DATA PROTECTION OF EMPLOYEES – CERTAIN ASPECTS OF ECHR AND GDPR PROTECTION

Jasna Cosabic

Dr iuris Jasna Cosabic, CIPP/E, Privacy professional, Salzburg, Austria,
www.linkedin.com/in/jasna-cosabic

Keywords: ***data protection, employee data, special categories of data, video surveillance, monitoring***

Abstract: *Privacy issues of employees have been dealt with by some of the key judgments of the European Court of Human Rights (´the ECtHR´), giving as such an interpretation of the European Convention for the Protection of Human Rights and Fundamental Freedoms (´the ECHR´), in particular Article 8, the right to respect for private life. The General Data Protection Regulation (´the GDPR´), has managed to regulate in a unique way privacy issues in the European Union (´the EU´), but under certain conditions having wider territorial implications. Privacy issues regarding the employees cover very detailed aspects before the employment, during the employment and after the employment. This paper does not aim to give exhaustive explanations to overall privacy issues connected to a working place and in general employees, but rather to point out to certain aspects of possible privacy violations with regard to workers/employees. It shall give a short comparison between the two most successful systems in Europe that may give protection to data privacy issues, which are the European human rights system, with the case-law of the ECHR developed by the ECtHR in Strasbourg, and the system of the protection of privacy data that has been implemented since 25 May 2018 under the GDPR.*

1. Introduction

Privacy issues of employees have been long dealt with by some of the key judgments of the ECtHR, giving as such an interpretation of the ECHR[1], in particular Article 8, the right to respect for private life.

The importance of private life and private time of employees has been highlighted in the legislation of certain EU countries, by underlying in the legislature the notion of private time of workers by enabling them not to be obligated to be online accessible after working hours.[2] However, growing exposure of privacy of employees as well as expansion of electronic workplace[3] or homeoffice, has been pronounced by information technology growth offering sophisticated methods of monitoring employees, which demand carefully designed legal methods of protecting them. The GDPR[4], has managed to regulate in a unique way privacy issues for the persons in the EU, which accompanied by valuable guidelines and interpretations by the European Data Protection Board (´EDPB´), formerly Article 29 Data Protection Working Party (`Article 29 Party´) constitute pivot of privacy protection in the EU.

The Charter of Fundamental Rights of the European Union (´CFREU´) follows the spirit to the ECHR, referring to it and to the case law of both the ECtHR and the European Court of Justice (`ECJ`).[5] However it has in its Article 8 dealt especially with the protection of personal data, which has, since its legally binding nature as from Lisbon Treaty in 2009, played an important role in the context of data protection in the EU. Moreover, in the wording of Article 8, we may recognise principles that have been adopted by the GDPR.

1 European Convention for the Protection of Human Rights and Fundamental Freedoms.
2 Cosabic, Right to be Disconnected – The Wave to Catch On, The Political Anthropologist, 2017.
3 See Ford/Notestine/Hill, Fundamentals of Employment Law, American Bar Association, 2000, p. 449.
4 General Data Protection Regulation.
5 See Preamble and Article 53 of the CFREU.

At the outset, it enshrines the right to protection of personal data, which may, according to European human rights standards, entail both positive and negative obligations, i.e. obligation to ensure the protection of personal data, and obligation to abstain from interference. Furthermore, from the wording ´data must be processed fairly for specified purposes´ (para 2, Article 8) the principle of fairness of processing personal data as well as principle of purpose limitation stem out. Consent of the person concerned, under the same provision will later in the GDPR be recognised as one of the criteria for lawfulness of processing[6]. ´Legitimate basis laid down by law´ speaks out of lawfulness criteria which extends also to what is legitimate under the European human rights standards with a view to notion ´prescribed by law´[7] and which is incorporated in the GDPR.[8] Right of access to data, and the right of rectification were furtherly provided by the above provision of the CFREU and were included as such in the GDPR providing for rights of data subjects when processing of their personal data is at stake[9].

Covid-19 pandemic and various measures adopted in order to control it, have given rise to questions as to possible human rights violations including data protection issues. Certain examples in this regard may be presented with respect also to data protection of employees.

One of the measures often performed by employers is scanning of the employees´ body temperature with devices usually mounted at the entrance of employer´s building. While this may be justified for the purposes of preserving public health even without consent of the data subject according to Rec. 54 of the GDPR, each employer should also regulate whether those data are kept in their system, and if so, for how long, etc.

It is also common praxis of certain employers to require regular PCR testing of its employees to be allowed to perform their everyday duties. It is especially pronounced in branches where employees are in often daily contact with customers, for example employees in hotels, restaurants, pharmacies, care centres, hospitals, etc. The results of the testing clearly present health data, and therefore special category of data, which should be kept according to strictly defined proceedings adopted by employers and for time necessary for achieving the purpose of testing. Austrian Economic Chambers has recommended that information on testing runs between the employee and the testing laboratory. In case of positive test results employee and relevant health institution are informed, and it is the obligation of the employee to inform his/her employer. It is also indicated that the results of the test could not be grounds for termination of employment, and employees are advised to challenge any such termination before the Court[10] At this point it is also very important that these data are not unnecessarily disclosed to public, media, etc., having in mind that apart from the necessary tracing of contacts in order that the pandemic is well controlled, unnecessary revealing of data of persons positive of Covid-19 bears other consequences such as social stigma[11]. Therefore, the principle of purpose limitation is pronounced in this instance requiring that processing of data such as the results of PCR testing, under the criteria of special data, should be done only for the purpose of controlling the pandemic and preventing of spreading the disease.

And the third example, that the Covid world society is yet to be faced with, is the question of vaccines. Whether vaccination is of obligatory nature or not is to be decided by each state. Certain countries in Europe provide for a compulsory vaccination, for a certain number of vaccines. Before the Grand Chamber of the ECtHR, several cases are pending against the Czech Republic, (Vavřička v. the Czech Republic and five other applications[12]), as to whether parents have the right to refuse the compulsory vaccination of their children. The right of conscientious objection is often pronounced as one of the basic human rights, in the light of freedom of conscience. On the other hand, in the age of pandemic such as Covid-19, a question of whether the

6 Article 6 (a) of the GDPR.
7 See for example judgment of the ECtHR in the case of Sunday Times v. the United Kingdom, 1979.
8 Article 6 (c) of the GDPR.
9 Article 16 - Right to rectification and Article 15 - Right of access.
10 Wirtschaftskammern Österreichs, Covid-19-Tests bei Mitarbeitern, https://www.wko.at/service/Infoblatt-Covidtest-Juni-2020.pdf.
11 See for example, Social Stigma associated with COVID-19, IFRC, UNICEF, WHO, 2020.
12 Press Release issued by the Registrar of the ECtHR (ECHR 003 2020) on 6 January 2020.

vaccination should be obligatory or not is again in the spotlight. While it may be hard to impose an overall obligation of vaccination, for employees who are in a daily contact with vulnerable groups of persons in respect of whom contracting the Covid illness may be fatal, such a solution may prove to be legitimate. According to the well-established case-law of the ECHR, when private life and freedom of conscience may be limited with reasons of preserving a public health, a fair balance must be struck between burden put on one party, in this case the eventual obligation of employees in specific branches to be vaccinated, and the danger to which the vulnerable group of persons could be exposed otherwise. Speaking of employees, data of whether an employee objects to receiving a vaccine or not, may be relevant for specific branches, and may have consequences on whether such employee would be allowed to work in those branches or not. For example if the employee of a nursing home refuses a vaccine, that data may have consequences to his/her working in that and other nursing homes as well[13]. At the same time, working in other branches, which do not include contacts with vulnerable groups, may not be affected.

Therefore, a careful implementation of data protection principles according to which both the privacy of the relevant employee but also the interest of a wider society to the extent of preservation of public health should be protected through a careful applying of fair balance of burdens put on both sides.

2. Data protection of employees – main considerations

Principles of transparency, lawfulness and purpose limitation established by the CFREU and the GDPR are especially pronounced in the context of employee data protection. According to Article 88 of the GDPR, Member States may adopt laws and collective agreements in order to provide for more specific rules when it comes to processing employees´ personal data. In that regard the national laws and collective agreements may put higher standards for the protection of employees´ data then GDPR. However, they cannot regulate what is below the minimum[14] of data protection enshrined by the GDPR. The Member States have the obligation to notify the European Commission (`EC`) about such provisions of the laws adopted with regard to Article 88. In that regard Austria has notified the EC on 27 June 2018 about the adoption of new provisions of laws within the jurisdiction of the Federal Ministry for Labour and Social Affairs, Health, Care and Consumer Protection Rights.[15]

Having in mind that the GDPR has given the Member States the right to regulate this issue in their national laws and collective agreements, legal diversity in the area of the data protection of employees is inherent in the EU. The practical approach to the issues of duration of keeping various data and documents of employees, legal grounds of processing those data, data that are processed mainly on the grounds of compliance with a legal regulation or of fulfilling contractual obligations or eventually on the grounds of consent[16] pursuant to Article 6 of the GDPR, are to be provided by national laws and collective agreements.

In Austria, issues of labour law have been regulated through very detailed net of specific laws and collective agreements. Collective bargaining has a tradition in Austria and a strong legal base where various branches have come to collective agreements often giving employees more benefits than laws. Provisions of data protection of employees stem out also from other laws covering not primarily labour law, for example Federal Tax Code which provides for a seven year time limit of keeping documents for tax purposes[17]. Having in mind

[13] Currently, possibilities are discussed at the Salzburg Land, of requiring the new employees to nursing homes, kindergartens, and alike, to receive COVID-19 vaccine (see for example https://www.diepresse.com/5907893/land-salzburg-ohne-impfung-keine-anstellung).

[14] See Sharma, Data Privacy and GDPR Handbook, Wiley, 2020, p.311.

[15] https://ec.europa.eu/info/sites/info/files/at_notification_art_88.3_complement_publish.pdf.

[16] One has to bear in mind that in the scope of working relation consent has to carefully applied due to the unequal nature of relation between the employer and employee and the question of existence of ´freely given` consent.

[17] § 132 Federal Tax Law, (Bundesabgabenordnung).

the complexity of national regulation of labour law issues, it is very demanding and complex to define certain institute of labour law in the light of the data protection of employees throughout the EU.

3. Timeframes of data protection of employees

In order to analyse the problem of data protection of employees, with a view to the time of occurring of data processing/controlling, we may examine data protection before, during and after the employment in the course of normal processing of data within labour contractual and legal obligations.

In this context it is worth noting that the GDPR has widened the notion of employee to the period preceeding employment and to the period after the employmenet, in order to provide for a thorough protection of data of employees.

3.1. Data protection in recruitment procedure

Recruitment procedure is the first instance where employer deals with personal data of a prospective employee. Personal data given by the candidate to the prospective employer, may include, apart from basic information, such as the name, address, age, also data which the candidate choses to share, such as religious belief, sometimes visible also in school certificates that are appended to a job application, membership to a trade union, or even health issues, when the candidate wishes to point out the physical readiness for a physically demanding job, or even submits a corresponding medical opinion. In that regard we come to the sphere of special categories of data (religious belief, membership to a trade union, health information) which should, as sensitive data, be dealt according to Article 9 of the GDPR. However, when it comes to explicit consent, as one of the grounds for processing/controlling sensitive data, Article 29 Party has contended that it is ´highly unlikely that legally valid explicit consent can be given´ since employees are not considered ´free´ to give such consent due to unequal legal relation between employer and employee. Although in the case of pre-employment the employee and employer are not yet in a labour relation, and employee is not yet financially dependent upon employer, one should have in mind that expected employment still deprives to a significant extent the explicit consent of its free will, and should be avoided as a grounds for processing/controlling special data. As regards other data, inherent in recruitment procedure, the employer should offer the candidate a choice of consenting to the retention of his/her data for a certain time after the application proceedings were finalized, or what is even better, rely on a legal ground for retention if there is one, when such proceedings had not been successful for the candidate. Moreover, Article 29 Party recommends the deletion of data as soon as it is clear that an offer of employment will not be made or it is not accepted by the candidate.[18] Also according to Article 5, para. 1 (e) of the GDPR personal data are to be kept ´for no longer than is necessary for the purposes for which the personal data are processed´. But, according to decision of Austrian Data Protection Authority Decision[19] in the case of a non recruiting, a 6 month time limit is to apply (seven months from the receipt of job application) having its legal base in Law on Equal Treatment[20]. Of course, the candidate can at any time request the erasure of data with a view to Article 17 of the GDPR.

3.2. Data processing during employment

The second period, which covers formal employment of the employee, is regulated by national labour laws and collective agreements which therefore make the ground for processing the personal data of the employees. Types of data processed and controlled include the usual data that are part of the employment contract, such as

[18] Opinion 2/2017 on data processing at work, Article 29 Party, of 8 June 2017, p. 11.

[19] Decision of the Austrian Data Protection Authority, GZ: DSB-D123.085/0003-DSB/2018 of 27 August 2018.

[20] § 29, para. 1 of the Law on Equal Treatment (Gleichbehandlungsgesetz).

name, address, bank account, social security number, but also data which are necessary for the payroll process such as marital status, number and age of children, address in the light of calculating distance between place of living and work, data of whether the marital spouse or partner is employed and if so upper limit of his/her earnings etc. However, the payroll system may also include special personal data such as data on sick leave which have to be dealt with according to Article 9 of the GDPR and national law.

The grounds for processing and controlling employee data during employment should be fulfilling of legal or contractual obligation or legitimate interest by the employer and not consent nor explicit consent due to presumption of non-existence of a free will at the consent, which must be freely given, in labour relation between the employee and employer, in which employee is financially dependent upon employer. Accordingly, processing of personal data of employees is regulated by labour laws and collective agreements.

Beyond formal and legal prerequisites, employees should feel safe that their data is handled with care and that that their personal information is kept secure within the organisation.[21] This is important both from the aspect of feeling legal certainty and confidence in relationship between employee and employer.

3.3. Data keeping after the employment

The third period, after the formal employment has ended, relates to the employer keeping the employee data. In that regard the former employee has the right to access to his/her data according to Article 15 of the GDPR. The employer should also strive not to keep data beyond from what was prescribed by law or collective agreement. For example, in Austria the time-limit for keeping employee´s certificate of employment is 30 years[22].

4. Personal communications

Monitoring of personal communications at the workplace is one of the most direct intrusions into employees´ privacy and according to Article 29 Party main threat thereto[23].

Where is the border between private and professional? Do employees have a right to private sphere during their working time? In the Copland v. the United Kingdom case, the ECtHR stated that e-mails sent from business premises could be a part of an employee´s private life and correspondence and that collection of such information without the knowledge of employee is interference with the employee´s rights.[24]

The communication of an employee is one aspect that should be subject to protection of privacy. As the Article 19 Working Party pointed out, the employee does not leave its privacy at the door when coming to his/her workplace[25]. The ECtHR has included communication into the sphere of private life by its judgment of Niemitz v. Germany[26]. However, the communication, especially in the fast-growing information technology sphere may be easily open to interference by employers.

In the case of Barbulescu v. Romania of 2016[27], the question arose of whether an employer is entitled to look into his employee's private messages. The messages were written by the employee during the working time, at the computer owned by the employer, were he exchanged messages with his fiancée on his private Yahoo Messenger account, and the employer has made a transcript thereof. The ECtHR has noted that the employer did not warn the employee of the possible monitoring, although the company had adopted internal rules pro-

21 Gupta, Handbook of Research on Emerging Developments in Data Privacy, IGI Global, 2015, p. 78.
22 § 1163 and 1478 of the General Civil Code (Allgemeines bürgerliches Gesetzbuch).
23 Opinion 2/2017 on data processing at work, Article 29 Party, of 8 June 2017, p. 12.
24 Judgment of the ECtHR in the case of Copland v. United Kingdom, 3 April 2007.
25 Working document on the surveillance of electronic communications in the workplace, Article 29 Party, p. 4.
26 Judgment of the ECtHR in the case of Niemitz v. Germany, of 16 December 1992.
27 Judgment of the ECtHR in the case of Barbulescu v. Romania, issued on 6 June 2016.

hibiting the use of office computers for private purposes. The ECtHR has found no violation as the employee, Mr. Barbulescu, could not have had ´expectation of privacy´ in such circumstances.

However, the ECtHR has departed from its opinion in the Grand Chamber judgment[28] finding a violation of Article 8 of the ECHR and providing for standards which had to be respected in order that Article 8 is complied with. These principles are a certain compromise when it comes to protecting the right of online privacy of employee and at the same time respecting the right of employers to restrict the use of electronic communications for private purposes during work hours. Standards[29] which have to be taken into consideration are clear and in advance notification to employees of possible monitoring by the employer, the extent of monitoring and degree of intrusion into the employee´s privacy, any legitimate reasons by the employer to justify the monitoring, existence of less intrusive methods, consequences of monitoring, the existence of adequate safeguards to employees.

Article 29 Party contends that loosing employee´s expectation of privacy does not lead to non-violation of privacy, and it does not find advance warning sufficient to justify any infringement of their data protection rights.[30]

Having in mind the above, the question of monitoring employees´ communications is very sensitive, and not a single justification is enough to legitimise it, but a list of conditions must be thoroughly fulfilled by the employer if he/she recourses to such a measure. In that regard one should have in mind the attitude of the Article 29 Party that ´prevention should be more important than detection´[31] encouraging employers to use technology measures to prevent employees to misuse the Internet as well as to open for them apart from professional e-mail account, also private account, in order that circumstances surging monitoring are prevented at the outset.

What is even more important are the negative consequences of any such monitoring to human dignity of a worker, and negative effects[32] that it brings to relationship between the employee and employer, which is often irreparable.

Accordingly, the monitoring of communications should be generally avoided, and prevented not only by technology measures but by building a trustful relationship between the employee and employer which would be to a mutual content. Legitimate claims of employees to privacy at work are also to be balanced with employers´ interests.[33] Although the monitoring is not absolutely prohibited neither by ECHR nor by GDPR, it should be used only as a last resort with all the safeguards thoroughly applied, and again exceptionally when no less intrusive methods are available.

5. Video surveillance

Another direct interference into employees´ privacy includes video surveillance, which has been dealt by the ECtHR as well as by Article 29 Party / EDPB.

In the case of Spanish supermarket chain, the employees, Ms Lopez Ribalda and four other employees, were monitored with covert CCTV while working at their cash registers, because the employer had a doubt that some or more of the employees were making frauds at their working places, as discrepancies in stocks and profit were noticed. In this case the ECtHR has issued two judgments, the first one in 2018[34], and the second

[28] Judgment of the ECtHR in the case of Barbulescu v. Romania, issued on 5 September 2017.
[29] Cosabic, The Right to Online Privacy Unfolding – Barbulescu Final Judgment, moderndiplomacy.eu, 2017
[30] Working document on the surveillance of electronic communications in the workplace, Article 29 Party, 29 May 2002, p. 8, 9.
[31] Ibid, p. 4.
[32] Ibid, p. 6.
[33] Sven Ove Nansson, Elin Palm, The Ethics of Workplace Privacy, P.I.E. Peter Lang S.A., 2005 p. 110
[34] Judgment of the ECtHR in the case of López Ribalda and Others v. Spain, issued on 9 January 2018.

one by the Grand Chamber in 2019[35]. In the first judgment the ECtHR has contended that the covert video surveillance was not aimed directly at the applicants in this case but at all the staff working on the cash registers, and that video monitoring was carried out without any time limit and during all working hours. The ECtHR has concluded that the employer in this case failed to ´previously, explicitly, precisely and unambiguously inform those concerned about the existence and particular characteristics of a system collecting personal data.´ The ECtHR has also criticized the failure of employer to inform the applicants of the installation of a system of video surveillance, at least generally. However, the Grand Chamber of the ECtHR has rendered a different judgment, finding no violation of Article 8. In this instance the ECtHR contended that although there was no time-limit of surveillance, it lasted for 10 days. Further, it was performed in a public space where expectation of privacy was lower then for example in private spaces such as toilets. The ECtHR did note the lack of transparency, in not informing the employees of the surveillance, indicating that in such a case the justification on the side of employer must be strong, which was present in this case due to suspicion of joint action by several employees. It has also importantly noted that a lower grade of suspicion on the part of employees could not justify the installation of covert video-surveillance by an employer.

In an earlier case of Köpke v. Germany[36] the ECtHR has come to a similar decision but opened the possibility of a different standing in the future, having regard to possible intrusions into private life by new, more sophisticated technologies.

In that regard the Article 29 Data Protection Working Party has drawn attention to the application of technology in the employment context which enable to collect data remotely, reduction in the cameras´ sizes, and the possibility of employer to monitor the worker´s facial expressions, to identify patterns, which it found to be generally unlawful, and likely to involve profiling and automated decision-making. While it gave a slight possibility for borderline exceptions, the use of such technology cannot be in general considered legitimate.[37] An employee, as noted by EDPB, in his/her workplace is not likely expecting to monitored by his or her employer[38], and the level of expectation of privacy was also highlighted by the ECtHR as important factor for determining violation of privacy.[39] Moreover, if we extend the notion of the place of work to home office, which has been especially pronounced during the Corona pandemic, surveillance processing would be disproportionate and according to Article 29 Party the employer is very unlikely to have a legal ground, for example, for recording an employee´s keystrokes and mouse movements[40], and let alone video surveillance.

According to GDPR, as video surveillance involves processing of personal data, the principle of transparency should be observed, in that persons that could be under the CCTV monitoring must be informed of the installation of cameras, at least by a visible CCTV sign. The first fine issued by the Data Protection Authority in Austria in September 2018[41], was related to a café in Graz, which had a camera installed over a public area in front of the entrance to the café, inter alia, due to lack of a sign of CCTV which would warn the pedestrians about the possibility of video surveillance.

Moreover, data obtained through surveillance may according to GDPR be considered as biometric data[42], often enabling for unique recognition of a person monitored, through facial recognition or even gait, and thus be dealt with as special category of data under Article 9 of the GDPR.

35 Judgment of the ECtHR in the case of López Ribalda and Others v. Spain, issued on 17 October 2019.

36 Judgment of the ECtHR in the case of Karin Köpke v. Germany, issued on 5 October 2010.

37 Opinion 2/2017 Article 29 Working Party, p. 19.

38 Guidelines 3/2019 on processing of personal data through video devices, European Data Protection Board, adopted on 10 July 2019, p. 11.

39 In Barbulescu case for example.

40 Opinion 2/2017 on data processing at work, Article 29 Party, of 8 June 2017, p.16.

41 https://edpb.europa.eu/news/national-news/2018/first-austrian-fine-cctv-coverage-summary_de.

42 Ustaran, European Data Protection Law and Practice, IAPP, 2018, p. 286.

Article 29 Party / EDPB seem to have stronger standing when it comes to video surveillance of employees then the ECtHR, leaving little space for exceptions. The GDPR itself, by considering data obtained through surveillance, under certain conditions, as biometric data, does not seem inclined towards the use of video surveillance. However, we must bear in mind that in this area, a great role is played by information technology growth and raise of its sophistication in unique recognition of persons, what the ECtHR has also indicated in Köpke case above, which would also have to raise a legal protection.

6. Conclusions

The protection of employee data is a complex and sensitive issue, even more as the GDPR has authorised the states to regulate this issue by their national laws and collective agreements. It requires thorough protection starting from the issues of payroll data which are processed on everyday basis, to issues of direct intrusions into employees´ privacy which becomes more exposed with the growth of sophistication of technology, therefore requiring corresponding legal protection which has to go hand in hand with such a growth. The ECHR system with its ECtHR case-law is a valuable resource giving states, employers and legal scholars necessary interpretation for all future dealings in similar cases. On the other hand, GDPR directly and also through national regulation, provides for specific steps that employers have to undertake on a daily basis in order to protect employees while processing their personal or even special personal data. Failing to do that, they may face with rigorous penalties, urging them to always be in line with GDPR requirements. Both systems, though different, provide for a high level of protection of privacy and private data of employees.

7. Literature

Cosabic, Jasna, Right to be Disconnected – The Wave to Catch On, The Political Anthropologist, 2017.

Cosabic, Jasna, The Right to Online Privacy Unfolding – Barbulescu Final Judgment, moderndiplomacy.eu, 2017.

Ford, E., Karen/Notestine, E., Kerry/Hill, N., Richard, Fundamentals of Employment Law, American Bar Association, 2000, p. 449.

Gupta, Manish, Handbook of Research on Emerging Developments in Data Privacy, IGI Global, 2015, p. 78.

Nansson, Ove, Sven/Palm, Elin, The Ethics of Workplace Privacy, P.I.E. Peter Lang S.A., 2005 p. 110.

Sharma/Sanjay, Data Privacy and GDPR Handbook, Wiley, 2020, p.311.

Ustaran, Eduardo, European Data Protection Law and Practice, IAPP, 2018, p. 286.