Athens, 04-08-2021 Prot. No.: 1818 A P O F A S H 32/2021 The Personal Data Protection Authority met, at the invitation of its President, in a regular meeting via teleconference on Monday 12.07.2021 at 09:30, adjourned from the meeting of 29.06.2021, in order to examine the case referred to in the history of the present. The President of the Authority, Konstantinos Menudakos, and the regular members of the Authority Spyridon Vlachopoulos, Konstantinos Lambrinoudakis and Charalambos Anthopoulos were present. Grigorios Tsolias, alternate member of the Authority, also attended the meeting, by order of the President, as rapporteur. Present, without the right to vote, were Anastasia Kaniklidou, Chariklia Latsiu, Eleni Martsoukou, legal auditors - lawyers, and Georgia Panagopoulou, IT - auditor, as assistants to the rapporteur and Irini Papageorgopoulou, employee of the administrative affairs department, as secretary. The Authority took into account the following: Following the decision 05/2020, which issued Guidelines regarding the processing of personal data in the context of the management of the COVID-19 coronavirus, the Guidelines 2/2020 for taking security measures in the context of teleworking and Directive 115/2001 on the protection of personal data in the context of employment relations, taking into account the intensity and extent that remote work has received, primarily due to the epidemic due to COVID-19, and the risks that lurk through the use of information and communication technologies (ICT) for the rights of the persons involved in it and the security of the infrastructures of the performers and services used, it is found necessary to issue them, in the context of the information from the Authority of the subjects of the data as well as the controllers and the processing, Guidelines special for the processing of personal data carried out during the provision of remote work, regardless of the form and type of employment, both in the private and public sectors, with the aim of specifying on the one hand the risks, rules, guarantees and rights of the subjects of data and, on the other hand, the obligations of public authorities and private bodies, as controllers, in compliance with the institutional framework for the protection of personal data. With regard to the extent of remote work provision during the initial wave of dealing with the pandemic crisis due to the coronavirus, more than 1/3 (37%) of the workers in the EU (27), who were employed for life in their workplace, joined a telework regime, while this percentage in Greece reached 26.2%1. In addition, the estimate for Greece regarding the remote work provision of salaried employees reaches 40%2, while based on a more recent study3 up to 25% of the total employed (salaried and self-employed, about 500,000 workers) could join in full telecommuting mode4. Already some supervisory authorities, within the framework of the advisory powers of article 58 par. 3 letter b of GDPR and on the occasion of the management of the coronavirus, have issued opinions, with which they point out specific issues 1 Source Eurofound 2020, https://www.eurofound. europa.eu/data/covid-19/working-teleworking 2 Sostero M, S Milasi, J Hurley,

E Fernandez-Macias and M Bisello (2020), “Teleworkability and the COVID-19 crisis: a new digital divide?” JRC Working Papers Series on Labour, Education and Technology 2020/05, European Commission. 3 Pouliakas, Konstantinos, 2020. "Working at Home in Greece: Unexplored Potential at Times of Social Distancing?," (IZA). http://ftp.iza.org/dp13408.pdf. 4 Detailed information on teleworking in the EU before and after the pandemic due to coronavirus can be found in Thematic Information Bulletin No. 3 of November 2020 of the National Institute of Manpower https://www.eiead.gr/publications/docs/EIEAD_THEMATIC__ISSUE_TELEWORK__FINAL.pdf IZA Discussion Human Economics Labor Institute 13408, Papers Labor and of 2 protection of personal data during the organization and execution of remote work5. At the national level, the issue of telework has concerned various bodies, which have pointed out specific risks related to the use of ICT when providing remote work and have proposed specific measures to prevent and deal with them6. The Authority, after evaluating the factual and legal data, after hearing the rapporteur and the clarifications from the assistant rapporteurs, who were present without the right to vote and left after the discussion of the case and before the conference and decision-making, after a thorough discussion, CONSIDERED IN ACCORDANCE WITH THE LAW 1. Because, from the provisions of articles 51 and 55 of the General Data Protection Regulation (Regulation 2016/679) - hereinafter GDPR - and article 9 of law 4624/2019 (Government Gazette A´ 137) that the Authority has the authority to 5 See indicative link of the competent supervisory authority of the United Kingdom - Information Commissioner's Office (ICO) https://ico.org.uk/for-organisations/working-from-home, of France - Commission Nationale Informatique & Libertés (CNIL) https:/ /www.cnil.fr/fr/teletravail-les-regles-et-les-bonnes-pratiques-suivre, https://www.cnil.fr/fr/les-questions-reponses-de-la-cnil-sur -le- teletravail, of Spain – Agencia espanola proteccion datos (AEPD) https://www.aepd.es/en/prensa- y-comunicacion/blog/privacy-online-meetings, of Ireland – An Coimisiún um Profecion Detainas (DPC) https://www.dataprotection.ie/en/dpc-guidance/blogs/protecting-personal-data-when-working-remotely. specialist workers 6 See indicative BSE: teleworking: opportunity for more productive businesses and better life for (2019) Authority https://www.sev.org.gr/Uploads/Documents/52083/SR_TELEWORK_final.pdf, Transparency, covid-19 techniques https:/ /aead.gr/images/manuals/teleworking/EAD-teleworking-guide.pdf, Prosecution of Electronic Crime - attempts to deceive via the internet due to the corona virus http://www.astynomia.gr/index.php?option=ozo_content&lang=% 27..%27&perform=view&id=93647 &Itemid=2425&lang, Ministry of Digital Governance, "Advice for safe work from home" https://mindigital.gr/archives/1291 Fraud Directorate protection guide National from 3 supervises the implementation of the

provisions of the GDPR, this law and other regulations concerning the protection of the individual from the processing of personal data. In particular, from the provisions of articles 57 par.1 item. a', b' and d' of the GDPR and 13 par. 1 item a΄ and b΄ of Law 4624/2019 it follows that the Authority has ex officio competence to monitor and enforce the implementation of the provisions of the GDPR and Law 4624/2019 and to promote the awareness of the public and the controllers and processors on understanding the risks, rules, guarantees and rights and on their obligations under the GDPR when processing personal data. 2. Because Article 2, paragraph 1 of the GDPR provides: "This regulation applies to the automated processing of personal data, in whole or in part, as well as to the non-automated processing of such data which are or are to be included in a system archiving". Accordingly, Article 2 of Law 4624/2019 states: "The provisions herein apply to, in whole or in part, the automated processing of Personal Data, as well as to the non-automated processing of such data, which are or are to be included in a system archiving by: a) public bodies or b) private bodies, unless the processing is carried out by a natural person in the context of an exclusively personal or domestic activity". The provision of remote work is based on the use of ICT and, as automated processing, falls primarily within the scope of GDPR and Law 4624/2019. 3. Because Article 5 of the GDPR defines the processing principles that govern the processing of personal data. Specifically, it is defined in paragraph 1 that personal data, among others: "a) are processed lawfully and legitimately in a transparent manner in relation to the subject of the data ("legality, objectivity, transparency"), b) are collected for specified, explicit and legitimate purposes and are not further processed in a manner incompatible with these purposes (…), c) are appropriate, relevant and limited to what is necessary for the purposes for which they are processed ("data minimization"), d) are accurate and, where necessary, updated; all reasonable steps must be taken to ensure that personal data that is inaccurate, in relation to the purposes for which it is processed, is deleted or rectified without delay ("accuracy") , e) are kept in a form that allows the identification of the data subjects only for the period required for the purposes of the processing of the personal data; the personal data may be stored for longer periods, as long as the personal data will only be processed for archiving purposes in the public interest, for the purposes of scientific or historical research or for statistical purposes, in accordance with Article 89 paragraph 1 and provided that the appropriate technical and organizational measures required by this regulation are applied to safeguard the rights and freedoms of the data subject ("restriction of the storage period"), f) are subjected to processing in a way that guarantees the appropriate security of personal data, including their protection against unauthorized or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organizational measures ("integrity and confidentiality")". 4.

Because, with regard to the principle of legality, objectivity and transparency of the processing according to article 5 par. 1 item a' of the GDPR, taking into account recital 39 of the GDPR7, it should be noted 7 "Each processing of personal data should be lawful and fair. It should be clear to natural persons that personal data concerning them is collected, used, taken into account or otherwise processed, as well as to what extent the personal data is or will be processed. This principle requires that all information and notices regarding the processing of such personal data be easily accessible and understandable and use clear and plain language. This principle concerns in particular the information of data subjects about the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing in relation to the natural persons in question and their right to receive confirmation and to achieve communication of the personal data related to them that are subject to processing. Natural persons should be informed of the existence of risks, rules, guarantees and rights in relation to the processing of personal data and how to exercise their rights in relation to this processing. 5 that teleworking has been regulated at the European level by the European Framework Agreement on Teleworking of 2002, which was incorporated into Greek law first with the National General Collective Labor Agreement of 2006 and 2007 (EGSSE 2006-2007), and included in the later EGSSE. Key points of this European Agreement consist of the following: a) teleworking is voluntary/based on the free consent of the employee, b) the employer is responsible for the provision, installation and maintenance of regular teleworking equipment, unless the remote worker uses his own equipment, c) the employer bears the costs directly caused by teleworking, especially those related to communication. In addition, the provision of Article 67 of Law 4808/2021 (Government Gazette A' 101) replacing Article 5 of Law 3846/2010 (Government Gazette A' 66), provides, among other things: "2. Teleworking is agreed between employer and employee, upon hiring or by amending the employment contract. 3. Exceptionally, as long as the work can be provided remotely, teleworking can be applied: a) Following a decision by the employer, for reasons of public health protection, the assistance of which is established by a decision of the Minister of Health and, as the case may be, co-competent Minister and for as long as these reasons last. b) Upon the employee's request, in the event of a documented risk to his health, which will be avoided if he works remotely and not at the employer's premises and for as long as this risk lasts. In case the employer disagrees, the employee can request the resolution of the dispute by the Labor Inspectorate, in accordance with article 3B of Law 3996/2011 (A' 170). By joint decision of the Ministers of Labor and Social Affairs and Health, the conditions, illnesses or disabilities of the employee, which can document the risk to his health, are determined, as well as the supporting documents, the competent bodies and the procedure for documenting the risk his". 6

Law 4807/2021 (Government Gazette A'96) also regulated the framework for the organization and effective implementation of teleworking in the public sector, both in normal and emergency situations, through the use of IT and communications technologies (Article 1). It is also provided that permanent civil servants and employees with a private law employment relationship of indefinite or fixed duration, including those employed under a salaried mandate contract, as well as seconded teachers who carry out administrative work, as long as the nature of their duties are subject to the regulations of this law makes it possible to carry them out through remote work, while exempting a) those performing the duties of a supervisor and b) the rest of the educational staff and trainers in all structures of every level of education and training (article 4). Further defined as general principles governing teleworking, among others, the protection of personal data and respect for private life (Article 5 letter c and d, respectively). With reference to the protection of personal data, Article 6 of this law provides: "1. The entity, as the controller of personal data, in order to ensure the appropriate level of security against risks to personal data, applies the appropriate technical and organizational measures, as defined by the General Data Protection Regulation (Regulation (EU) 2016 /679 of the European Parliament and of the Council, of April 27, 2016 (L 119) and national legislation and in particular, Law 4624/2019 (A' 137). 2. The entity, with the assistance of the Data Protection Officer, is responsible to adequately inform, train and assist telecommuters in the implementation of procedures for the protection of personal data. 3. For access to the network, the body, as a data controller: a) ensures that there is a possibility of secure remote access to resources of the organization's information systems, b) determines the terms and conditions according to which remote access is allowed c) ensures the connection to the operator's computer systems through a "remote desktop" service only through a virtual private network connection with encrypted and protected data routing, d) installs a secure wireless connection protocol with a strong code on the 7 telecommuting device used by the teleworker , when the latter connects to the internet via a wireless network and e) ensures that the use of files with personal data in teleworkers' personal online storage services is avoided. 4. The teleworker is obliged to make exclusive use of the institution's official e-mail when performing telework. 5. For the use of a terminal device and storage media, an anti-virus and "firewall" system is installed on the telecommuting technological device with the care of the operator. The organization takes care of: a) the regular updating of the aforementioned systems, b) the installation of the latest updates of the application software and the operating system on the telecommuter's device, c) the use of the latest versions of Internet navigation programs by the teleworker with the not keeping a history or deleting it after telecommuting ends, d) the separation of personal data related to telecommuting on the

telecommuter's device, and e) the use of appropriate encryption procedures and procedures for obtaining copies of files containing personal data. 6. Without prejudice to the second paragraph, it is not allowed to use systems for capturing and recording moving images of the teleworker (camera) built into the teleworking device, during teleconferences and to check the performance of the teleworker. If any system is put into operation, it must be dictated by the operational needs of the work provided by the agency and limited to the scope of the intended purpose. 7. To conduct video conferences, the operator uses platforms that support security services, such as encryption and protection of the scheduled video conference. 8. In the event that the operator, as the person in charge of processing personal data, does not ensure at least the specifications of the above paragraphs, telecommuting does not start or is interrupted. 9. Before the start of teleworking, an impact assessment is carried out on the protection of personal data, under the responsibility of the organization". of link 8 5. Because, with regard to the principle of integrity and confidentiality of personal data according to article 5 par. 1 item. f of the GDPR, taking into account recitals 39 8 and 499 GDPR, and based on Article 32 of the GDPR, the data controller must implement appropriate technical and organizational measures in order to ensure an appropriate level of security against risks to the rights and the freedoms of natural persons from processing. In the case of telecommuting, the data subjects are both the employees and the natural persons of other categories (e.g. customers, recipients of services, etc.) whose data is required to be legally processed by the controller. 6. Because, with regard to the principle of personal data protection by design and by definition, based on Article 25 of the GDPR, and guidelines 4/2019 10 of the GDPR and taking into account recital 78 GDPR, the data controller must effectively apply , both at the time of determining the means of processing and at the time of processing, appropriate technical and organizational measures, such as pseudonymization, designed to implement data protection principles, such as data minimization, and the incorporation of the necessary guarantees 8 "(…) Personal data should be processed in a way that ensures the appropriate protection and confidentiality of personal data, including to prevent any unauthorized access to such personal data and to the equipment used for their processing or the use of this personal data y character and the equipment in question". 9 "The processing of personal data, to the extent that it is strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or information system to withstand, at a given level of confidence, random events or illegal or malicious actions that jeopardize the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, as well as the security of the relevant services offered by said networks and systems or that are accessible through said networks and systems, or offered by public authorities, IT emergency

response teams (CERTs), computer security incident response teams (CSIRTs), electronic communications network and service providers, and security technology and service providers , is a legitimate interest of the data controller concerned. This could include, for example, preventing unauthorized access to electronic communications networks and the distribution of malicious code, and stopping denial-of-service attacks and damage to IT and electronic communications systems." 10. by definition, only the personal data necessary for its respective purpose are processed. When designing the policies and procedures related to teleworking, the measures and safeguards applied should achieve the desired result in terms of data protection. The controller should have documentation of the applied technical and organizational measures, including appropriate performance indicators to demonstrate their effectiveness. 7. Because, according to the provisions of article 5 paragraph 2 of the GDPR, the data controller bears the responsibility and must be able to demonstrate compliance with the principles of processing established in paragraph 1 of article 5. As the Authority11 has judged, with the GDPR a new compliance model was adopted, the central element of which is the principle of accountability in the context of which the controller is obliged to design, implement and generally take the necessary measures and policies, in order for the processing of data to be in accordance with the relevant legislative provisions. The importance of the controller's internal compliance with GDPR requirements is highlighted by the provisions of article 24 para. 1 and 2 GDPR, according to which the application of appropriate technical and organizational measures is required, which includes the preparation and implementation of appropriate policies and procedures. In addition, the data controller is burdened with the further duty to demonstrate at all times his compliance with the principles of article 5 par. 1 GDPR. Compliance with the requirements of the GDPR and national legislation is an ongoing process that begins even before the collection and processing of the data with the design of the relevant procedures and ends only with the final deletion of the data. 11 See Authority decision 26/2019, paragraph 8, available on its website. 10 8. Among the tools for fulfilling the principle of accountability pursuant to Article 5 para. 2 in conjunction with Articles 24 para. 1 and 32 GDPR, taking into account recital 83 GDPR, is the Data Protection Impact Assessment (DPA), which is provided for in article 35 of the GDPR. The GDPR allows data controllers to comply with GDPR requirements whenever high-risk data processing is planned or implemented but also to demonstrate that they implement and generally take appropriate measures to ensure such compliance. In the case of the planning and organization of teleworking, regardless of the fact that the specific case of processing is included in the national list of processing for which the execution of a Personal Data Protection Act is required (decision no. 65/201812 of the Authority), the performance of the Personal Data

Protection Act can contribute to the identification and minimizing the data protection risks of the whole process. 9. Because article 88 of the GDPR provides: "1. Member States, through legislation or through collective agreements, may establish special rules in order to ensure the protection of rights and freedoms against the processing of personal data of employees in the context of employment, in particular for the purposes of recruitment, performance of the contract employment, including the performance of obligations provided for by law or collective agreements, management, planning and organization of work, equality and diversity in the workplace, health and safety at work, protection of the property of employers and customers and for purposes of exercise and enjoyment, on an individual or collective basis, rights and benefits related to employment and for purposes of termination of the employment relationship. 2. These rules include appropriate and specific measures to safeguard the human dignity, legal interests and fundamental rights of the person to whom the data refer, with particular emphasis on the transparency of the processing, the transmission of personal data within a group of companies, or of a group of companies that carry out joint economic activity and 12 https://www.dpa.gr/sites/default/files/2019-09/65_2018anonym.pdf 11 monitoring systems in the workplace.3. Each Member State shall notify the Commission of the provisions it adopts under paragraph 1 by May 25, 2018 and, without delay, of any subsequent amendment." Furthermore, according to Recital 155 of the GDPR: "Member States' law or collective agreements, including 'employment agreements', may lay down specific rules for the processing of employees' personal data in the context of employment, in particular for conditions under which personal data in the context of employment may be processed based on the consent of the employee, for the purposes of recruitment, performance of the employment contract, including the performance of obligations provided for by law or collective agreements, management, planning and work organisation, equality and diversity in the workplace and health and safety at work, as well as for the purposes of exercising and enjoying, on an individual or collective basis, rights and benefits related to employment and for the purposes of terminating the employment relationship". Finally, article 27 of Law 4624/2019 regarding the processing of personal data in the context of employment states: "1. Personal data of employees may be processed for the purposes of the employment contract, as long as it is absolutely necessary for the decision to conclude an employment contract or after the conclusion of the employment contract for its execution. 2. In the event that the processing of an employee's personal data exceptionally has as a legal basis his consent, for the judgment that this was the result of free choice, the following must be taken into account mainly: a) the dependency of the employee existing in the employment contract and b) the circumstances under which the consent was granted. The consent is given either in written or electronic

form and must be clearly distinguished from the employment contract. The employer must inform the employee either in writing or electronically about the purpose of the 12 processing of personal data and his right to withdraw consent in accordance with Article 7 paragraph 3 of the GDPR. 3. By way of derogation from Article 9(1) of the GDPR, the processing of special categories of personal data within the meaning of Article 9(1) of the GDPR for the purposes of the employment contract is permitted, if it is necessary for the exercise of rights or the fulfillment of legal obligations arising from labor law, social security and social protection law and there is no reason to consider that the legitimate interest of the data subject in relation to the processing prevails. Paragraph 2 also applies to consent to the processing of special categories of personal data. Consent must be explicitly stated in this data. Article 22 paragraph 3 sub-paragraph b is applied accordingly. 4. The processing of personal data, including special categories of personal data of employees for the purposes of the contract is permitted The negotiating parties comply with Article 88 paragraph 2 of the GDPR. 5. The data controller shall take appropriate measures to ensure that the principles for the processing of personal data set out in Article 5 of the GDPR are observed in particular. 6. Paragraphs 1 to 5 shall also apply, when personal data, including special categories of personal data of employees, are processed without being stored or intended to be stored in a filing system. 7. The processing of personal data through closed-circuit visual recording within workplaces, whether publicly accessible or not, is permitted only if it is necessary for the protection of persons and property. Data collected through closed-circuit visual recording may not be used as a criterion for evaluating employee performance. Employees are informed in writing, either in written or electronic form, of the installation and operation of closed-circuit visual recording within the workplaces. 8. For the purposes of this law, employees are defined as collective labor agreements. employment based on 13 those employed with any employment relationship or project or service contract in the public and private sector, regardless of the validity of the contract, job candidates and former employees". With reference to the provision of article 27 of Law 4624/2019, the Authority has ruled, among other things, with Opinion 1/2020: "With the version, in which par. 1 of article 27 of the law introduces a unique legal basis processing for every purpose of processing in the context of employment relations, in which the legal bases of article 6 par. 1 GDPR are essentially "merged" and therefore their independent application is excluded (except for consent, which is expressly provided for in paragraph 2 of the article 27 of the law), the regulation contradicts the provisions of article 88 para. 1 GDPR which allows the "establishment of special rules" for the specialization of processing rules based on the legal bases of article 6 para. 1 GDPR and not for the creation of new legal bases or the exclusion of the application of the legal bases of the GDPR. (…) With the opposite correct view that the

independent application of the other legal bases of article 6 par. 1 GDPR is not excluded, the employee is given the possibility of checking the correct and legal application of the relevant legal basis, which could ultimately lead to in prohibition of processing e.g. when judged in the case of article 6 par. 1 sec. e' GDPR that the processing does not concern the fulfillment of a duty performed in the public interest or in the case of article 6 par. 1 sec. in the GDPR that the fulfillment of the employer's legal interest does not prevail over the interest or the fundamental rights and freedoms of the employee (cf. GPA 26/2019 par. 16 with references to the Opinions of the Working Group of article 29) (…) 13". 10. Because article 22 of the GDPR, in terms of which recital 72 must also be taken into account, provides with regard to automated individual decision-making, including profiling: "1. The data subject has the right not to be subject to a decision made solely on the basis of automated processing, 13 Opinion 1/2020 of the Authority p. 16-19, available on the Authority's website. 14 including profiling, which produces legal effects concerning it or significantly affects it in a similar way. 2. Paragraph 1 does not apply when the decision: a) is necessary for the conclusion or performance of a contract between the data subject and the data controller, b) is permitted by Union law or the law of a Member State to which it is subject the controller and which also provides for appropriate measures to protect the rights, freedoms and legal interests of the data subject or c) is based on the express consent of the data subject.3. In the cases referred to in paragraph 2 items a) and c), the data controller applies appropriate measures to protect the rights, freedoms and legal interests of the data subject, at least the right to ensure human intervention on the part of the controller processing, expressing an opinion and contesting the decision. 4. The decisions referred to in paragraph 2 shall not be based on the special categories of personal data referred to in Article 9(1), unless Article 9(2)(a) or (g) applies and appropriate measures are in place to protect rights, of the freedoms and legal interests of the data subject". Besides, the Authority with Directive 115/2001 regarding the protection of personal data in the context of employment relations (under the previous legislative regime) accepted that: of the employees' personality, such as their behavior or efficiency, may not be obtained solely on the basis of automated processing of personal data. Such a process would reduce workers to informational objects and insult their personality." 11. Because telecommuting and "mobile technology" blurs the lines between home and work. The new forms of work often require greater participation and initiative of the employees but also entail 15 greater intrusion into private space and time14, de facto questioning the protection of privacy, personal data and the right to private life (Article 9 par. 1 second paragraph and 9A of the Constitution), and at the same time forming a mentality of "permanent presence and permanent vigilance of employees", which has a negative impact on the balance between their professional and

personal lives15. Therefore, the right to disconnection16 must be a fundamental right, of vital importance for the protection of the physical, mental health and well-being of employees17. The need to strengthen a protective network for the employee is even intensified as a regulatory obligation for the legislator and the law enforcer the harder the working conditions and relationships develop and consequently the more vulnerable the dependent - worker becomes18. In this regard, article 18 of Law 4807/2021 regarding teleworking in the public sector provides that "after the end of his working hours, the teleworker disconnects from the IT and communication means he uses to perform his duties". Accordingly, paragraph 10 of article 67 of Law 4808/2021 on teleworking in the private sector provides that: "The teleworker has the right to disconnect, which consists in his right to completely refrain from providing his work and in particular, not communicates digitally and not to respond to phone calls, emails or any form of communication outside of working hours and during his statutory holidays. Any proposal, legislative, is prohibited14 Lilian Mitrou, Privacy, Personal Data and labor relations, Labor Law Review, Volume 76, Issue 2, Year 2017, page 138. 15 The need to enshrine in European law the right of employees to digitally disconnect from their work after the end of the of their work without repercussions was presented to the European Parliament, which called on the European Commission to file https://www.europarl.europa.eu/news/en/press- relevant room/20210114IPR95618/right-to-disconnect-should-be- an-eu-wide-fundamental-right-meps-say, https://The right to disconnect – European Sources Online, https://The right to disconnect (europa.eu). 16 See and Guide of the International Labor Organization (ILO) on "Practical guide on teleworking during the Covid-19 pandemic and beyond", p. 17), where the necessity of exercising the right to disconnect, without repercussions for the employee, is underlined. 17 This right was born - not only for the teleworker - jurisprudentially in France in 2001 by the Cour de cassation. 18 Lilian Mitrou, The data protection of employees in Leonidas Kotsali (ed.), Personal Data, Analysis-Comments-Implementation, Law Library, Athens 2016 p. 220. see 16 adverse discrimination against a teleworker, because he exercised the right to disconnect. The technical and organizational means required to ensure the disconnection of the teleworker from the digital communication and work tools are mandatory terms of the telework contract and are agreed between the employer and the representatives of the workers in the company or farm. In case of lack of agreement, the means of the previous paragraph are determined by the employer and communicated by him to all employees"19. It is defined in paragraph 5 item. a' of the same article that the immediately above disconnection right is included in the conditions that the employer is obliged to notify the employee in any convenient way (including e-mail) within eight days from the start of teleworking. 12. Because the use of personal computer equipment in a

business context known by the acronym "B.Y.O.D.", which is an abbreviation of the English expression "Bring your own device", ("Bring your own device"), is widely observed in the context provision of remote work and in addition this possibility is now provided by law20. Regarding the use of B.Y.O.D. use of private equipment before the start of personal data processing. In this context, according to Opinion 2/2017 of the Article 29 Working Group "in principle, access by the data controller, organization or company, to the parts of the household appliance is not allowed , which are assumed to be used only for private purposes (e.g. photo storage folder shelves that 19 It should be noted that until December 2020 only four Member States had fully enshrined in law the teleworker's right not to answer outside working hours. 20 no. 67 par. 4, 5 sec. c' n. 4808/2021 17 are taken with the device)"21. In addition, appropriate measures must be applied to distinguish between the private and professional use of the device, especially when through the monitoring of the location and traffic of these devices it is possible to collect data related to the private and family life of the employee. Also, the data controller must implement methods by which personal data processed in the context of official or business activity are securely transmitted between the employee's device and his network. Also, when the traffic of the data takes place via VPN, the controller, in order to avoid the risk of privacy violation during the personal use of the device by the employee, it is recommended that the controller choose devices that offer additional protection, such as sandboxing , limiting data within a specific device). FOR THESE REASONS, the Authority issues the following Guidelines: 1. Teleworking constitutes a form of organization and/or execution of work within the framework of a contract or employment relationship or service relationship with the State using ICT, provided outside the organization's facilities or business22. In addition, with regard to the public sector remote work 29 wp. of 249, in the available 08.06.2017, private law indefinite or definite 21 Opinion 2/2017 on data processing in the work of the Working Group of the article website https://ec.europa.eu/newsroom/article29/items/610169, p. 20. 22. In Law 4807/2021 telework is defined as "the form of organization and execution of work in the context of which the permanent civil servant or the employee employed in a sector employment relationship, including those employed under a salaried contract, performs the tasks of using IT and communication technologies, remotely" (article 3 letter a'). Accordingly, in article 67 paragraph 1 of Law 4808/2021 the following definition is provided: "1. Teleworking is the remote provision of dependent work of the employee and with the use of technology, by virtue of the full-time, part-time, rotational or other form of employment contract, which could also be provided from the employer's premises". In article 2 of the relevant European Framework Agreement, teleworking is defined as "a form of organization and/or execution of work, within the framework of a contract or employment relationship, with the use of time in

the public 18 may be provided voluntarily in accordance with article 7 par. 1 and 2 of Law 4807/2021, or to be imposed for imperative reasons of public interest (see decision 05/2020), in accordance with paragraph 3 of the same article. Moreover, according to article 5 par. 2 and 3 of Law 3846/2010, as replaced by Article 67 of Law 4808/2021, teleworking in the private sector is the subject of an agreement between employer and employee and exceptionally in certain cases may be decided by the employer or requested by the employee without a relevant agreement. The data controller, in accordance with the principles of article 5 par. 1 item a' - c' in conjunction with recital 39 GDPR, and before starting the processing of personal data, must inform the employee, in a transparent manner, not only of the terms of execution, but also of the benefits and risks of telecommuting and, in addition, to ensure that the personal data processed is limited only to what is necessary for the purpose of processing and is kept for the period of time required on a case-by-case basis to achieve this. 2. In any case, the organization of remote employment for any reason, especially in the context of the employment relationship in the private sector due to the inequality of employee and employer, must not lead to inequalities and discrimination (salary, career development opportunities, participation in vocational training programs) and affect the employment, insurance and social rights of employees, nor further lead to automated individual decision-making, including the profiling of employees remotely in violation of information technologies, which, while it could be provided to premises of the employer, is provided instead on a fixed basis, outside these premises in a regular (systematic) manner'. However, in all cases, the definitions of teleworking that are encountered converge on the following two characteristics: a) the provision of work, in whole or in part, in a place other than the premises of the company/organization and b) the performance of the specific work tasks necessarily with the use of electronic devices. 19 provision of article 22 of the GDPR, in direct violation of the right to personality, in accordance with Directive 115/2001 of the Authority23. 3. The controller must have complied with the requirements of the GDPR and the relevant national legislation for the protection of personal data before processing them, by taking the required technical and organizational measures (see for the bodies subject to the provisions of Law 4807/2021 according to Article 3(c), in particular, the relevant provisions of Articles 5(c) and (d) and 6 of this law), from which its compliance is also demonstrated (e.g. preparation and implementation of policies and procedures).The obligation to satisfy the rights exercised by the data subjects is kept intact during performing the work remotely (see point 3 of the Authority's decision 5/2020). In addition, the controller must constantly adapt to the new conditions created when organizing remote work (e.g. due to the extraordinary circumstances caused by the coronavirus pandemic) and demonstrate compliance within the framework of the principle of

accountability according to article 5 par. 2 of the GDPR, by taking, in particular, a series of technical and organizational measures, pursuant to the provision of article 24 and recital 74 of the GDPR, as listed below (under point 13). It is pointed out, finally, with regard to possible delays in responding to requests that constitute the exercise of rights by the subjects, in this case in particular by employees, that on the one hand no provision of the GDPR and national legislation provides for the temporary suspension of the relevant deadlines and obligations to satisfy the rights, on the other hand, that it constitutes an obligation of the data controller to internally document the reasons for delay or non-satisfaction of the exercised rights, taking into account both the principle of law "no one is obliged to the impossible", as well as the object and conditions of exercising the activity of the data controller which possibly burdened by the 23 See Directive 115/2001 point 7, page 12, available on the website of the Authority. 20 emergency condition (such as hospitals in the case of the pandemic). In any case, any invocation of reasons for relevant delays both against the data subjects and against the Authority in the exercise of its audit powers should be particularly well-documented and not pretentious given that the required technical and organizational measures should already be in place received and applied before the start of the processing of personal data. 4. When providing remote work, the data controller is entitled, if in principle the conditions arising from the provisions of articles 5 para. d' section are met. b,' 15 para. c', d' of Law 4807/2021 and 67 par. 8 of Law 4808/2021, to check whether the employee actually provides the agreed work in terms of observing working hours (hours) and fulfilling the of this terms. In addition, the controller must comply with the principles governing the legality of the processing of personal data according to article 5 paragraph 1 of the GDPR. In this context, it would in principle be legitimate for the controller to request additional confirmation (authentication) from the ICT user (PC, communication software - electronic mail) - assuming that he actually provides the agreed work and keeps the relevant information . 5. Regarding the more specific issue of any continuous surveillance of the employee with the obligation to operate the computer camera and the use of T.N. software. (e.g. facial and motion recognition) or the sharing of the screen or the installation and operation of keylogger type recording software or even the obligation of the employee to perform very regular actions to prove his presence behind his screen, the Authority has judged in a series of its decisions (see APD 34/2018, 26/2019 and 43/2019), including the aforementioned under no. 5/2020 GDPR that "a 21 systematic, continuous and generalized collection of personal data that leads to the creation and continuous renewal of profiles could hardly be characterized as in accordance with the principle of proportionality". In addition to the prohibitions set by laws 4807/2021 (in particular article 6 par. 6) and 4808/2021 (in particular article 67 par. 8 second paragraph) regarding the use of a camera (web

cam), to control the employee's performance the data controller, in the context of his responsibility for accountability, should take into account and consider interpretatively the provision of article 27 par. 7 of Law 4624/2019 (by which measures were taken to implement the GDPR,) in which it is defined that "the processing of data through closed-circuit visual recording within workplaces, whether publicly accessible or not, is permitted only if necessary for the protection of persons and property. Data collected through closed-circuit visual recording may not be used as a criterion for evaluating employee efficiency.' In addition, the legality of taking any such relevant measure that constitutes processing of personal data presupposes the prior notification of the data subject, based on both the provisions of the GDPR and any more specific provisions (e.g. see article 6 par. 2 n 4807/2021 and article 67 par. 9 of law 4808/2021). Finally, the Authority, in accordance with the jurisprudence of the European Court of Human Rights and the Opinions of the Working Group of Article 29 of Directive 95/46/EC (currently the European Data Protection Council) with its recent decisions (see in particular the APD 34/ 2018, 43/2019 and 44/2019) prescribed the conditions, terms and procedures under which the employer may have access to the personal data processed by the employees in the context of employment relations through computers, servers, etc. but also the provisions and any restrictions of the employees in the way of using the computer and communications infrastructure 22 of the organization (see also articles 6 par. 4 and 5 par. d and 12 par. 3 of Law 4807/2021 and article 67 par. 5 para. d. Law 4808/2021) However, it should not be overlooked that in the context of his managerial right the employer has the authority to take the necessary measures related to the provision of work for the orderly organization of the business that involves the processing of personal data but also to exercise the necessary and appropriate control over the work provided, the fulfillment of contractual obligations, including the employee's duty of loyalty as well as the obligations to provide the necessary information, among other things, in the context of control of the protection of financial resources and infrastructure of the business. The measures adopted by the employer in this direction should respect the fundamental rights of the employees, in accordance with the principle of proportionality: for example, it is not justified to monitor, through appropriate software (e.g. TLS appliance) every outgoing by the Internet traffic company in view of the above purposes, when they can be achieved with milder preventive means24. Moreover, from the provisions of articles 5 para. c', 6 para. 4, 12 para. 3, 15 para. c-e of Law 4807/2021 which regulates telework issues in the public sector, in combination with the content of the authorization provided by article 19 of the same law for the issuance of a Presidential Decree, it follows that the controller must, in compliance with the special legislation governing the official or employment relationship and telecommuting, take the appropriate technical and organizational measures to comply with the

protection requirements of the teleworker's personal data. 24 See also Opinion 2/2017 of the Working Group of Article 29. 23 6. According to the provisions of article 5 par. 1 item. a' and b' of the GDPR principles of legality and limitation of purpose, the teleworker has the right after the end of the time during which he has an obligation to provide work (including periods during which he is on any form of leave), taking into account and the provisions of articles 18 of Law 4807/2021 and 67 par. 10 of Law 4808/2021 for the employees of the public sector and the private sector, respectively, to disconnect, without adverse effects, from digital media (software, digital platform, social networks, wireless connections, electronic messages, internet/intranet) used to organize employment. The right to digital disconnection after the end of working time is a fundamental right of employees, of vital importance and directly linked both to the fundamental right to the protection of privacy, personal data, the right to private life and respect for private and family life (articles 9 par. 1 second paragraph and 9A of the Constitution and 8 of the European Convention on Human Rights), as well as with the balance of professional and personal life, the protection of the physical, mental health and well-being of employees25. 7. With reference to the security of the processing according to articles 24 and 32 of GDPR, and specifically the observance of the principle of integrity and confidentiality of personal data in accordance with article 5 par. 1 item. in the GDPR, i.e. their protection against unauthorized or illegal processing in them and in the equipment used for their processing, on the one hand the permanent obligation of the controller to obtain technical 25 Although under the telecommuting regime, accurate measurement and observance of working time becomes difficult, the employer's obligation to implement a reliable and objective system for measuring the daily working time of each employee still exists. who provides his work outside the employer's premises [See and the decision Federación de Servicios de Comisiones Obreras (CCOO) v Deutsche Bank SAE C-55/18 of 14 May 2019 of the Court of Justice of the European Union, concerning the interpretation, inter alia, of Articles 3, 5, 6, 16 and 22 of Directive 2003/88 of the European Parliament and of the Council, of 4 November 2003, on certain elements of the organization of working time (OJ 2003, L 299, p. 9), according to which Member States must impose on employers the obligation to implement a system for measuring the daily working time of each employee]. 24 security measures and the relevant information of the employed, by utilizing the services of the DPO of the company or organization (Article 39 par. 1 item a' GDPR) and on the one hand the obligation to observe secrecy-confidentiality-loyalty by the employed, as applicable of the relevant provisions, including articles 26 of Law 3528/2007 and 1 of Law 146/1914, in a way that ensures that third parties to the employment relationship (e.g. family members) do not gain access to the records of the organization or business. It is pointed out that the controller is responsible for the secure

processing of personal data in the context of the operation of the business that takes place through the company's hardware and software systems, VPN networks, etc. used by employees, including those stored on terminals, servers, etc., whether owned by the company or the employees themselves. In the same context, the forwarding of e-mail messages, both by the business or organization and by the remote worker to the personal e-mail address of the latter, should be further avoided, especially when the content of the message is not encrypted. Finally, the printing of official/company documents at the employee's home or in a place/space other than the workplace must be carried out in a way that ensures that personal data cannot be leaked to unauthorized third parties. 8. With regard to the security of processing, and specifically the availability of personal data, which is often threatened by ransomware-type attacks26, the data controller must take appropriate technical and organizational measures, such as the use of appropriate malware detection tools, adequate management of software updates on the devices through which telecommuting takes place, as 26 A type of malware that threatens to release the victim's personal data or cut off the victim's access to it, until a ransom is paid by the victim. 25 and the appropriate backup procedure. It must also provide the means to ascertain whether messages received by e-mail or other means of communication are authentic and reliable. Employees should be trained to recognize attempts at such attacks (e.g. identifying "suspicious" e-mails), when such an attack has taken place, and be aware of their obligation to report it immediately to the security manager or data protection, based on a clearly documented data breach incident management process. 9. When carrying out teleconferences, taking into account the relevant prohibitions and limitations provided by the legislation, such as the provision of article 6 par. 6 of Law 4807/2021 on the provision of teleworking in the public sector, the remotely employed such public, as well as in the private sector, he is entitled, in accordance with the principle of data minimization, to activate the possibility of the platform used, for his participation in it only through a microphone, and not continuously during its implementation through a camera, especially when there are reasons that require it (e.g. protection of minors). In addition, the remote employee is recommended to choose features of the platform used that allow the background to be hidden by blurring or by adding an image (virtual background) in order to avoid the risk of revealing personal information that may arise from viewing. 10. With reference to the recording of teleconferences carried out in the context of the employee's obligations as they arise from the telework contract or the law, the controller (employer) must, taking into account the relevant provisions of the relevant legislation (see in particular article 6 par. 6 of Law 4807/2021) not to proceed with it, in application of the principle of proportionality and minimization. In any case, to carry out this type of processing, the controller, before processing, takes

appropriate measures to protect 26 personal data and, where necessary, conducts an impact study. In the event of recording a teleconference with a third person/party (other than the employee) that takes place during a legitimate professional practice with the purpose of providing evidence of a commercial transaction or other communication of a professional nature, article 4 paragraph 3 of Law 3471/2006 shall apply accordingly, that is, after prior information for the purposes of recording, the prior consent of the parties to the communication is required. 11. With regard to the use of personal devices (B.Y.O.D.) of remote workers and access to the network the employer remains responsible for the security of personal data processed by the company or organization, even when stored on terminals where does not have physical control or ownership, but for which it has authorized the making of arrangements so that employees have access to data (cf. see articles 6 par. 1, 3, 5, 7 and 9 n. 4807/2021). The use of B.Y.O.D. must be decided on the one hand in accordance with the provisions of the special legislation (see e.g. articles 12 par. 1 and 15 para. c. Law 4807/2021), on the other hand, after weighing the interests and disadvantages presented by this usage, which blurs the line between personal and professional life. The controller must identify the risks, taking into account the particularities of each case (equipment, applications, data) and assess them in terms of seriousness and the likelihood of occurrence of incidents of violation in order to determine the measures to be implemented and included in the security policy. Indicative security measures could include: the physical or logical separation of the parts of the personal device intended for use in a professional environment (creating a "bubble 27 delete equipment, security remote"), the control of remote access through a strong control mechanism user identity (if possible using an electronic certificate, smart card, two-factor authentication, etc.), the definition of encryption measures for information flows (VPN, TLS, etc.), the definition of a procedure for recovery in case of damage or loss personal device (network administrator information, providing a professional alternative to business data stored on the personal terminal), the requirement to observe basic security measures such as locking the terminal with a password according to best practices and using an up-to-date anti-virus program , the awareness t of users about the risks, prior approval of the network manager and/or employer for the use of personal equipment, informing everyone of their responsibilities and stating the precautions to be taken in a binding map. 12. In the event that personal data is transferred to third countries when teleworking or teleconferencing takes place, the data controller selects and uses tools and platforms that comply with the provisions of Chapter V of the GDPR for transfers of personal data to third countries or, following the repeal by the Court of Justice of the European Union Schrems II of the EU-US Privacy Shield for transatlantic data transfers ("Privacy Shield"), uses approved Standard Contractual Clauses for the transfer by the European Commission

and remain in force27. 27 COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of of the European Parliament and of the Council and COMMISSION IMPLEMENTING DECISION (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllersprocessing and processing based on article 28 paragraph 7 of the regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7). of Regulation (EU) 2018/1725 of the European Parliament and of the Council.

28

13.

In any case, it is emphasized that the obligation to comply and accountability of the controller, organization or business, to institutional framework for the protection of personal data is one continuous/permanent process which starts even before the collection of the data with the design of the procedures and ends only with the definitive deletion of them data.

In particular, the data controller must adapt and constantly conforms to the new conditions created during the provision telecommuting, namely:

• To update the log of Article 30 GDPR.

• To update – modify the data processing contracts with processing under no. 28 GDPR.

• To update the policies and procedures for the processing of personal data, but also consider the possibility to draw up and implement a personal data processing policy

With the two aforementioned Executive Decisions of the European Commission they are now covered all cases of transfers under standard contractual clauses from its countries European Economic Area to third countries, i.e. transfers between a) Controllers

Controller to Controller, b) Controller and Processor

(Controller to Processor) c) Processor to Processor and d) Processor

the Processing and Processor to Controller. The new standardized ones

contractual clauses are fully adapted to the GDPR as well as to its reasoning

Decision of CJEU Schrems II (C-311/2018).

Except in cases where personal data are transferred to third countries

on the basis of Article 46 of the GDPR, i.e. on the basis of appropriate guarantees such as those mentioned above

standard contractual clauses, it should be taken into account that the European Commission has already,

under Article 45 of the GDPR, acknowledge that the following countries provide an adequate level

personal data protection ("adequacy decision"): Andorra, Argentina, Canada (only

for commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan,

Jersey Island, New Zealand, Switzerland, Uruguay. Negotiations are underway with the

United Kingdom for the adoption of an adequacy decision regarding the GDPR and the Directive

2016/680 (Protection of personal data during their processing by police officers and

judicial authorities) as well as negotiations with South Korea on the GDPR. Additionally

negotiations are taking place between the European Union and the USA with a view to a new

of the "EU-US Privacy Shield" agreement to avoid

future Schrems III decision.

for reasons related to extraordinary circumstances (e.g. Covid19) and

dealing with related incidents

• Have a policy and procedures for telecommuting

• To have policy and procedures for the use of private equipment in

professional context (B.Y.O.D.)

• To carry out where necessary an impact assessment

• To consult the Ministry of Foreign Affairs

• Train staff on data protection

of a personal nature when providing telework

• In the event of any processing of said employee data

from the employer outside the EU (including UK soon)

the decision of the CJEU Schrems II should now be taken into account.

14. With the provisions contained in laws 4807/2021 and 4808/2021

the principle of accountability is reflected and extradition is provided for

presidential decrees (see article 19 of law 4807/21 and article 67 par. 12 of law 4808/21)

for the specialization of the appropriate technical and organizational measures for the

compliance with the personal data protection requirements of

telecommuters.

Therefore and given the legislative provision for extradition

of the Authority's previous Opinion on the plans of P.D/s, the Authority reserves the right to

placed in more detail.

The president

The Secretary

Konstantinos Menudakos

Irini Papageorgopoulou