General Data Protection Regulation (GDPR): Legal, Ethic and Other Issues, Especially in Covid-19 Time

Submitted: 11.04.2021
Revised: 27.05.2021
Accepted: 07.07.2021

Article submitted to peer blind review

Ana Isabel Guerra*
ORCID: https://orcid.org/0000-0002-4579-9579
Maria João Machado**
ORCID: https://orcid.org/0000-0002-0196-232X
Maria Malta Fernandes***
ORCID: https://orcid.org/0000-0003-1857-1488
Patrícia Anjos Azevedo****
ORCID: https://orcid.org/0000-0002-0779-9076
Sérgio Tenreiro Tomás*****
ORCID: https://orcid.org/0000-0003-1017-6467
Susana Sousa Machado******
ORCID: https://orcid.org/0000-0001-8434-2398

DOI: https://doi.org/10.26512/lstr.v13i2.37425

Abstract

[Purpose] This paper intends to present an academic analysis about the legal, ethic and other issues raised by the General Data Protection Regulation, especially in Covid-19 time. In this context, we present the main legal aspects of networked privacy, online privacy literacy, transparency, data integrity and others. Besides, we present the employee´s rights in the context of the Covid-19 pandemic, such as the right to erase data, temperature monitoring, the employee´s consent, the legitimation of the processing of personal data and body temperature control. We also give a word about data protection and teleworking. Our purpose is to contribute for the evolution of law, regarding the challenges and all the changes in our daily-life, provoked by the Covid-19 pandemic.

[Methodology] Our objectives are fundamentally achieved with a legal and doctrinal analysis, which is our methodology. The topics presented in this paper are linked between each other and this kind of joint treatment is our goal.

[Findings] Privacy is a broad concept that includes a set of personal characteristics that go beyond a user's name and location. Personal data includes the fundamental rights that privacy helps to guarantee. The GDPR is a legal basis for the processing of personal data, which is directly applicable in the European Union and does not require national transpositions. Employers are facing increasingly complex challenges in the day-to-day of their companies, given the need to stop the spread of coronavirus. To respond to the

*Invited Professor, ESTG/P. Porto. Address: ESTG – Rua do Curral, 4610-156 Margaride (Santa Eulália), Felgueiras, Porto, Portugal. E-mail: aimg@estg.ipp.pt.
**Professor, ESTG/P. Porto and Member of CIICESI. E-mail: mjm@estg.ipp.pt.
***Professor, ESTG/P. Porto. E-mail: mdf@estg.ipp.pt.
****Invited Professor, ESTG/P. Porto and Member of CIICESI. E-mail: pamv@estg.ipp.pt.
*****Professor, ESTG/P. Porto and Member of CIICESI. E-mail: smt@estg.ipp.pt.
******Professor, ESTG/P. Porto and Member of CIICESI. E-mail: scm@estg.ipp.pt.

growing threat of coronavirus, many employers are considering monitoring the health of their employees to minimize the risk of infection and contagion in the workplace. Consent as a free, informed and unequivocal manifestation, required by the GDPR, collides with the existing asymmetries in the employment relationship. Despite all the difficulties in framing consent, it is unequivocal that the employment relationship requires the collection and processing of numerous employee data. It is an inevitability. Teleworking, provided from the employee's home, was one of the first measures adopted in the context of the pandemic caused by the Covid-19 disease. This type of work provision raises a number of questions regarding the protection of employees' personal data, namely in terms of control by the employer.

Keywords: General Data Protection Regulation. Networked Privacy. Employee´s Rights. Telework. Covid-19.

INTRODUCTION

The EU's General Data Protection Regulation (GDPR) has entered into force on 25 May 2018 – Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. The Article 99 of GDPR under the heading «entry into force and application» refers to

> "This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union", "It shall apply from 25 May 2018" and "This Regulation shall be its entirety and directly applicable in all Member States".

The GDPR is a legal basis for the processing of personal data, which is directly applicable in the European Union and does not require national transpositions. As such, it will facilitate the harmonization of legal regimes for the protection of personal data in Europe. Better yet, the GDPR has a principle of extraterritoriality that allows, in certain circumstances, to extend its scope beyond European borders.

According to Mondschein and Monda (2019),

> "although GDPR has the objective of introducing harmonization of data protection law throughout European Union, the fact that it contains a substantial number of opening clauses which create space for Member States to take decisions on the implementation of the GDPR at national level may undermine this attempt" (MONDSCHEIN; MONDA, 2019).

Scope of Application

The General Data Protection Regulation contains guidelines regarding the protection of natural persons when their personal data are processed and rules relating to the free movement of personal data (Article 1). It also states that the GDPR seeks to protect fundamental rights and freedoms of natural persons and, more specifically, their right to the protection of personal data.

The analysis of its scope will be divided into two parts: material scope (what types of processing of personal data the regulation applies?) and territorial scope (where do persons and organizations have to be located in order to be obliged to observe the regulation?). Article 2 governs the material scope and Article 3 governs the territorial of the GDPR.

Material Scope

Regarding the material scope, it can be said that the regulation applies to the processing of personal data completely or partly by automated means, such as, for instance, carried out with the use of computers containing digital databases. Moreover, the processing of personal data by any other means is also regulated by the GDPR when that data is included in a file system or are intended to be used in the file system, in accordance with Article 2(1). Examples include collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure, erasure, or destruction.

As stated by Mondschein and Monda (2019), the GDPR applies to both public bodies as well as private organizations, but exist distinct rules for the European Union institutions, bodies and agencies [Article 2(3)] (MONDSCHEIN; MONDA, 2019).

There are also a number of situations that are not covered by the GDPR and are listed in Article 2(2) of the GDPR. It is the case for example of the situation in which a natural person exercise of exclusively personal or domestic activities or performed by the competent authorities for the purpose of prevention, investigation, detection and prosecution of infractions criminal offenses or the enforcement of criminal sanctions, including safeguarding and preventing threats to public security.

Territorial Scope

As regards territorial scope of the application of the GDPR, three aspects must be addressed (Article 3).

The Regulation applies to the processing of personal data by controller or processors with an establishment in the European Union, regardless of whether the processing takes place in the Union or not [Article 3(1)].

Mondschein and Monda (2019) highlight that the applicability of the GDPR is not linked to nationality of a Member State or to European Union

citizenship but applies to all data subjects located within the Union (MONDSCHEIN; MONDA, 2019).

Secondly, according to Article 3(2), the Regulation is applicable when controllers and processors are not established in the European Union but process personal data of individuals who are in the Union. In that case, processing activities must be related to the offering of goods or services for a payment or for free to these individuals or to the monitoring of the behavior of these persons as far as this behavior takes place in the European Union.

Finally, and thirdly, the GDPR regulates the processing of personal data by controllers that are not established in the Union but somewhere else where laws of a European Union Member State apply by virtue of public international law, such as, diplomatic missions.

Notions of Personal Data and Processing

The GDPR has as its main objective the protection of personal data of natural persons. Considering that this protection is a fundamental right, regardless of nationality or place of residence, there is a contribution to security and justice with the objective of economic and social union of citizens in the European area. Basically, it is not only the defense of the fundamental rights of natural persons that is at stake, but also the free movement of personal data between the member states of the European Union.

In this context, let us say that the GDPR has a dual basis: on the one hand, it aims to facilitate the free flow of personal data; on the other hand, it serves to better protect the fundamental rights of individuals, with a focus on the right to privacy and data protection. In fact, the right to the protection of personal data is part of the European Union Charter of Fundamental Rights (European Union, 2012) - Article 8 of de Charter (2000/C 364/01) clearly states that "everyone has the right to the protection of personal data concerning him/her" (CRUTZEN, PETERS and MONDSCHEIN, 2019).

The GDPR in its Article 4, paragraph 1 defines personal data as

> "any information relating to an identified or identifiable natural person ('data subject')" and adds that "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".

Personal data is all information about a specific individual that can be identified directly or indirectly, in terms of his or her private or professional life.

The scope of personal data includes genetic data, relating to physical or mental health or biometric data, that is, specific technical treatments relating to physical characteristics, information about a person's physiology or behavior that may determine his identification.

The GDPR also defines a specific category of personal data: sensitive data. This category includes information such as that relating to political ideology, religious beliefs, pregnancy, sexual orientation, among others.

NETWORKED PRIVACY, ONLINE PRIVACY LITERACY, TRANSPARENCY, DATA INTEGRITY AND OTHER ISSUES

The growth of online business and trades in the internet made a huge revolution in data protection. In the last years, the traditional position of Europe can be reached in the way that the old continent protects data and privacy in the web environment. We clearly saw that protection in the cookies policy implemented in the web to protect the dates of whom needs to navigate in the web is a common and concerted work in all of European Union. All the users need to accept cookies to access to websites and see all kind of contents.

Instead, in US data protection policy, each entity makes this management individually. Despite their differences both, the United States and Europe try to organize reliable and credible protection systems given the sensitivity of the data to be protected. Privacy and anonymity of all web users must be controlled by themselves and it is not tradable in bulletin board systems, videotext, online services and web browsers.

Although Lisbon Treaty in Article 8, had gave to all European countries the principles for a common data protection policy, a global policy should be promoted. There must be an evolution of authentication and control practices that are universally adapted to all regions of the world (JONES; ACKERMANN, 2020).

Privacy should be seen as a broad concept that includes a set of personal characteristics that go beyond a user's name and location. Personal data includes the fundamental rights that privacy helps to guarantee. These rights must prevail over the economic interests of large groups and institutions worldwide. The behavior on the web by those who manage this data must be guided by a non-intrusion in the reservation of the privacy of any user. Users do not have their own mechanisms to protect themselves and are therefore the weakest and most exposed to the potential misuse of their personal data. Creating a faultless protection system is almost an impossible task. However, this system must be reliable and not illusory, allowing the user to obtain all the sufficient information to decide whether or not to give up any of their data, as well as the extent and exact measure of that transfer according to their free and personal choices. The data protection

policy on the web must be multidimensional so that users can critically appreciate what they are allowing and know how to act if any of the permissions they give regarding their personal data are exceeded or disrespected, being aware of the risks that the authorizations it gives support. So, the more informed users are, the more protected they will be (MASUR, 2020).

Most processes for processing personal data are unclear. Many users are faced with texts, authorizations and permissions to use their personal data unintelligible to ordinary people due to their elaborate technical and legal language. More and more personal data of the web users are tradable and personal databases are considered as valuable assets for most companies. Web users should be alert to protect their personal data on the internet in the same way that they protect them in the real world beyond the screen (BETZING et. al., 2020).

If personal data is subject to terrorism, its use or modification can cause severe damage to its holders. Given the unpredictability of attacks on personal data, their protection must be ensured by those who make them available and those who use them (KUMAR et. al., 2020).

EMPLOYEE'S RIGHTS UNDER THE EUROPEAN UNION'S GENERAL DATA PROTECTION REGULATION (GDPR) IN THE CONTEXT OF THE COVID-19 PANDEMIC

Article 88 of the GDPR opens the door for EU Member States to establish, in their legal system or in collective agreements, more specific rules to guarantee the defense of rights and freedoms with regard to the processing of personal data of employees in the labour context.

Notwithstanding this possibility, Article 9 of the GDPR determines the prohibition of the processing of personal data that reveal data related to health, unless:

- The treatment is necessary for the purposes of preventive medicine or work for the assessment of the employee's ability to work, provided that his data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy or by another person equally subject an obligation of confidentiality (Number 2, H and Number 3);
- Treatment is necessary for reasons of public interest in the field of public health, such as protection against serious cross-border threats to health, under appropriate and specific measures that safeguard the rights and freedoms of the data subject, in particular professional secrecy – Number 2, I).

In this way, there is the possibility of the processing of employee data by the employer concerning a possible diagnosis of Covid-19, whenever some of the reasons listed justify it.

The Right to Erase Data

The right to erase data or the "right to be forgotten" may be relevant in the employment law relationship. In this sense, Article 17 of the GDPR determines that the employee has the right to erase his personal data, without undue delay, by the employer and he has the obligation to delete the personal data without undue delay, when some of the reasons mentioned there, highlighting the situations in which personal data are no longer necessary for the purpose that motivated their collection or treatment.

Article 17 provides in its Number 3, C that the right to erasure does not apply when they are necessary for reasons of public interest in the field of public health. In this way, the employee who suffers or has suffered from Covid-19 disease, can only request the deletion of this data as long as the said interest no longer justifies its existence.

In turn, Article 23, of the same legal document, determines that the law of the Union or of the Member States, to which the data controller of the employee is subject, may limit, by legislative measure, the scope of the right erasure, provided that such limitation respects the essence of fundamental rights and freedoms and constitutes a necessary and proportionate measure to ensure, inter alia, important objectives in the general public interest of the Union or a Member State in the fields of public health – Number 1, E).

Temperature Monitoring in a Pandemic Context

Employers are facing increasingly complex challenges in the day-to-day of their companies, given the need to stop the spread of coronavirus. To respond to the growing threat of virus, many employers are considering to monitor the health of their employees to minimize the risk of infection and contagion in the workplace.

The employment relationship requires the treatment of many personal employee data. The GDPR also applies to employment relations where the employer processes personal data of employees, within the meaning of Article 4 (1). There are several data that can be the target of such treatment, including sensitive personal data such as biometric data, health data, genetic data, etc.

In the context of a pandemic, on the one hand, and the enhancement of data protection, on the other, a question arises: can the employer measure the temperature of employees as a way of reducing infections? In fact, the human body temperature measurement was considered a mechanism to reduce the risk of infection (WU, et al., 2020).

The EU Member States supervisory authorities in relation to body temperature measurements in the COVID-19 context have provide guidance, but there are divergent points of view, depending on the national law (AIDINLIS, 2020). These divergences are also highlighted in a comparative study carried out by Böröcz and Gkotsopoulou (BOROCZ; GKOTSOPOULOU, 2021).

The Employee's Consent

Firstly, it is clear that the data obtained through this measurement is sensitive data, in accordance with Article 9 (SHABANI, 2020). As a consequence, the rule will be that these data cannot be processed without the consent of the data subject, which does not apply to the employment relationship (ŠVEC, 2018).

Employers who seek to rely on consent should pay attention to the fact that, in the employment context, consent is often considered invalid due to the imbalance of power between the parties. In order to solve this problem, it is important to start with the analysis of Recital 43, which states that:

> "consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller".

This is certainly the case in the employment relationship in which there is an imbalance between the parties and, therefore, for the employer to be able to process employee data, mere employee consent is not enough.

Consent as a free, informed and unequivocal manifestation, required by the GDPR, collides with the existing asymmetries in the employment relationship. Consent of the data subject is understood as

> "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" (Article 4 (11)).

The definition of consent is completed by Article 7, which states that

> "where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data" (1) and "when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract" (4).

Therefore, it is considered that, in the labour field, consent has little relevance, since the employee is in an unequal position in relation to the person

responsible for the treatment, this is, the employer. In this relationship, it is not possible to consider a freely given consent when consent itself is a requirement for maintaining the job. The employee has no real freedom of choice.

Legitimizing the Processing of Personal Data

Despite all the difficulties in framing consent, it is unequivocal that the employment relationship requires the collection and processing of numerous employee data. It is an inevitability.

The solution will be to legitimize the processing of personal data, not through the employee's individual consent, but through the principle of legitimacy and the pursuit of specific purposes, respecting the principle of proportionality (MOREIRA, 2020). Thus, even in cases where the employee has given consent, the treatment must be relevant, necessary and respect a lawful purpose.

However, the GDPR clearly provides for situations in which data processing is possible, of which we highlight:

> "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" (Article 9(2) B)

> "processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3" (Article 9(2) H.

Such conditions and guarantees are that the

> "personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy." (Article 9 (3)).

Body Temperature Control

From what has been said previously it seems possible to carry out tests for employees to control body temperature, but only in certain circumstances. It is known that the employer has a duty to protect the employee's safety and health and that, on the other hand, the employee has to respect the imposed rules. It is

also noted that according to Article 88, Member States may lay down rules specifically applicable legal to each national legal system.

The European Data Protection Supervisor issued orientations on the use of body temperature checks by Union institutions, bodies, offices and agencies (EUIs) in the context of the COVID-19 crisis, emphasizing that a careful assessment and appropriate data protection safeguards are necessary (EDPS, 2020). The guidance provided by the European Data Protection Supervisor on September 1, 2020, asserts that

> "systems of temperature checks, operated manually and followed by registration, documentation or further processing of an individual's personal data, or systems operate d automatically with advanced temperature measurement devices would, in general, fall under the scope of the Regulation" (EDPS, 2020).

As Suder's study analyses,

> "national data protection authorities seem to look for a reasonable and pragmatic approach regarding compliance with the GDPR in light of the Covid-19 emergency. However, their guidance differs in several areas and the views in between nation states are not always aligned. A more specific, clear and uniform pan-European vision concerning the processing of employees' data in times of emergency is needed to better protect employees and limit the spread of the virus" (SUDER, 2021).

The main question in this matter is related to the modus operandi of these tests. How is it done? In what way? By whom? We do not think it is possible to find a basis for banning the body temperature measurement. Doubts focus on how it is done and by whom it is done.

The measurement of body temperature cannot violate the right to individual data protection, that is, it can only be performed by health professionals, or under their guidance, and always subject to professional secrecy. As regards health data, this treatment must always respect certain principles:

- **Principle of Purpose Limitation:** to be used only for the protection of the health and safety of employees and third parties;
- **Principle of Proportionality:** to be carried out only by health professionals or under their supervision;
- **Principle of Transparency:** to obey clear rules on treatment, registration and erasure.

Finally, it should be noted that Article 17, which concerns the right to data erasure, provides that these data must be erased when the reasons for the treatment no longer exist.

Regardless of the national legal context on which it is based, employers always need to ensure that they comply with data protection principles, as with any treatment of personal data. The data minimization and purpose principles are particularly relevant when considering body temperature measurement. Despite all the difficulties, we could conclude that it is possible to measure the body temperature of employees while respecting data protection.

Data Protection and Teleworking

Teleworking, provided from the employee's home, was one of the first measures adopted in the context of the pandemic caused by the Covid-19 disease. This type of work provision raises a number of questions regarding the protection of employees' personal data, namely in terms of control by the employer.

Despite the power to control the employee, the employer cannot use means of remote surveillance (be it computer software programs or the computer's video camera), measures aimed at protecting the safety of people and property, with the purpose of controlling the employee performance. Access to the employee's personal data, the invasion of his privacy sphere, conflict with the principles set out in Article 5 of the GDPR:

> "personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject" and "(b) collected for specified, explicit and legitimate purposes".

However, the control of the employee is still necessary (of attendance, compliance with the schedule, carrying out the work), and it is possible, provided that through computer programs that comply with all the requirements of the processing of personal data, having the responsible for the treatment (the controller) to ensure that

> "both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measure [and that,] by default, only personal data which are necessary for each specific purpose of the processing are processed" (Article 25 GDPR).

The employee (the data subject), on the other hand,

> "shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data"

and to a set of information and data rights (Articles 15 to 22 GDPR).

If the employer does not have the appropriate technological resources, he can always determine that the employee communicates the start and end times of the work, by email or telephone (CNPD, 2020), as well as can regularly schedule meetings with him to evaluate the work, which may also constitute an important measure to break the isolation to which teleworking votes the employee.

CONCLUSION

Privacy should be seen as a broad concept that includes a set of personal characteristics that go beyond a user's name and location. Personal data includes the fundamental rights that privacy helps to guarantee. These rights must prevail over the economic interests of large groups and institutions worldwide.

The GDPR is a legal basis for the processing of personal data, which is directly applicable in the European Union and does not require national transpositions. Article 88 of the GDPR opens the door for EU Member States to establish, in their legal system or in collective agreements, more specific rules to guarantee the defense of rights and freedoms with regard to the processing of personal data of employees in the labour context.

The right to erase data or the "right to be forgotten" may be relevant in the employment law relationship.

Employers are facing increasingly complex challenges in the day-to-day of their companies, given the need to stop the spread of coronavirus. To respond to the growing threat of virus, many employers are considering monitoring the health of their employees to minimize the risk of infection and contagion in the workplace.

Consent as a free, informed and unequivocal manifestation, required by the GDPR, collides with the existing asymmetries in the employment relationship. Despite all the difficulties in framing consent, it is unequivocal that the employment relationship requires the collection and processing of numerous employee data. It is an inevitability. Consent is not enough to legitimize the processing of an employee's personal data due to the lack of balance of power between the employee and the employer. Thus, free consent is not possible on the part of the employee in this scenario, and the solution offered in the work is the need to respect the principles of processing of employee data, such as proportionality.

Concerning body temperature control of the employees, there is a legal basis for its implementation by the employers, but highlights the importance of respecting data protection rights and principles, more precisely: purpose limitation, proportionality, and transparency.

As for teleworking, it raises a number of questions regarding the protection of employees' personal data in terms of control by the employer. The answer to that would be the implementation of appropriate control techniques that respect the principles and rights guaranteed by the GDPR. In fact, teleworking, provided from the employee's home, was one of the first measures adopted in the context of the pandemic caused by the Covid-19 disease. This type of work provision raises a number of questions regarding the protection of employees' personal data, namely in terms of control by the employer.

REFERENCES

AIDINLIS, S. The EU GDPR in Times of Crisis: COVID-19 and the Noble Dream of Europeanisation, *Journal of European Consumer and Market Law* 9(4), 2020.

BETZING et. al. The impact of transparency on mobile privacy decision making. *Eletronic Markets*, 30, p. 607-625, 2020.

BOROCZ, I.; GKOTSOPOULOU, O. Between masks and curfews: Critical synopsis of the guidance issued by national supervisory authorities on analogue and digital body temperature measurement in the context of the COVID-19 pandemic in the EU, *PinG* 1/2021.

COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS (CNPD). *Orientações sobre o controlo à distância em regime de teletrabalho*, 2020.

CRUTZEN, R., PETERS, G. J. Y. & MONDSCHEIN, C. F. Why and how we should care about the General Data Protection Regulation, *Psychology & Health*, 34(11), p. 1347-1357, 2019.

EUROPEAN DATA PROTECTION SUPERVISOR. *Body temperature checks by EU institutions:* Careful assessment and data protection safeguards are necessary, 2020.

JONES, M. L. & ACKERMANN, K. Practicing privacy on other networks: network structures, economic arrangements, and identity strategies before cookies, *Internet Histories*, 2020.

KUMAR et. al. A wake-up call for data integrity invulnerability. *Computer Fraud &Security*, 2020.

MASUR, P. K. *Online privacy literacy, self data protection and self-determination*, 2020.

MONDSCHEIN, C.F., MONDA, C. The EU's General Data Protection Regulation (GDPR) in a Research Context, in: Kubben P., Dumontier M., Dekker A. (Eds.) *Fundamentals of Clinical Data Science*. Springer, 2019.

MOREIRA, T. C. Privacidade em tempos de pandemia. Covid e trabalho: o dia seguinte. In: Maria do Rosário Palma Ramalho e Teresa Coelho Moreira (Eds.). *Estudos Apodit 7*, AAFDL Editora, Lisboa, 2020.

MOREIRA, T. C. Privacidade e proteção de dados pessoais em tempos de pandemia, in *COVID-19, Implicações na Jurisdição do Trabalho e da Empresa*, Coleção Formação Contínua, 2020. Lisboa: Centro de Estudos Judiciários, 2020.

PINHEIRO, A. S. *A COVID-19 e a proteção de dados pessoais*, Observatório Almedina, 2020.

SHABANI, M., GOFFIN, T., MERTES, H. Reporting, recording, and communication of COVID-19 cases in workplace: data protection as a moving target, *Journal of Law and the Biosciences*, 7(1), 2020.

SUDER, S. Processing employees' personal data during the Covid-19 pandemic. *European Labour Law Journal*, 2021.

ŠVEC, M.; HORECKÝ, J.; MADLEŇÁK, A. GDPR in labour relations - with or without the consent of the employee?, *Ad Alta: Journal of Interdisciplinary Research*, 8(2), p. 281-286, 2018.

WU, J.; WANG, J.; NICHOLAS, S.; MAITLAND, E.; FAN, Q. Application of Big Data Technology for COVID-19 Prevention and Control in China: Lessons and Recommendations. *Journal of Medical Internet Research*, 22(10), 2020.

The Law, State and Telecommunications Review / Revista de Direito, Estado e Telecomunicações

Contact:
Universidade de Brasília - Faculdade de Direito - Núcleo de Direito Setorial e Regulatório
Campus Universitário de Brasília
Brasília, DF, CEP 70919-970
Caixa Postal 04413

Phone: +55(61)3107-2683/2688

E-mail: getel@unb.br

Submissions are welcome at: https://periodicos.unb.br/index.php/RDET