Athens, 30-03-2022 Prot. No.: 808 DECISION 19/2022 The Personal Data Protection Authority met, following the invitation of its President, in an extraordinary meeting via video conference on 26-

10-2021 and time 10:00, following the meeting from 06-10-2021, in order to examine the case mentioned in the history of this present. Konstantinos Menudakos, President of the Authority, regular members Spyridon Vlachopoulos, as rapporteur, Konstantinos Lambrinoudakis and Charalambos Anthopoulos were present. At the meeting, without the right to vote, the auditors Anastasia Kaniklidou and Panagiotis Tsopelas, expert scientists-auditors, as assistants to the rapporteur, were present, by order of the President, who left after the discussion and before the conference and the decision-making, and Irini Papageorgopoulou, employee of the Department of Administrative Affairs, as secretary. The Authority took into account the following: With its complaint No. C/EIS/182/12-01-2021, A complains before the Authority that Vodafone - PANAFON S.A.E.T improperly satisfied the right access to personal data concerning her. In particular, the following are mentioned in the complaint: The complainant, a former employee ... at ... Address of the company being complained about, on ... sent a request by e-mail to the company, requesting full information regarding the personal data concerning her, copies of the personal data the complainant keeps in the files (such as indicative certificates, evaluations, e-mails, correspondence) as well as all the information requested under the General Data Protection Regulation, submitting at the same time a request for 1 Kifisias Ave. 1-3, 11523 Athens T: 210 6475 600 E: contact@dpa.gr www.dpa.gr to limit the processing of her personal data, in order to use them in view of the pending trial with the accused. In said request, the complainant replied on …, asking the complainant to send a new request, using the form that the company had, thus making it difficult – according to the complainant's claims – to exercise the right of access, which the complainant did not. The Authority, in the context of examining the above complaint, with its document No. C/EXE/505/28-01-2021, informed the complainant about the complaint and invited her to present her views on it. The complainant responded on ... with her document under protocol number C/EIS/1099/15-02-2021, with which she also submitted relevant documents. In the said response, the complainant states that she is a quasi-universal successor, after absorption, of the anonymous company with the name "...", in accordance with the protocol no. with which their partnership was terminated on …, at which point the contract was terminated by … from the above company (that is, before the absorption of … by the one being terminated) and was fully compensated on … by …, without ever having transferred the employment relationship from on ... to the complainant. Irrespective of the above, according to the complainant, following the complainant's access request, on ... he asked the complainant to complete the relevant printed form for exercising the right of

access as well as to send the relevant identity documents for the identity check. Subsequently, on ... in a relevant letter sent to the complainant, it informed her that, a) it processes employee data in general in accordance with the Employee Personal Data Protection Statement, b) with regard to the exercised right of access, because the search and retrieval of relevant physical file became difficult due to the extraordinary measures to deal with the corona virus and teleworking, the complainant had launched the required actions on the request until the end ..., while repeating that in order to grant her copies of the data she requested, document 2 would be needed in any case proof of her identity. It concluded by stating that it responded in a timely and appropriate manner to the complainant's request, since on ... the complainant was asked to complete the relevant application of a former employee for access to personal information and to attach proof of identity for the identity check, however the complainant refused, sending her reply from an email address unknown to the complainant. Subsequently, according to the complainant's claims, in a letter to ... she informed the complainant to receive the copies of her personal data, presenting her proof of identity, while in the accompanying letter upon delivery of these to ... the complainant stated that the related documents with the contract ... and its resolution delivered to the complainant are kept for twenty years from the complaint for the purpose of proving compliance with the legal obligations of the complainant, stemming from the current insurance legislation. As regards the rest of the documents that they handed over to the complainant, these are kept for a period of 5 years from the complaint for the purposes of establishing, exercising, supporting the legal claims, and after the complainant files a lawsuit, the data is kept for as long as there is pending litigation, thus satisfying the relevant request of the complainant to limit the processing. In addition, the complainant, in the aforementioned relevant letter to the complainant, referring to the delivered documents or e-mails, requested further specification of the request from her in order to examine the possibility of its satisfaction, because their volume was enormous, stating at the same time that "the electronic account that she maintained as an employee of ... has automatically been abolished 90 days after the termination of the employment contract". However, according to the complainant, the complainant did not satisfy her request in the least, since she only forwarded to her a small amount of her personal data, omitting critical data, such as evaluation reports, copies of electronic communications, and copies of data stored in the corporate computer. 3 Subsequently, the Authority, with its letter C/EXE/952/29-03-2021 to the complainant, requested further clarifications regarding the contents of its letter dated ... to the complainant and in particular: a) With reference to her claim complainant, which is included in her letter from ... to the complainant, according to which "with regard to your personal data, which may be contained in deliverable documents, which

you have drafted/edited/corrected or in e-mails that you have exchanged with employees of our company, as you understand their volume is huge ..[…].. please specify your above request in terms of the specific documents/messages/deliverables, with criteria that facilitate their detection", but also of claim that "the e-mail account you maintained as an employee of the company ..., has automatically been removed 90 days after the termination of your employment contract , as well as the contents of your respective account folders e-mails" to clarify the meaning of said claims, and in particular to clarify whether the above data contained in deliverable documents are no longer kept or there is difficulty in tracing them. of b) If he had informed the complainant about the cancellation of the e-mail account she maintained when she was employed by the company ..., 90 days after the termination of the employment contract, and if so, in what way, and finally invited her to send the Authority the written "Employee Personal Data Protection Statement", as well as to clarify whether and in what way it informs the employees of the company about its existence and content (generally all employees but also in this particular case the complainant). To the above questions, the complainant responded with her document under protocol no. C/EIS/2351/06-04-2021, stating the following: a) According to the Records Management & Data Retention Policy that applies to the complainant and its subsidiaries, is defined as mandatory deletion of the corporate e-mail account within 90 days of the 4 termination of the employment contract, i.e. as long as deemed necessary for business continuity purposes. It should be noted that during the absorption of ... by the complainant, due to the limited capacity of the servers, it was deemed necessary to delete all the corporate e-mail accounts of ... . However, the said deletion action was related to the employee's account and could not be extended to any sent emails that are scattered inside and outside the organization. In this context and given that the volume of these messages is huge and requires a disproportionate effort, invited the complainant to specify her request, b) The complainant, in addition to the "above limited data" does not process other personal data, such as e.g. evaluations, in addition to those delivered to the complainant, as this conflicts with the principle of "limitation of the storage period" imposed by Article 5 of the GDPR, c) regarding the prior or non-information of employees regarding the deactivation of their account in 90 days after the termination of the employment contract, the information in question was the responsibility of the employer, i.e. in this case the company ..., and after the acquisition of the company in question, the latter adopted the speech policies of the terminated company, and the employees were informed according to the termination of the employment relationship and the process of handing over the computer to the IT department, when they were asked to remove any personal files as they were informed that in 90 days the content of the account would be permanently deleted. In conclusion, it notes that its obligations

from the principle of accountability do not cover the acts and practices in general followed by ... in the year 2015. Finally, regarding the data protection statement of the employees (which the complainant sent to the Authority) stated that employees are informed about it at the time of their recruitment (and their training process), and it is available directly to every interested employee in the company's official internal Policy and Procedures information channel called "Corporate Documentation Library". 5 (since, as also stated in After the granting to the complainant, following her relevant request, of the complainant's reply letters, the complainant with her protocol number C/EIS/3001/07-05-2021 memorandum to the Authority, states that the complainant did not meet her obligations, pursuant to the provisions on the right of access and portability of data, stating at the same time that she herself was ... of both ... and the complainant C/EIS/2386/27-04-2021 supplementary document from … of … to … of … functionally moved to the offices of the complainant, staffing the … Directorate, using its logistical infrastructure, and participating in the evaluation of the complainant's executives for the year …), while in any case it is not disputed that it is for personal data located in the filing system of the complainant, regardless of the characterization of the mandate relationship. In addition, she adds that the fulfillment of the right of access was flawed, as she was not provided with copies of the evaluation reports, nor copies of her electronic communications from her e-mail account, nor data stored on her computer. Regarding the complainant's claim to delete the company account within 90 days of the termination of the employment contract, according to the "Record Management & Data Retention Policy", the complainant states that she was never notified of such a document before or during the termination of the relationship ..., which constitutes a violation of her right to information on the data concerning her, while the fact of deleting the account does not imply the deletion of the content of the e-mail, because the ability of a company to remove an e-mail address (e-mail) it is different and distinct from the content of the messages that have been exchanged, and the content of the messages is kept within the limitation period of any claims, since legal claims with former service providers may arise from it.... It also asks the Authority, if the complainant persists in her refusal to prove her claim, to conduct an on-site audit of the filing system, in order to establish whether copies of e-mail content and other electronic data are kept from the computers of the former ... of the complainant. Besides, the e-mails also have a recipient (other employees within the company) from where the complainant's e-mails could be searched. Finally, with regard to the evaluations, as stated by the complainant, the complainant has agreed that they are part of the data for which the twenty-year statute of limitations applies and therefore still adheres to them, while in accordance with the international standard BS 25999 for the "Business Continuity Management System » according to the ISO 22301 standard applied by the

complainant, copies are kept for security reasons, while an evaluation of the human potential is carried out, regardless of the employment relationship, and therefore, the complainant keeps the personal data requested by the complainant. Finally, the Authority, in its document under protocol no. C/EXE/1522/17-06-2021 to the complainant, asked her to provide the policies in relation to the retention of files related to e-mail accounts, including policies for security copies and action logs, and policies for dealing with events of forced deletion of user data in situations of risk of exhausting the capacity limits on storage media or in cases where it is deemed necessary to serve the implementation of changes in the system as well as to describe with how these policies have been implemented in practice. It also required her to produce any records from action logs maintained in relation to the procedures for deleting the complainant's account and its data. In response to the above document of the Authority, the complainant responded with her document under protocol no. with backups, the policy in relation to action logs, the policy in relation to incident response and the policy in relation to system changes. 7 In view of the above, the Authority called both parties before the Authority's Plenary Session on 19 -07-2021 in order to discuss the above complaint. During the hearing on 19-07-2021, the attorney of the complainant Vasilios Sotiropoulos appeared, after the complainant A, and on behalf of the complainant the attorneys Nikolaos Nikolinakos and Emmanuel Chalkiadakis appeared, while the Data Protection Officer of the complainant was also present at the hearing , B, in case there was a need for further clarifications, without however taking a position on the issues raised at the hearing. Both parties, after orally developing their views, were given a deadline during this meeting to submit memoranda to further support their claims and the complainant submitted in due time the memorandum No. G/EIS/5045/30-07-2021 her, and the complainant her memorandum No. Prot. C/EIS/5074/02-08-2021, with which they presented briefly, among other things, the following: In particular, the complainant during her above hearing, but also with No. C/EIS/5045/30-07-2021 with a hearing, she supported the following: a) the presence of the data protection officer of the defendant to defend the data controller before the Authority during the hearing conflicts with the obligations of independence that govern his role according to Article 38 para. 3 of the GDPR, b) the requirement to send the police identification card to satisfy the right of access is excessive and contrary to the principle of proportionality in a case cases such as this one, where the right is exercised by a former employee of the data controller; and the presentation of a copy of a police identity card was requested by the complainant on …, at which point the complainant sent it electronically, c) the communication of a … about … issues such as … which edited by the complainant are useful information for the company itself that have not been deleted, are kept by each company for the purposes of concluding and monitoring their correct

execution, d) all of the said information and documents that 8 were circulated through the complainant's e-mails as ... it is not only information related to her work ... but also information that refers to her as the subject of the data, since all of this information also includes information that refers to the complainant by name, such as the telephone and e-mail, with the result that all e-mail carried out in the context of the performance of the duties of a ..., as long as it is attributed to him by name, is also information that refers to him as a data subject and therefore includes personal data concerning him and has ' of them and the right of access. It also refers as relevant to the decision No. 186/2020 of the Supreme Court (A1 Civil Division), ..., in which the Supreme Court ruled that ".., this document was sent by the appellant (plaintiff) in the form of an attachment via e-mail to the legal representative of the company "... LTD" .... and therefore remained in the digital data of the company in question, as a result of which it is easy to access this data of e-mail messages with specific criteria, such as the date of sending, the sender, the subject, etc. Also, a critical issue in this case is not whether or not the respondent legally obtained knowledge of the appellant's personal data included in this document, but that, although the document in question came into his possession, he subsequently processed it further by presenting it as evidence document to the aforementioned Court and therefore using the information recorded therein, which concerned, among others, the amount of the appellant's remuneration, her bank account number and all her location details (exact address/telephone/ Email)". In addition, the complainant repeats in her memorandum that she participated in the evaluation process for the year ... carried out on ... of the same year (with the evaluator being the Head of the ... Directorate and with the participation of three of her colleagues), as an internal ... from the year ... she participated in the evaluations of the staff of ..., while after ... the evaluations are done electronically in 9 electronic forms through an information system. Next, the complainant states that there are at least ten certificates of participation in Vodafone's internal training program, which she wishes to receive. It also points out in its memorandum that the provider for the installation and management of the operating system for the evaluation of employees is the company UNISYSTEMS, and can, as the processor, forward the requested data to the complainant on behalf of the controller, while the physical file of both ... and Vodafone is contractually digitized and can therefore be traced electronically in a short period of time. In addition, the complainant cites in her memorandum the thesis published in the digital database of the University of Athens "Pergamos" entitled "Modern Human Resources Practices in Telecommunications Companies", of the year 2018, carried out with the cooperation of executives of the Human Resources Department of Vodafone, and in which the relevant Vodafone personnel evaluation process is recorded. From the above procedure, according to the allegations of the complainant, it follows that the

evaluation of the staff is also carried out in other periods as was done on ... of ... (and not only once a year). Regarding the personal data found on her laptop computer [such as working hours, participation in projects and other information about her work, which were recorded through the use of the "..." program used to organize of her work as ...] and which are maintained until today, the complainant repeats that they have not been granted to her until today without justification. Finally, the complainant points out in her memorandum that the data controller (the occupational doctor) also keeps her information regarding her health data (such as certificates of fitness for work, imaging tests, information about surgeries, her participation in the group insurance policy of its employees) and which have not been delivered to it. 10 The complainant through her attorney, during the above hearing of 19-07-2021, but also with the – timely filed – No. C/EIS/5074/02-08-2021 with a hearing supported her that: (i) Vodafone complied with the complainant's access request in a timely manner, pointing out that after receiving the complainant's request on …, it contacted her on …, requesting the completion of a relevant form and the presentation of a copy of the police ID, a form which the complainant in bad faith refused to complete and submit the relevant documents with her identification. However, the complainant did not insist on filling out the form but only on the need to present a copy of her identity card. As the complainant repeats in her memorandum, on ... she again asked the complainant to submit a document proving her identity, while informing her of the need to extend the response deadline until ..., due to the special conditions in the midst of the coronavirus pandemic, but and the passage of time since the end of the cooperation with Vodafone. In addition, the complainant states that, after thoroughly checking the warehouses containing all the material of the company "..." since the complainant's request as submitted on ... was incomplete, on ... he sent a new letter informing her that her file was ready and she could pick it up by showing her proof of identity, which the complainant eventually did via email on … . Therefore, according to the claims of the complainant, the complainant's request became complete and was duly submitted only on ... when the complainant sent a copy of her identity card, and Vodafone immediately (specifically the next day, i.e. on ...) proceeded to satisfy this. (ii) With reference to the complainant's allegations regarding the incomplete satisfaction of her request, the complainant pointed out that she provided the complainant with the entire individual work file (i.e. employee census card, educational qualification, CV, certificate of previous service, ADT, bank account number payroll, certificate of registration in the Fund …, 11 Certificate of Insurance in the Fund …, certificate …, all the agreements found as well as the no.), while it became impossible to locate any written evaluations of the complainant during the time she worked at Vodafone, while evaluations were not found in her files either ... because they did not exist, repeating that no written

evaluations had been carried out by Vodafone for its employees ... during the operational integration of the two companies. Referring to the evaluation process, the complainant explains with her memorandum that the evaluation was carried out after the end of the financial year (which starts on April 1 of each year until the end of March of the following year), while in the middle of each year, i.e. in the fall , an interim evaluation of each employee was carried out, through an oral discussion with the respective supervisor. (iii) Regarding the e-mail account maintained by the complainant, the complainant points out again with her memorandum that it was abolished 90 days after the termination of the employment contract, as was likewise the case with the contents of the respective folders of the e-mail account . Furthermore, in relation to data held in electronic form, the document "Records Management & Data Retention Policy" stipulates as mandatory the deletion of the company email account within 90 days of the termination of the employment contract. The complainant invokes the relevant decision No. NAIH/2020/34/3 of the Hungarian supervisory authority, in a case in which a former employee requested, in the framework of the exercise of the right of access under the GDPR, a copy of all corporate e-mail from the year 2018, which included, among other things, personal correspondence. In this decision, the Hungarian supervisory authority considered, inter alia, that the former employee's right of access could only be partially upheld, given the volume of e-mails requested, as well as the fact that the former employee did not specify which messages 12 of the professional messages, including e-mail, related to his request, while he should have specified his request so that it could be satisfied by the data controller. Likewise, the complainant invokes the December 2020 guidelines issued by the Danish data protection authority regarding the processing of personal data in the context of an employment relationship. According to these guidelines, the employer may deny the employee the right of access to correspondence related to his activity, e-mail, if he considers the relevant request to be excessive. In addition, the complainant relies on a decision of the Federal Labor Court of Germany1, which ruled that the data subject should specify the e-mails for which he wishes to receive a copy, otherwise the relevant claim is not considered sufficiently specified and as therefore it is not possible to satisfy him request. Finally, the complainant concludes that the exercise of the subject's right of access in a general way, which includes access to all corporate e-mail, cannot be considered as giving rise to an absolute obligation on the part of the data controller to grant all corporate e-mail correspondence (incoming and outgoing emails, as well as all emails from other employees that may contain information about the subject). (iv) It also mentions that as it has been judged both by jurisprudence but also supported by theory, the right to the protection of personal data is not absolute. Therefore, it is the duty of the data subject to indicate the specific corporate e-mail messages as well as files stored on

electronic devices, which contain data, in order to facilitate the controller in satisfying the right. (v) Next, the complainant points out that after a relevant audit that 1 See Decision BAG 27.04.2021- 2 AZR 34/20 of the Federal Labor Court of Germany. 13 was carried out, no medical data of the complainant was found in the records of …, nor information about automated decision-making or profiling. (vi) Finally, the complainant concludes by stating that based on the principle of data minimization, data for which there is no legitimate reason for retention must be deleted. The Authority, after examining all the elements of the file and after hearing the rapporteur and the assistant rapporteurs, who (assistants) withdrew after the discussion of the case and before the conference and decision-making, and after a thorough discussion, THOUGHT IN ACCORDANCE WITH THE LAW 1. Because, from the provisions of Articles 51 and 55 of the General Data Protection Regulation (Regulation 2016/679) and Article 9 of Law 4624/2019 (Government Gazette A´ 137) it follows that the Authority has the authority to supervise 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 f of the GDPR and 13 par. 1 item g' of Law 4624/2019 it follows that the Authority has the authority to take charge of A's complaint against Vodafone - PANAFON A.E.T. and to exercise, respectively, the powers granted to it by the provisions of articles 58 of the GDPR and 15 of Law 4624/2019. 2. 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 (…) ("purpose limitation"), c) are appropriate, relevant and limited to what is necessary for the purposes for which they are processed (" data minimization") (...)". 3. Because, according to the provisions of article 5 paragraph 2 of the GDPR, the data controller bears the responsibility and must be able to prove his compliance with the principles of processing established in paragraph 1 of article 5. As the Authority2 has judged, with the GDPR a new model of compliance was adopted, the central dimension of which is the principle of accountability in the context of which the data controller is obliged to plan, 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. In addition, the data controller is burdened with the further duty to prove himself and at all times his compliance with the principles of article 5 par. 1 GDPR. 4. Furthermore, in view of article 8 paragraph 1 of the Charter of Fundamental Rights of the European Union, article 9A of the Constitution and recital 4 of the GDPR, the right to the protection of personal data is not

absolute, but is assessed in relation with his function in society and is weighed against other fundamental rights, according to the principle of proportionality. The GDPR respects all fundamental rights and observes the freedoms and principles recognized in the Charter, as enshrined in the Treaties, in particular respect for private and family life, residence and communications, protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom of enterprise, the right to an effective remedy and an impartial tribunal, and cultural, religious and linguistic diversity. 5. Because, in accordance with the provision of article 12 paragraph 3 GDPR: "The data controller provides the data subject with information about the action 2 See Authority decision 26/2019, paragraph 8, available on its website. 15 carried out upon request pursuant to articles 15 to 22 without delay and in any case within one month of receipt of the request. This deadline may be extended by a further two months if necessary, taking into account the complexity of the request and the number of requests. The data controller shall inform the data subject of said extension within one month of receipt of the request, as well as of the reasons for the delay. If the data subject makes the request by electronic means, the information shall be provided, if possible, by electronic means, unless the data subject requests otherwise.' 6. Because according to the provision of article 12 paragraph 6 of the GDPR it is provided that "Without prejudice to article 11, when the data controller has reasonable doubts about the identity of the natural person submitting the request referred to in articles 15-21 , the controller may request the provision of additional information necessary to confirm the identity of the data subject." 7. Because according to article 15 par. 1, 3 and 4 of the GDPR "1. The data subject has the right to receive from the controller confirmation as to whether or not the personal data concerning him is being processed and, if so, the right to access the personal data and the following information: [...] 2. […] 3. The controller shall provide a copy of the personal data being processed. […] 4. The right to receive a copy referred to in paragraph 3 does not adversely affect the rights and freedoms of others.' 8. Because, according to recital no. 63 of the preamble of the GDPR "a data subject should have the right to access personal data collected and concerning him and be able to exercise this right freely and at reasonably regular intervals, in order to be aware of and to verify the legality of the processing". 16 9. Because, according to recital no. 64 of the preamble of the GDPR "The data controller should use all reasonable measures to verify the identity of the data subject who requests access, in particular in the context of online services and online identifiers'. 10. In view of the above, the standard forms used in order to exercise the right of access, although they facilitate the recognition of a right of access, its exercise is equally powerful if the subject submits it by letter, e-mail or verbally. Therefore, it is not mandatory to use the standard form and subjects are simply encouraged to use it3.

11. Because, in the case under consideration, from the data of the case file, the hearing procedure and the parties' memoranda, the following emerged: The complainant on ... sent a request by e-mail to the complainant, requesting full information regarding with the personal data that concerned her, copies of the personal data that the complainant keeps in her files (such as indicative certificates, evaluations, e-mails, correspondence) as well as all the information she requested under the General Data Protection Regulation in order to use them in view of pending litigation with the accused, submitting at the same time a request to limit the processing of her personal data. To the said request, the complainant replied on ..., asking the complainant to resend a request, filling in a specific standard form "for access to the data from external partners/former employees of Vodafone in order to be able to proceed with her request" (the which included fields about submitting the necessary identification documents) that the company had for this purpose, which 3 See the UK supervisory authority link – Information Commissioner's Office (ICO) https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection- regulation-gdpr/right-of-access/how-do-we-recognise-a-subject-access-request-sar/ 17 the complainant did not. Subsequently, on ... the complainant informed the complainant of the need to extend the deadline for responding to her request until ... stating the reasons for this extension, namely the extraordinary measures to deal with the coronavirus and the telecommuting implemented by the complainant, as well as the fact that a long time has passed since the end of her cooperation with the complainant, and at the same time she was asking her to attach proof of her identity. Finally, on ... the complainant sent a letter dated ..., in which she informed the complainant that she had prepared a copy of her personal data, and invited her to receive it by presenting a document proving her identity, a copy of which finally on ... the complainant sent by email to the complainant. document As for the complainant's claim that the complainant's request became complete as soon as she received a copy of her identity card, it is rejected, because in the present case it is judged that it was not necessary to present a copy of the complainant, taking into account the fact that the latter was a person known to the complainant and worked at her … as … in conjunction with the fact that verification of her identity could be achieved through telephone communication (given that the complainant's mobile phone number was listed in the application by which the right of access was exercised and was therefore known to the complainant). identification of the In addition, 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 (due to e.g. extraordinary conditions created by the coronavirus pandemic), on the other hand, it constitutes an obligation of the person in charge processing to document internally the reasons for delay or non-satisfaction of the

exercised rights4, while in the present case it must also be taken into account that the object of the activity of the responsible 4 See Decision of the Authority 32/2021, available on its website. 18 processing cannot be considered to be included in those that may be burdened by the emergency condition (such as hospitals in the case of the pandemic). Therefore, in the present case, from the data in the case file and also based on what emerged from the hearing process, it follows that the complainant, in violation of Article 12 para. 3 of the GDPR, did not inform the data subject within one month of receipt of the relevant request for the extension of the deadline provided for in this article as well as for the reasons for the delay. 12. Furthermore, from the submitted documents and the hearing process, it appears that the complainant's request regarding the granting of information and copies of personal data, concerned - among other things - literally: "Any personal data concerning me as a former ..., employed at ... Address, in any physical or digital file, by category of data, whether these are included in the employee's individual file (such as indicative certificates, Evaluations, Agreements, email, correspondence, etc.) including those kept by the occupational physician (of any nature health data), in any physical or digital medium, such as documents, opinions, certificates, conclusions, profiles, etc." As for the part of the complainant's request that concerned her being granted a copy of the electronic communications from the complainant's professional email address, in this case it appears that the complainant did not document the necessity of accessing specific professional email messages, nor did she specify which specific elements of the professional e-mail he wished to access and for what exact reason these are related to the trial which, according to the present complaint, has been opened and is pending before the Single-Member Court of First Instance X, given that in the present case the e-mails in question not only concern the complainant but also the complained company, which was also the administrator of the 19 e-mail account and according to article 15 paragraph 4 of the GDPR "The right to receive a copy referred to in paragraph 3 does not affect lives adversely to the rights and freedoms of others". Such a specialization would be necessary in order for the controller to be able to examine, within the framework of the principle of accountability, whether there is a question of an adverse effect on the rights and freedoms of others, and therefore whether there is a legitimate reason for not granting them. Rights of third parties that could possibly be affected are personal data of the other parties to the communication (sender - recipient), any information protected by any professional - commercial confidentiality, etc. It should be noted that, as can be seen from the information in the file, the complainant invited the complainant to specify the access request in the part that concerns any personal data contained in e-mails sent to current employees, in order to subsequently examine the possibility of satisfaction them in the light of conflict or non-conflict with provisions to ensure operational

confidentiality as well as with rights and freedoms of third parties, specialization in which however the complainant did not proceed. 13. As a result of the above, there is no need to consider the additional issue of deleting the company email account within 90 days after the termination of the employment contract. Besides, the complainant's further claim that she was not informed by the complainant about the aforementioned deletion of the e-mail account, can be examined on the basis of Law 2472/1997 since the termination of the employment contract dates back to a time prior to its entry into force of the GDPR, i.e. the year 2015. In accordance with the provisions of this law, the period of data processing and file retention constituted information, which the data controller had the obligation to notify the Authority, according to article 6 paragraph 1 e ', during the establishment and operation of the file or the start of the processing, but was not included in the data, for which, according to article 11 of the same law5, he had to inform against 5 According to article 11 of Law 2472/1997 "the controller must, during the stage of personal data collection, inform in an appropriate and clear manner the 20 stage of the collection of personal data personal character. Besides, the relative deletion of the e-mail account when an employee leaves the organization is expected and common knowledge of the diligent citizen6. 14. With reference to the rest of the information requested by the complainant with the access request (such as indicative certificates, Assessments, documents kept by the occupational doctor – all kinds of health data) and which were not granted to her by the complainant, neither from the information in the file nor it emerged from the hearing that the complainant maintains files containing the complainant's personal data that she has not provided to the complainant. 15. The Authority, taking into account the seriousness of the violation found, i.e. the delayed notification of the data subject by the Data Controller for the extension of the response to the right of access and the reasons for it, after one month has passed since the receipt of the request, in accordance with article 12 par. 3 of the GDPR, considers unanimously that it must exercise the right provided for in article 58 par. 2 sec. b GDPR its power and to issue a reprimand, as stated in the operative part of the present, which is judged to be proportional to the gravity of the violation found. FOR THESE REASONS The Authority, taking into account the above: Reprimands "Vodafone - PANAFON ANONIMI HELLENIKI ATEIREIA HELLENIKI TELECOMMUNICATIONS" subject to at least the following elements, based on article 58 par. 2 b' of Regulation (EU) 2016/679: a . his identity and the identity of any representative of him b. the purpose of the processing. c. the recipients or categories of recipients of the data. d. the existence of the right of access". 6 Regarding the issue of the management of e-mail messages for the time after the termination of the employment relationship, the Supervisory Authority of Belgium ruled with no.64/2020 decision of (https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-

fond-n-64-2020.pdf).

21

(VODAFONE-PANAFON S.A.E.T.) for the violation of the provision of article 12

par. 3 of Regulation (EU) 2016/679.

The president

Konstantinos Menudakos

The Secretary

Irini Papageorgopoulou

22