects to be informed, even in cases in which the personal data were not collected by the data subject. The previously stated on article 13 also apply, while the employee should have further information regarding the categories of personal data concerned and the source from which the personal data originate, and if applicable, whether it came from publicly accessible sources. The employer is obliged to provide this information in a reasonable period of time after the collection of the data, not exceeding one month, exempt from the exceptions set out in paragraph 5.

The right to information is the only right provided by the GDPR which is applicable without a previous action from the data subject. The information shall be provided clear and concrete, without any delay complying with the transparency principle.

The right of access

An employee, as a data subject, has the right to obtain confirmation from the employer as to whether or not personal data concerning him or her are being processed, and,

[67] see above, p. 13

wherever that is the case, access to information corresponding to article 13 and 14[68]. The employer, as a controller, shall provide a copy of the personal data undergoing processing, even by electronic means when possible, unless the exercise of this right adversely affects the rights and freedoms of others[69] [70].

The right to rectification

According to article 16 *"The data subject shall have the right to obtain from the controller, without undue delay, the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement"*. Hence, an employee may request the rectification of any inaccurate or the supplementation of his/her data without any delay (within a month in principle), otherwise the employer shall inform the employee on the grounds the request could not be accepted. For instance, the inaccurate data that are mentioned on an employee evaluation sheet could lead to him/her being fired or demoted, therefore the exercise of the right to rectification is actually impactful. It is interesting to note that the right to be informed and the right to access are actually prerequisites to the right to rectification, which is an alternative to the right to erasure.

The right to erasure ("right to be forgotten")

An employee, while operating as a data subject, has the right to obtain by the employer the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay in case: i) the data are no longer useful in order to attain the purpose for which they were initially collected, ii) the consent of the employee is withdrawn and there is no other lawful basis justifying the processing, iii) the employer exercises the right of article 21 (1)(2)[71], iv) the personal data have been unlawfully processed, v) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject or vi) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1)[72].

The aforementioned shall not apply only to the extent that the processing is necessary for i) exercising the right of freedom of expression and information, ii) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, iii) 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), iv) 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 v) for the

[68] Article 15 par. 1
[69] Article 15 par. 3,4
[70] Recital 63
[71] See below, "The right to object", page 22
[72] article 17 par. 1

establishment, exercise or defence of legal claims[73]. For example, an employer could lawfully store the necessary data of a former employee in order to prove the payment of salaries for a reasonable period.

The right to restriction of processing

Pursuant to article 18 par. 1 *"The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies: (a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data; (b)the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead; (c)the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims; (d)the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject"*. Paragraph 2 states that *"Where processing has been restricted under paragraph 1, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State"*, while according to par. 3 *"A data subject who has obtained restriction of processing pursuant to paragraph 1 shall be informed by the controller before the restriction of processing is lifted"*[74]. This right is in fact useful in cases that it is not clear whether the right to erasure can be applied, and this right provides the data subject with a temporary protection.

The right to data portability

The right to data portability introduced in article 20, is a provision firstly introduced by the GDPR. Pursuant to it, an employee has the right to receive his/her personal data in a structured, commonly used and machine-readable format and transmit them without hindrance to another controller, for example a new employer, in case the processing was based on consent, it was necessary for the performance of the contract or the processing was carried out with automated means.

The right to object

Article 21 provides data subjects with the right to object against processing of their data. This right is supplementing the rest of the rights entitled to data subjects. An employee could object against the processing of his/her personal data even if it is based on a lawful basis. The employer is forced to stop the processing, unless he/she can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. The stopping of the processing shall not be general, but only binds the employer regarding the purposes the employer is objecting against. It is worth mentioning in order to underline the importance of this right, that the GDPR dictates that the data subject

[73] article 17 par. 3
[74] Also see Recital 67

shall be informed in detail regarding the right to object, separately from his/her other rights.

The right not to be subject to a decision based solely on automated processing (including profiling)

The advances in the sector of technology have given data controllers the ability to use profiling[75] and automated decision making techniques, which are more cost and time efficient. This progress has not left employers, as data controllers, unattached. However, this practice conceals dangers for the protection of employees' (and data subjects' in general) rights, since automated systems often demonstrate insufficiencies similar to humans, which might actually result in unfair discrimination of employees. Furthermore these systems allow the rapid processing of a vast amount of data without any check regarding the accuracy and necessity of them. For instance, a prospective employee might unlawfully have his/her job application rejected due to an evaluation of CVs with automated means[76]. Hence, there is a need for a solid legal framework for automated processing and profiling.

The GDPR includes several references to the issue. Articles 13 and 14 provide an ex ante protection via the right to be informed. However, these provisions offer a precautionary protection and cannot provide legal protection after a decision was made based solely on automated processing[77]. Article 22 par. 1 states that *"The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her"*, unless the decision is necessary for contractual purposes between the data controller and the data subject, there is a Union or National law allowing so, or the data subject has provided explicit consent (par. 2). For the first and the third exceptions par. 3 of article 22 requires that the controller shall have implemented safeguard measures for the protection of the data subject's rights and legitimate interests at least in order to obtain human intervention to the decision-making, express an opinion or give consent. An issue arising from par. 1 regards element of "bases solely on automated processing", since there are instances in which data controllers might fabricate a human involvement. According to Article 29 Working Party, it is necessary for the human involvement to be meaningful, with an actual effect on the decision, actually able to also overturn it, and not just a token gesture[78].

Last but not least, it should be mentioned that a reference regarding this topic in Recital 71 of the GDPR. According to some scholars, Recital 71 is the only available mention in the GDPR regarding the "right to explanation". This right is described as the

[75] According to article 4 (4) GDPR "'profiling 'means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements"

[76] Kanellos, The GDPR Handbook, 2020, p. 156

[77] Wachter, Mittelstadt, Floridi, Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation2016, p. 14, [https://ssrn.com/abstract=2903469], accessed 22 December 2021

[78] Article 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, p. 21

right of the data subject to obtain an explanation regarding the functionality of the automated decision-making system and the reasons and rationales of specific automated decisions[79]. Nonetheless, many support the opinion that since the only reference lies on the Recital, the right to explanation is not protected by the GDPR, since the Recital does not provide with legally binding rules[80].

Employer's Obligations as Data Controller

Accountability

According to the accountability principle[81], the employer carries the burden to prove his/her compliance with the provisions of the GDPR regarding the protection of employees' persona data, except for the compliance itself. Even in an occasion of a data breach, any measures that the employer has taken towards the completion of this obligation will be evaluated positively by the supervisory authorities[82].

Records of processing activity

According to article 30, every controller is obliged to hold a record of the processing activities. Regarding employers specifically, the maintenance of a record is not obligatory for enterprises or organisations employing fewer than 250 persons, unless the processing poses risks in regard to rights and freedoms of employers, the processing regards special categories of data or personal data relating to criminal convictions and offences referred to in Article 10[83]. This provision repealed the previous one of the Data Protection Directive, which provided for a general obligation to notify the processing of personal data to the supervisory authorities, which posed administrative and financial burdens and was not always efficient enough[84].

Security of processing

Pursuant to article 32, an employer shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. This article also includes an indicative list of such measures including pseudonymisation and encryption, measures ensuring confidentiality, integrity, availability and resilience of processing systems and services, measures assisting the timely restoring and access to personal data in case of technical or physical incidents and a process evaluating the efficiency of such measures. The same apply also to data processors, while both data controllers and processors shall ensure that natural persons having access to data shall not process them without the instructions of the controller.

[79] For more information ibid, p. 6
[80] Kaminski, The Right to Explanation, Explained, 2018, p. 194 [https://ssrn.com/abstract=3196985], accessed 22 December 2021
[81] see above, p. 15
[82] Article 57 par. 1 (d)
[83] Article 30 par. 5
[84] Recital 89

Notification of a personal data breach to the supervisory authority

Under the provision of article 33, in case of employees' data breach, the employer, not later than 72 hours after becoming aware of it, shall notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless there is not any existent danger for the rights and freedoms of the employee.

Data protection impact assessment

Article 35 introduces the obligation of the data controller to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. This provision applys in particular when the processing is operated with the use of new technologies and is likely to create risks regarding data subjects' rights and freedoms. This obligation is highly relevant to the context of employment relationships, since employers often use new technologies to monitor employees, like video and voicing capturing and position tracking systems. Article 35 also cites some particular cases in which the assessment is required. Under paragraph 3 *"A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of: (a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; (b)processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or (c)a systematic monitoring of a publicly accessible area on a large scale".*

Legal Protection - Sanctions

The GDPR includes preventive causes for the illegitimate processing of personal data, which also, as mentioned, are applicable to employment relationships, putting obstacles to the unlawful processing of employees' data. On the one hand, the threat of administrative sanctions, civil claims, even criminal charges, act proactively towards the protection of data subjects' rights, discouraging data controllers from unlawful processing, while on the other hand the enforcement of the above aims to cease the unlawfulness and restrict the damages the data subjects suffered.

To begin with the *administrative sanctions*, article 57 par. 2 of the GDPR provides for a set of corrective powers entitled to supervisory authorities. Among these powers supervisory authorities are competent to also impose administrative fines, which may be actually significant. Pursuant to article 83 par. 2, for the estimation of the amount of the administrative fee the supervisory authority shall take into consideration a variety of grounds depending on each individual case, like the gratitude of the infringement, the categories of infringed personal data, any previous infringements by the controller (or processor), whether the infringement occurred due to negligence or intent, etc., while the total amount of the fine could reach 10.000.000 EUR for the infringements mentioned on paragraph 4 or 20.000.000 EUR according to paragraph 5. The GDPR acknowledges strict liability of the controller, meaning that fault is not a requirement for the imposition of fine[85], while furthermore a fine could be imposed even if the data

[85] Koukiadis, 2017, p. 143

subject suffered no damages. A potential infringement could be communicated to the authorities by the employee himself/herself, as article 77 of the GDPR introduces an additional right of data subjects, according to which data subjects have the right lodge a complaint with a supervisory authority, while article 78 states that data subjects could also proceed with legal actions against a legally binding decision of a supervisory authority.

In addition to the administrative sanctions, the GDPR also acknowledges the *civil liability of the data controller* (and sometimes of processor[86]). According to the first paragraph of article 79 *"Without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority pursuant to Article 77, each data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights under this Regulation have been infringed as a result of the processing of his or her personal data in non-compliance with this Regulation"*, while the second paragraph settles issues regarding competence. Pursuant to article 82 paragraph 1, a data subject that suffered material or non-material damage as a result of an infringement of the GDPR provisions shall have the right to receive compensation from the controller or processor for the damage. An employee could base his/her claims against his/her an employer either on tort liability or on the breach of the labour contract. Unlike administrative sanctions, civil liability requires that the infringement of the Regulation has caused damages to the data subject. Except for compensation, an employee could also claim the annulment of an employer's decision[87]. Article 82 par. 3 states that the data controller (or processor) carries the burden to prove his/her lack of responsibility.

Last but not least, article 84 of the GDPR allows Member States to introduce *criminal sanctions* for data processing related infringements via national legislation, as long as the penalties are effective, proportionate and dissuasive. Those penalties may also allow for the deprivation of the profits obtained through infringements of this Regulation[88].

[86] Article 82 par. 2

[87] Koukiadis, 2017, p.150

[88] Recital 149

Specific issues regarding monitoring of employees

The progress in the technological sector has enabled employers to implement a wide variety of measures for the monitoring of employees. Methods like video surveillance, access to electronic devices used by employees, monitoring of employees' communications and social media, biometric methods and vehicle tracking systems are some of the techniques that employers use.

Video surveillance

One of the most common and discussed methods of employee monitoring is the use of video surveillance systems in the workplace. One the one hand, an employer has the right to protect the interests of his/her enterprise. An employer would use video surveillance systems mainly for the prevention of crimes in the workplace, especially property crimes like theft, and the protection of the employees and customers in such cases. In fact, there are instances that even the law could require the use of video recording, depending on the particularities of the workplace[89]. Furthermore, sometimes such systems would assist employers to the assessment of employees' productivity and work ethic. Especially nowadays, the progress in technology allows an employer the possibility to access the collected data easily and remotely (for example via smart phone)[90].

On the other hand, video monitoring is highly intrusive to employees' privacy. The use of such systems in proved to create anxiety resulting into a stressful working environment. Employees are trying to adapt their behaviour to what they believe employers would approve of, consequently there is the risk for an unrepresentative profiling of employees' character. Actually, even if the video surveillance is only occasional, it is highly probable to affect the behaviour of employees even when such systems are turned off[91].

Hence, for the fairness and lawfulness of video surveillance a balancing between employers' and employees' rights is vital, along with the proportionality principle[92]. An important aspect regarding the legitimate use of such systems is whether they are necessary and appropriate for the accomplishment of the pursued purpose, while there is not an effective alternative. The purpose of property protection and employees' safety could be achieved with video surveillance systems, however the use of such systems would be unlawful if it exceeds the limits of proportionality. For instance, the video surveillance of places like locker rooms or toilets would be completely disproportionate, due to the fact that it would infringe massively the employees' right to privacy[93]. Furthermore, it is important that the purposes of monitoring are stipulated prior to the installation of such systems[94]. An employee has the right to be informed

[89] Douka, 2011, p. 184
[90] Article 29 Data Protection Working party, Opinion 2/2017 on data processing at work, p. 10
[91] ibid
[92] Zerdelis, 2014, page 611
[93] Article 29 Data Protection Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance, p. 25
[94] Enic Pogace, 2016,p. 6

about the purposes of the processing according to the provisions of the GDPR. Hence, if the purpose of the monitoring via CCTV in the workplace is the safety of property and employees, the further use of the data collected by such means in order to evaluate the efficiency of an employee would be unlawful.

The decision of the Grand Chamber of ECtHR, regarding the López Ribalda and Others v. Spain, is relevant to this issue. In this case the applicants were informed that in the supermarket, where they were working as cashiers, there were CCTV cameras installed, since there were suspicions for stealing incidents. However, the employer also installed some hidden cameras without the employees' knowledge. The court, after balancing the rights of each side, concluded that there was not an infringement of employees' right to privacy, taking into consideration that the data collecting process was not excessive, as it only lasted 10 days, and the data were accessed by a minor amount of persons, just for the purpose of finding the person responsible for the illicit activities[95].

Access to electronic devices

For the purpose of the performance of labour contract, employers are used to providing employees with devices, mainly personal computers and mobile phones. An issue arising regarding the use of these devices is whether they could be used for private reasons, irrelevant to work, and if so, which is the appropriate method of monitoring.

First of all, the use of such devices, along with the internet access at workplace, is able to consume a lot of working time, affecting the quality and quantity of work an employee provides for. From this perspective an employee has a legitimate interest to monitor employees or put some ground rules regarding the use of such devices. According to article 24 of the GDPR employers shall implement specific policies regarding the use of such devices, like prohibiting the use of them for reasons unrelated to the employment relationship and informing that the employer could proceed to the monitoring of such devices, communicating the purpose and implemented safeguard measures of the monitoring. However, if there is not such policy or the policy allows the use for private purposes, in case an employer accesses private information saved on an electronic device it is considered processing of personal data and it would be considered legitimate only if it was based on a lawful basis. In such an occasion, yet again it would be necessary to find a balance between the legitimate interests of the employer or public interest and employees' privacy.

The decision number 954/2020 of the Greek Supreme Court is quite representative regarding the access to an employees' Professional Computer[96]. In this case two employees of a Greek Court, whose responsibilities were related to criminal charges and prosecution, were repeatedly hiding documents, in order to avoid the great workload. Their unlawful actions created obstacles to the administration of criminal justice. The main evidence the Court of Appeal used for their conviction was a conversation on the application "Messenger" of the platform "Facebook", which was

[95] For more information access https://hudoc.echr.coe.int/fre#%7B%22itemid%22:[%22002-12630%22]%7D

[96] Access at http://www.areiospagos.gr/nomologia/apofaseis_DISPLAY.asp?cd=MEZGNPCZG7966EV1T1F3VHJR62OZWZ&apof=954_2020&info=%D0%CF%C9%CD%C9%CA%C5%D3%20-%20%20%C6

found on the professional computer of one employee. The employees referred to the Supreme Court stating that the evidence was unlawfully obtained by violating their right to data protection and privacy. However, the Supreme Court decided that there was not such a violation, since the personal data were collected from a professional computer and the authorities accessed only the necessary information, while furthermore the website password was saved on the browser and anyone using the professional computer could access it easily.

Monitoring of communications

Another issue that has repeatedly concerned the jurisprudence of the Court is the monitoring of employees' communications. An employee communicates with clients, suppliers or other individuals via mail, telephone or other means while working, and these communications could potentially create obligations for the employer and his/her enterprise. Hence, the monitoring of employees' communication is reasonable in this sense. Crucial for the distinction between the lawful and unlawful monitoring of communications of employees is whether the nature of these communications is professional or private[97].

One of the most infamous court decisions regarding the lawfulness of Internet communications is on the Barbulescu v Romania case[98]. Barbulescu was employed as an engineer in charge of sales at a private company. This company fired Barbulescu on the ground that he used a "Yahoo messenger" account created by the company for professional purposes, for private communications. Barbulescu took legal actions against his firing. The ECtHR ruled at first instance that there was not a breach of article 8 of the European Convention of Human Rights, as the legitimate interest of the employer prevailed. However, the Grand Chamber overruled the initial decision, due to the fact that it was not proved that the employers had informed the applicant regarding the monitoring of his communications and if so, surely not to the extent of monitoring private communications.

Regarding the monitoring of telephone calls, the ECtHR decided on the Halford v UK case[99]. Ms Halford was a British employee at the Police Corps, who was denied promotion. She supported that the denial was a result of discrimination and was based on the interception of data from private phone calls, made by a device given by the police agency, but destined for private communications. The ECtHR denied the allegations of the British government that those phone calls shall not be protected under article 8 of the European Convention of Human Rights due to the fact that the phone device was provided by the police. Instead, the Court ruled that there was a breach of the employee's right to privacy, since private calls shall be considered private even if the device was provided by the employer and took place at workplace, and also the employee was not informed regarding a potential monitoring of that type.

[97] Zerdelis, 2014, p. 609

[98] Access at https://hudoc.echr.coe.int/eng?i=001-177082

[99] Access at https://hudoc.echr.coe.int/eng?i=001-58039

Monitoring of Social Media

Nowadays social media have become a part of everyone's daily life, and they are established as one of the most widespread means of socialising. There is a wide variety of personal data that are uploaded to social media in regard to pretty much every aspect of someone's life. This voluntary exposure of data might, in fact, lead to different forms of processing depending on the purposes of the data controller. Putting the aforementioned to the context of the current study, it is obvious that employers would be interested to collect as much information as possible regarding employees, prospective employees or even ex-employees.

Regarding the performance of the labour contract, an employer would have a legitimate interest in checking whether during the working schedule an employer is active on social media, instead of focusing on working or check whether an employee vilifies the enterprise or colleagues publicly. However, it is important to point out that in order for such monitoring to be lawful, the activities of the employer on social media shall be publicly accessible, otherwise it is doubtful that the monitoring would be legitimate.

Furthermore, even before the conclusion of the employment contract, employers are often monitoring the social media profiles of prospective employees. The personal data available on social media could be certainly useful for employers in order to evaluate who is the most qualified candidate, especially regarding profiles on social media, like "Linkedin", that are meant to demonstrate career profiles. The use of the data collected shall be based on the interests of the enterprise, instead of personal preferences. Nevertheless, a prospective employee has no mean available in order to discover whether an employer bases the rejection of the job application to objective criteria or discriminatory reasons.

Last but not least, an employer could have legitimate interest to monitor ex-employees' social media. A former employer could lawfully monitor a social media profile of a former employee in case they have agreed to a non-compete clause, but only as long as this clause is active[100].

Position Tracking Systems

The technological developments have given employers the opportunity to track vehicles using Global Pointing Systems (GPS). These systems allow the employer to monitor vehicles' position, as well as the employees', in other words collect personal data. The installation of such systems may serve legitimate interests of employers or could also be imposed by law for the safety of the driver[101].

The legitimate interest of an employer could be interpreted in many ways. For instance, the installation of a GPS on a professional vehicle, could assist to the tracking of its location in case of theft. Regarding the context of employee monitoring, a GPS allows the employer to optimize the operation of the enterprise by discovering the shortest route or assess the ability of a professional driver. Nonetheless, this monitoring is simultaneously processing of personal data, consequently the provisions and principles of the GDPR also apply. Hence the use of GPS shall be appropriate and

[100] Opinion 2/2017 on data processing at work, p. 12
[101] Ibid, p.19

necessary for the accomplishment of the aimed purpose, when there is not a less invading into employees' privacy alternative. Furthermore, the employer is obliged to inform the employee regarding the existing of a location tracking system. In addition to the previous, given the particularities of the data the use of GPS provide for, the monitoring of employees position outside the working schedule should be excluded[102]. Moreover, in case that the employee is allowed to use a professional vehicle for private purposes, the GPS shall have a turn-off button.

As the opinion 12/2011 on Geolocation services on smart mobile devices of Article 29 Working party states *"Vehicle tracking devices are not staff tracking devices. Their function is to track or monitor the location of the vehicles in which they are installed. Employers should not regard them as devices to track or monitor the behaviour or the whereabouts of drivers or other staff, for example by sending alerts in relation to speed of vehicle".*

Biometric systems

In recent years, the use of biometric methods has become more and more popular for the monitoring of entry and exit in workplaces from the employers. The biometric systems are applications of biometric technologies, which allow the automatic identification, and/or authentication/verification of a person[103]. These techniques can be divided in two categories: a) physical and physiological-based techniques which measure the physiological characteristics of a person (for instance fingerprint verification, face recognition, voice recognition, eye iris verification etc.) and b) behavioural-based techniques, which measure the behaviour of a person and include hand-written signature verification, keystroke analysis, gait analysis, etc.[104].

Such systems utilize biometric data, which according to article 4 (14) are *"personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data"*. These data are considered sensitive under the provisions of the GDPR and are included in the special categories of personal data of article 9 par. 1. Hence, the processing of such data is prohibited, unless the exceptions of paragraph 2 apply. Given their nature it is obvious that biometric data are not meant to be processed for insignificant purposes. It is vital that the proportionality principle is not breached. For instance, the processing of biometric data for the sole purpose of entering into an office would be totally unlawful, since there are other appropriate measures that are less intrusive, like entry cards. Nevertheless, for the entry in places of high importance, like a military base or specific banking facilities, the processing of biometric data could be considered legitimate.

In any case, the data processor is obliged to inform the employee regarding the processing of such data and carry out an assessment of the impact of the envisaged processing operations on the protection of personal data according to article 35 of the GDPR.

---

[102] ibid, p. 20

[103] Article 29 Data Protection Working Party, 12168/02/EN WP80m Working document on biometrics, p. 3

[104] ibid

Conclusions

The rapid developments in the sector of technology the past decades have provided employers with several tools, assisting the monitoring of employees' personal data. The use of professional computers and devices in general, e-mails, video surveillance systems, vehicle tracking systems, biometric systems, along with the excessive use of social media in the modern era, have generated new needs regarding the balancing between employers' legitimate interests and rights and employees' rights to data protection and privacy. An employee could seek for protection of his/her privacy from monitoring in several international legal documents. Probably the most important one is Article 8 of the European Convention of Human Rights, which became the source for a multitude of important decisions of the ECtHR, while at the same time national legislation provides employees with a wall of protection.

The biggest step towards the safeguard of the right to data protection on an EU level was the application of the General Data Protection Regulation. Even though the provisions of the GDPR are of general application and there is not a specific provision for the protection of employees from monitoring by their employers, the fact that monitoring is a form of personal data collection means that the GDPR provisions also apply in such occasions, since data collecting is a from of processing. Hence, all rights of data subjects arising from theGDPR protect employees, while the obligations of data controllers bind employers as well. Employers, while monitoring employees, have to respect the provisions and principles set by the GDPR on a contractual and pre contractual level, since they collect employees' data even before the conclusion of a labour contract, for instance during interviews. Afterwards, during employment relationship, employers still process employees' data for several purposes, like the compliance with legal obligations or the performance of the contract. Lastly, an employer might still have a legitimate interest to monitor an employee after the end of the employment relationship, for instance in case there is a non-compete agreement signed.

An employee has a multitude of rights as a data subject, like the right to be informed, the right to access, the right to rectification, the right to erasure, the right to restriction of processing, and the right to data portability. Also, an employee has the right to lodge a complaint with a supervisory authority and the right to an effective judicial remedy. On the other side the GDPR is the source of several employers' obligations. For instance, an employer is obligated to be able to prove the compatibility of employee monitoring with the provisions of the GDPR (accountability), implement the appropriate measures for the security of employees' personal data, assess the impact of the processing to personal data and keep records of the processing. In case of a breach of the GDPR provisions by the employer, the Regulation provides for administration, civil or criminal sanctions against him/her.

Last but not least, an employer has to base any processing of employees' personal data, hence monitoring as well, on a lawful basis. Lawful basis could be the consent of the data subject, the necessity of the processing for the performance of a contract or the necessity for the compliance with a legal obligation of the employer. The processing of special categories of personal data, which are often processed in the context of an employment relationship, is only exceptionally allowed. Regarding the

consent as a lawful basis, it shall be mentioned that it should be considered only as a last resort, since the imbalance of powers between employers and employees rarely allows the consent to be considered freely given.

Bibliography

Books

Aleksandropoulou-Aigiptiadou E. K. (2016). Προσωπικά Δεδομένα: βασικές έννοιες και αρχές επεξεργασίας, υποχρεώσεις υπεύθυνου επεξεργασίας, δικαιώματα υποκειμένου, κυρώσεις, διασύνδεση αρχείων και διασυνοριακή ροή δεδομένων, ηλεκτρονικές επικοινωνίες, κωδικοποιημένη νομοθεσία (Personal Data: basic notions and processing principles, data controller obligations, data subjects' rights, sanctions, connection of files and transborder flow of data, electronic communications, codified legislation), Nomiki Vivliothiki, Athens, Greece

Chrysogonos K. C., Vlachopoulos S. V. (2017). Ατομικά και Κοινωνικά Δικαιώματα (Individual and Social Rights), 4th edition, Nomiki Vivliothiki, Athens, Greece

Donos, Mitrou, Middleton, Papakonstantinou (2002). Η αρχή προστασίας των προσωπικών δεδομένων και η επαύξηση της προστασίας των δικαιωμάτων (The principle of protection of personal data and the increase of the right protection, Sakkoulas, Athens - Thessaloniki

Douka V. (2011). Η προστασία των προσωπικών δεδομένων στη σχέση εργασίας (The protection of personal data in the employment relationship), Sakkoulas, Athens - Thessaloniki, Greece

Igglezakis I. (2018(Ο Γενικός Κανονισμός προστασίας Προσωπικών Δεδομένων - Εισαγωγή στο νέο νομικό πλαίσιο προστασίας προσωπικών δεδομένων (The General Data Protection Regulation - Introduction to the new legal framework of personal data protection, INTERACTIVE BOOKS, Greece

Kanellos L. (2020). The GDPR Handbook, Nomiki Vivliothiki, Greece

Kizza J. M. (2017). Ethical and Social Issues in the Information Age (6th ed.), Cham: Springer International Publishing

Koukiadis (2017). Εργατικό Δίκαιο: ατομικές εργασιακές σχέσεις και το δίκαιο της ευελιξίας της εργασίας (Labour Law: individual employment relationships and the law of the flexibility of work), 8th edition, Sakkoulas, Thessaloniki, Greece

Ladas D. (2018). Το δικαίωμα της προσωπικότητας του εργαζομένου (The personality right of employee), Nomiki Vivliothiki, Athens, Greece

Liksouriotis G. D. (2017). Ατομικές εργασιακές σχέσεις (Individual Employment Relationships), 5th edition. Nomiki Vivliothiki. Athens, Greece

Malgardi A. K. (2010). Νέες τεχνολογίες, προσωπικά δεδομένα και εργατικό δίκαιο (New technologies, personal data and labour law), Sakkoulas, Athens-Komotini, Greece

Michos S. (2007). Η επιτήρηση των τηλεπικοινωνιών μέσω ίντερνετ στον χώρο εργασίας (The monitoring of telecommunications via Internet in the workplace), Sakkoulas, Athens, Greece

Zerdelis D. (2014). Ατομικές Εργασιακές Σχέσεις (Labour Law, Individual Employment Relationships), 4th edition, Sakkoulas, Athens-Thessaloniki, Greece

Zerdelis D. (2016), Συλλογικό Εργατικό Δίκαιο (Collective Labour Law), Sakkoulas, Athens - Thessaloniki

Articles and Journals

Adrienn L. (2017), To post or not to post-that is the question: Employee monitoring and employees' right to data protection, Masaryk University Journal of Law and Technology, Vol. 11, No. 2, Hungary, pp. 185-214

Cohen, J. (2013). What Privacy is for, Harvard Law Review, Vol 126, No. 7, USA, pp. 1904-1923

Cohen, J. (2019). Turning Privacy Inside Out Theoretical Inquiries in Law 20.1, USA

Douka V. (2018) Προσωπικά δεδομένα και εργασιακές σχέσεις: προστασία σύμφωνα με τον Γενικό Κανονισμό Προστασίας Δεδομένων (Personal Data and Employment Relationships: protection according to General Data Protection Regulation), ΕΕργΔ (Revision of Labour Law), p. 641

Lempesi D (2017). Γενικός Ευρωπαϊκός Κανονισμός για την προστασία των προσωπικών δεδομένων 679/2016 ΕΕ- Κατάργηση της Οδηγίας 95/46/ΕΚ - Συγκρητική Μελέτη (General European Regulation for the protection of personal data 679/2016/EU- Repeal of Directive 95/46/EC - Comparison Study, Δελτίον Εργατικής Νομοθεσίας (Labour Legislation Ticket), Greece, p. 497

Mitrou L. (2017). Ιδιωτικότητα, προσωπικά δεδομένα και εργασιακές σχέσεις (Privacy, personal data and employment relationships), ΕΕργΔ (Revision of Labour Law), p. 140

Pogace, E. (2016). Employees' Data Protection in the Workplace and its Legal Implications, A Comparative Overview of EU's Legal Framework, International In-House Counsel Journal, Vol. 10, No. 37

Simitis S. (1999), Reconsidering the Premises of Labour Law: Prolegomena to an EU Regulation on the Protection of Employees 'Personal Data, European Law Journal, Vol. 5, No.1, Blackwell Publishers Ltd, Oxford, USA, pp. 45–62

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

Wachter S., Mittelstadt B. ,Floridi L. (2016). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, International Data Privacy Law, Oxford, USA

Warren S. D. and Brandeis L. D. (1890). The Right to Privacy, Harvard Law Review, Vol. 4, No. 5, p. 193-220.

Legislation - Legal Documents

Convention for the Protection of Individuals with Regard to Automatic Processing of personal Data (Council of Europe, 1981)

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data

European Convention of Human Rights (Council of Europe, 1950)

Guidelines for the Regulation of Computerized Personal Data file (U.N., 1990)

International Covenant on Civil and Political Rights (U.N., 1966)

Kaminski M. (2018). The Right to Explanation, Explained, 34 Berkeley Technology Law Journal. Vol. 34, No. 189, p. 190

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (September, 1980)

Recommendation No. R (89) 2 of the Committee of Ministers to Member States of the Council of Europe on the Protection of Personal Data used for Employment Purposes

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, (General Data Protection Regulation)

Universal Declaration of Human Rights (U.N., 1948)

Article 29 Data Protection Working Party Documents

12168/02/EN WP80m Working document on biometrics

Guideline on Consent under Regulation 2016/679, wp279 rev. 01

Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679

Opinion 1/2010 on the concepts of “controller” and processor”

Opinion 2/2017 on data processing at work

Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance