No. Fac.: 11.17.001.007.220 August 6, 2020 Decision in the form of an Order in accordance with the provisions of Article 58(2)(d) of the GDPR SUBJECT: Complaint by O.VI.E.K. – S.E.K. and S.E.V.E.T.Y.K. – PEO of the employees of KEO PLC, for a possible violation of the GDPR Bearing in mind the provisions of: (a) Articles 55(1), 56(2), 57(1)(a) and 58(2)(d) of the General Regulation (EU) 2016/679 and (b) of article 19(5) of Law 125(I)/2018, the following Order is issued: A. Facts: 1. On 14/10/2019, a complaint was submitted to my Office by representatives of O.VI.E.K. - S.E.K. and S.E.V.E.T.Y.K. – PEO (hereinafter Complainants) on behalf of the employees of the company KEO PLC (hereinafter Complainant), in relation to the replacement and upgrade of the card swipe system, so that it is consistent with modern technology and software systems. 1.1. Specifically, the representatives of the employees of O.VI.E.K. - S.E.K. and S.E.V.E.T.Y.K. - PEO to the Complaint, they claim that both the content of the Policy Statement and the Information Form entitled Upgrading the Entry/Exit Time Recording System, do not comply with the provisions of General Regulation (EU) 2016/679 (hereinafter GDPR). 1.2. In the form submitted to my Office, the use and duration of data retention, the processing of personal data, as well as the fact that the entry/exit card is an excessive measure, were briefly mentioned as matters to be investigated. 2. On 17/10/2019, an Officer of my Office, sent an email to XXXXXXXX of the Complainant's personnel department, requesting her position, on the allegations of the Complainants, until 11/11/2019, as well as a) Impact Assessment carried out for the effects/risks of using such a System (Article 35 of the GDPR), b) Activity Record, c) Posted Protection Policy and d) Data Protection Officer details of KEO PLC. Positions of the Plaintiff represented by a lawyer and attachments: 3. The lawyer of the Plaintiff, on 11/18/2019, sent a letter with her positions and opinions. On 12/30/2019, the Office raised various issues arising from the letter, which are recorded below as well as the appendices that the Defendant sent the complaint. On 14/02/2020, the lawyer of the Complainant sent a second reply letter. Together with the two letters he sent, he attached a) the Statement on the Protection of Personal Data of Employees and/or Representatives, b) the Time and Attendance System Upgrade Notice, c) the Impact Assessment, the Activity Record, d) the Privacy Statement Data in relation to Job Candidates and e) the KEO GENERAL DATA PROTECTION PRIVACY POLICY form, as Annexes. 3.1. In the two letters of the complainant, dated 18/11/2019 and 14/02/2020, the following are mentioned, among other things: 3.1.1. the complaint of the guilds does not appear to have been submitted by an organization whose statutory purposes include the protection of personal data or to have been submitted by the data subjects themselves. Therefore, it is not a legitimate complaint and to this end the Defendant reserves all her rights, 3.1.2. the Defendant, for the purposes of cooperation with my Office, considered it necessary to answer the Questionnaire dated

10/17/2019. In the event that the said complaint is submitted in a legitimate way in the future or if it is informed in the future that the said complaint is being officially investigated, then the Defendant reserves the right to present additional comments and positions in defense of her rights. 3.2. Kat'is sent the complaint on 3/10/2019, for GDPR compliance purposes, via e-mail and/or delivered by hand to the employees (Complainants) a Personal Data Protection Statement. 3.3. He did the same on 9/10/2019, where for the purposes of implementing the mentioned measure, he sent and/or delivered a separate notice in relation to the replacement and installation of the new card swipe system. 3.3.1. In said notice, the Complainant informed her staff that through the new devices they would collect, store and use the employee's card number, entry/exit date, entry/exit time and a low resolution photograph of the employee to the purpose of observing working hours and compliance with contractual obligations with the ultimate goal of time management and dealing with any complaints and disciplinary offences. 3.4. For the information of my Office, please attach the Employee and/or Agent Privacy Statement and the Time and Attendance System Upgrade Notice sent and/or delivered to the employees, respectively. 3.5. The position of the Complainant is that the replacement and installation of the said system as well as the processing of said data is necessary for the execution of an agreement between the Complainant and the Complainants as well as for the satisfaction of the legal interest that sought by the data controller (in this case the Complainant). At least one of the following cases of Article 6 of the GDPR applies to the processing in question, as it states: "b) The processing is necessary for the execution of a contract to which the data subject is a contracting party […..] f) the processing is necessary for the purposes of the legal interests pursued by the data controller or a third party" 3.6. For the information of my Office, he has attached the Impact Assessment. 3.7. It is the Plaintiff's position that the replacement and installation of the new card swipe system cannot be considered to be a reprehensible, unjustified or disproportionate action. The complainant previously used the card swipe system, collecting through this device the employee card number, date and time of entry/exit. The only substantial change with the replacement and installation of the new system is the collection and storage of a low-resolution photo of the employee and in this regard the Complainant has limited the photo retention time to one month as opposed to other data which it is necessary, as he claims, to be maintained for a longer period. Cases have arisen in the past where individuals have used another employee's card for purposes of circumventing the time rules. 2 3.8. The retention period for the rest of the data was set at 7 years, after taking into account the limitation periods applicable in relation to contractual disputes under Cypriot Law. In the Impact Report, it is stated that this issue will be re-evaluated and amended if deemed necessary. 3.9. The range of data kept has been limited to what is absolutely necessary,

the employee card number, the date and time of entry/exit and a low resolution photograph of the employee. Additionally, access to specific items has been restricted. 3.10. As Kathis states in the complaint, the present case does not concern video surveillance and the use of biometric systems, but rather the collection of a low-resolution photograph of the employee. However, it considers it appropriate to refer by analogy to the below reference of Opinion 2/2018 that I issued on 19/10/2018 based on Article 58(3)(b) of the GDPR on Video-surveillance in the workplace and the use of biometric systems, "Therefore, the use of biometric systems (facial recognition or fingerprinting) by employers, for the purpose of checking the time of arrival and departure of employees at their workplace, is prohibited. The controller must choose other means less intrusive/burdensome to human dignity than those entailed by the collection and use of fingerprints. As such means are, for example, the card swipe system, frequent/unannounced checks by the Manager/Supervisor in the card system, the presence of a supervisor in the area where the system operates, or alternatively, the placement of a surveillance camera above the card machine" . 3.11. The collection and processing of the employee's low-resolution photograph in combination with the card machine as a whole, as implemented by the Complainant, cannot be considered an excessive measure. On the contrary, it is a less burdensome and proportional measure (as opposed to a surveillance camera which would continuously video the specific points and would not be limited only to the moments when an employee taps his card). It concludes that this measure is consistent with the provisions of the GDPR. 3.12. The complainant, during the selection of the features of the mentioned card system, had extensive conversations and consultations with the provider of the system in question with a view to the best possible compliance with the GDPR. For this purpose, they requested and received legal tips. 3.13. For the information of my Office, the Activity Record of Ms. the complaint has been attached. 3.14. During the period of application of the GDPR, a team was operating, which consisted of people from the Directorate and the Personnel Department and who took all the necessary steps and measures for the Complainant's compliance with the GDPR. At this stage, the role of Data Protection Officer (hereinafter DPO) is performed by XXXXXXXXXX. 4. In a letter from the Office, dated 30/12/2019, to the lawyer of the Complainant, the content of which does not constitute an exhaustive list of the findings of my Office as several issues have been highlighted that need correction in the forms provided , the Complainant sent a reply letter on 14/2/2020, in which she states the following: 4.1. He notes the position of my Office regarding the legal form of the complaint and clarifies that the report concerned whether the employees of the Complainant were delegated in accordance with the directive, "Procedure for examining complaints". 4.2. He wishes to clarify that the low-resolution photo associated with the system in question is not

biometric data. In other words, the system in question does not collect biometric characteristics, which are unique, measurable, physical characteristics used 3 in order to recognize the identity of a person. Therefore, it is not necessary to find other ways since the system used is not a biometric data collection and processing system. 4.3. He believes that the system in question, which involves taking a low-resolution photo at the time of entry and swiping the card, instead of biometric data or continuous video recording, which will record the data subject for a few seconds as he arrives at work , is a measure which takes into account the principle of proportionality. 4.3.1. The replacement and implementation of the system in question was deemed necessary for the better implementation of the agreement between the Complainant and the Complainants (data subjects) and the satisfaction of the legal interest sought by the data controller (Article 6(b) and (f) of the GDPR). 4.3.2. Placing a camera that takes low-resolution photos (keeping them only for a month) and subsequently collecting and processing them, is not an excessive measure but a measure that takes into account the principle of proportionality. 4.3.3. The data collected by the said system is necessary for the intended purposes of the processing, i.e. the monitoring and evaluation of the observance of working hours and the compliance of contractual obligations with the ultimate goal of time management and dealing with any complaints and disciplinary offences. Retaining photos for one month is a proportionate measure. Relevant, as stated, the references in relation to Opinion 2/2018 of my Office on page 3 of the letter dated 11/18/2019. 4.4. In relation to the Declaration form for the Protection of Personal Data of Employees and/or Representatives (hereinafter Declaration) and other individual issues, notes the following: 4.4.1. In no case has the Defendant in the complaint relied on Article 6(1)(a) of the GDPR, which concerns securing the consent of the data subjects (in this case the Complainants). The Complainant sent and/or delivered the Statement to the data subjects and what she requested was confirmation of receipt of said documents and assurance of compliance with the Transparency Authority. 4.4.2. On page 7 of the Declaration, it clarifies that consent is not a condition of the employment contract, not even for the special categories. 4.4.3. On page 4 of the Declaration, the cases concerning the conditions of Article 6 are clearly stated with the relevant legal bases for processing and while there are specific legal bases in that part of the Declaration, there is nevertheless no reference to the consent provided for in Article 6(1)(a) of the GDPR. 4.5. The individual issues listed in my Office's letter dated 12/30/2019 and which, as I already mentioned, do not constitute an exhaustive list of my Office's findings, as several issues have been highlighted in the forms provided, are the following: - to do more clear and specific how the information is collected and why. Generality, eg we collect information about whether you have declared bankruptcy, is not sufficient. White criminal record information should be directly related to the

nature of the job. - there is confusing information, for existing employees and for potential employees. They must be separated and specified what concerns whom. - the form mentions a protection policy and generally a policy of the Complainant. Is this policy posted somewhere? Is it easily accessible? - the term particularly sensitive personal data is not valid, under the GDPR there is a special category of data. if the service provider is from a country within the EU, a third party is not understood. - 4 - if it is from a country outside the EU then an Assignment Agreement must be concluded pursuant to Article 28 GDPR. - the Need to Know Principle should be observed for everyone (employees and non-employees). - have procedures been established for the exercise of rights of access, erasure and restriction? Are they easily accessible? - the collection of data is done for a specific purpose and the necessary ones are requested. - who is the Company's Data Protection Officer? Contact info; 4.5.1. According to the complaint, she gives her own position on the above, as follows: - she considers that the Declaration under the circumstances is quite clear, but she is ready to proceed with its further review, in order to study the possibility of introducing amendments to make it even more understandable, especially in the point that it concerns the way and the reasons for which the data is collected, - with regard to the criminal record, it clarifies that the provision existed for the cases where for any reason an employee or representative voluntarily decides to present whether such information is sent by a third party to the Complainant, - recently, the external auditors of the Complainant, suggested that a certificate should be requested where the nature of the subject's work requires the presentation of a clean criminal record, - for the same reason there was also the provision regarding if someone becomes bankrupt, such information should be sent to the Complainant. - as provided in the Bankruptcy Law, notification of any decree declaring the debtor bankrupt is notified, among others, to the employer of the bankrupt, - indeed in the Declaration there are references to information collected during the stage before employing someone. This exists to cover cases where it is necessary to retain such information afterwards, i.e. at the stage when someone becomes an employee, - for people who simply remain "potential employees" there is a separate data protection statement, which has been attached as Annex A to letter dated 14/2/2020. Therefore, no further separation should be made in the Statement, which concerns persons who have become employed, - there is a more general and more concise document regarding the personal data protection policy of the Complainant in relation to all employees/Complainants, as well as a form that can be given by the ombudsman's Office of the Complainant in case it is requested by anyone (Appendix B of the letter dated 2/14/2020). This document will also be posted on the complainant's website, where there is already a special data protection policy for the use of the website. - the reason the term "sensitive personal data" was used is because it is widely

used, as for example by the European Commission itself on its website when it provides explanations for the legal reasons for processing with reference to the GDPR itself. There are also such references in recitals 10 & 51 of the GDPR. - in any case it is clarified that the Complainant does not send information about employees outside the EU. - the only service provider of the Complainant that personally processes the data of its employees (Complainants) is the company that provides the SAP system ERP. A relevant assignment contract has been prepared between the complainant and the provider, which will be signed by 2/29/2020, - the Complainant aims and seeks to create and implement procedures and culture in the workplace that limit access to data concerning the employees (Complainants) in such a way that access is only available to the people who need to have access, - the According to the complaint, it has established procedures for exercising the rights of access, erasure and restriction, which are contained in a form that can be given by the DPO to case requested by any employee. 5 - the Complainant understands that any information she collects and maintains about the subjects is because such a thing has become necessary for the purposes of a working relationship. After all, this is the main purpose of the Complainant's compliance, - the Complainant understands that full compliance with this principle in a workplace requires a culture change from all parties involved and from everyone without exception, - until the previous DPO was XXXXXXXXXXXX, which, however, is leaving after the complaint, therefore procedures are being carried out to appoint a new DPO. 4.6. Furthermore, the Time and Attendance System Upgrade form, which consists of almost three pages, has provided all the necessary information in relation to the replacement and installation of the new system, so that the staff receives the necessary information about the system. 4.7. In relation to the concern raised as to whether the low resolution photograph will undergo any special processing, the Complainant states that the low resolution photographs collected by the entry/exit recording system will not be transferred or stored in the SAP ERP software but on the Complainant's server with limited access. The time entry/exit recording system is a completely separate system from SAP ERP. The Defendant in the complaint confirms that no special treatment will be given to the low resolution photos. 4.8. The SAP ERP people are employees of a third party independent company, which provides the system to the Complainant. This system stores all the data collected with the new devices, except for low-resolution photos, and is only accessible to people in the Human Resources Department and the IT Department. 4.9. As stated in the Impact Assessment form carried out, SAP ERP people have access to the software, only after authorization from the Complainant for the purpose of upgrading the software or repairing any damage that may occur in the software, which cannot be repaired by the IT Department of the Complainant. 4.10. According to the complaint, the time of

one month to preserve the low-resolution photos is accordingly legitimate. 4.10.1. Regarding the retention of data related to the time and date of entry and exit to the workplace, the retention period has at this stage been set at 7 years, since limitation periods under Cypriot Law regarding contractual disputes (6 years) were taken into account. and civil offenses (3 years). 4.10.2. It is possible in relation to an employee (Complainant) that a legal dispute may arise regarding issues for which the limitation period for the transferable rights according to Cypriot Law amounts to 6 years and the entry/exit data may be relevant evidence in such cases. 4.10.3. It is possible for a case to arise with an employee (Complainant) and the Complainant, except those included in the jurisdiction of the Labor Disputes Court, for which the limitation period is shorter. For this reason, the Complainant received legal advice, such as keeping such data for a period of 7 years, except of course in cases where a case arises, where the data related to the case will be kept for as long as the case is pending. 4.10.4. The retention of the specific data for a period of 7 years is not an excessive period as the input/output data in the workplace is not of such a nature as to create a serious risk to the rights and freedoms of the data subjects (Complainants). At the same time, it remains at the disposal of my Office to discuss and adjust this detail accordingly in the future as the system has only recently been implemented. 5. Subsequently, on 12/3/2020, an Officer of my Office, sent an electronic message to the Complainant's DPO, informing him of the allegations of the Complainant, asking for his positions and opinions until 13/4/ 2020. Positions of Complainants who are represented by a lawyer: 6. On 13/4/2020, the lawyer of the Complainants sent a letter with the positions and opinions of his clients, as follows: 6.1. In order to answer the question of whether the Complainant is authorized to photograph the Complainants/employees upon their entry/exit from employment, the legislative framework within which the Complainant may proceed to said processing. 6.1.1. According to the Principles provided for in Article 5 of the GDPR and concludes that the adoption of the measure of taking a photo of the employee during the entry/exit process may be allowed, only when the employer is able to justify the legality and necessity of the control and of monitoring and when there is no other less intrusive way to achieve the purposes it seeks. 6.1.2. The positions and reasons put forward by the Complainant for the installation of the upgraded photo card system can be satisfied both with the existing card system and by adopting other methods such as frequent unannounced checks by a Supervisor on the system card or even with the presence of a supervisor in the area where the card system operates. 6.1.3. Furthermore, the Complainant did not indicate the reasons why it was deemed necessary and/or necessary to upgrade the card system. The defendant in the complaint was content with a simple mention of the purposes without documenting the necessity that led her to this decision. 6.1.4. Since the photograph to be

taken identifies the employee, even though it is of low resolution, it falls under the interpretation of the term "personal data". 6.1.5. Given the Principle of Proportionality, taking a photograph of the employee constitutes an intrusive measure that limits the right to privacy and does not even serve the purposes that the Complainant stated that she wants to serve. 6.1.6. It expected that the Plaintiff, as the Processor before the upgrade of the card system, would try to find a balance between the legitimate interest of protecting her rights and the fundamental right of protecting the privacy of her employees. 6.2. Regarding the data retention period, the retention period is defined as the period necessary to satisfy the purposes for which the controller collects the data. 6.2.1. In the present case, the Complainant informed that the data concerning the time and date of entry and exit to the workplace are 7 years old. In calculating the time period in question, the limitation periods provided for by the Limitation Law were taken into account, i.e. 6 years for contracts and 3 years for civil offences. 6.2.2. The reasoning is correct but the calculation by the Complainant is wrong given that any difference arising in relation to the entry/exit hours of the employees 7 will be reduced to a labor dispute and therefore should be taken into account limitation period for labor disputes, which amounts to 12 months. 6.3. In the SEP ERP system software, employee data is correctly entered. However, Kathis will have to explain and justify the complaint as to whether there is a reason to register data on KEO PLC's server. In addition, the issue of a signed delegation agreement between the Complainant and the company that operates the SEP ERP system is also raised. 6.4. Concluding, on the positions of the Complainants, he stated that taking a photo of the employees is not necessary to protect the legal interests of the Complainant, since this can be ensured in less burdensome ways, while in any case the retention period of the entry/exit card data should be limited to a maximum of 2 years. B. Legal analysis: 7. The photograph of a natural person, to the extent that his identity is immediately or indirectly revealed, constitutes "personal data", according to the definition given in Article 4 of the GDPR, which defines that "personal data " is "any information concerning an identified or identifiable natural person (data subject)". 7.1. The same article also defines as processing "any act or series of acts carried out with or without the use of automated means, on personal data or sets of personal data, such as collection, registration, organization, structuring, storage, the adaptation or alteration, retrieval, retrieval of information, use, disclosure by transmission, dissemination or any other form of disposal, association or combination, the restriction, erasure or destruction". 7.2. Further, a controller is defined as anyone (the natural or legal person, public authority, agency or other entity) who, "alone or jointly with another, determine the purposes and manner of processing personal data". 7.3. In addition, it defines as "filing system": any structured set of personal data that is accessible according to specific criteria, whether this set is centralized or

decentralized or distributed on a functional or geographical basis. 8. In Article 5 of the GDPR, the Principles governing the processing of personal data are defined as follows: "1. Personal data: "... c) are appropriate, relevant and limited to what is necessary for the purposes for which they are processed ("data minimization"), ... e) are kept in a form that allows the identification of the data subjects only for the period required for the purposes of processing 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 as long as the appropriate technical and organizational measures required by this regulation are applied to ensure the rights and freedoms of the storage period"),... 2. The data controller bears the responsibility and is in position to demonstrate compliance with paragraph 1 ('accountability sia")". of the data subject ("restriction 8.1. Based on the Data Minimization Principle established by Article 5(1)(c) of the GDPR, the Complainant must, in any case, ensure that the personal data are appropriate, relevant and limited to what is necessary for the purposes for which they are processed and based on the Principle of the limitation of the storage period, which establishes Article 5(1)(e) of the GDPR, the data must be kept in a form that allows the identification of the data subjects only for the period necessary to achieve the purposes of the processing. 8 8.2. In Reason 39 of the Preamble of the GDPR it is explained, among other things, that "Personal data should be sufficient and relevant and limited to what is necessary for the purposes of their processing.This requires in particular to ensure that the period of storage of personal data is limited to the minimum possible. Personal data should only be processed if the purpose of the processing cannot be achieved by other means." 8.3. Recital 4 of the GDPR's Preamble explains that, "the right to the protection of personal data is not an absolute right; it must be assessed in relation to its function in society and weighed against other fundamental rights, in accordance with the principle of proportionality ». 8.4. Further, Recital 47 explains that, "The legitimate interests of the controller, including those of a controller to whom the personal data may be disclosed or of third parties, may provide the legal basis for the processing, provided that they are not overridden of the interests or fundamental rights and freedoms of the data subject, taking into account the legitimate expectations of the data subjects based on their relationship with the controller". 8.5. Related to the issue are also, (a) Opinion no. 06/2014 on the concept of legitimate interests of the controller issued on 9/4/2014 by the Article 29 Working Party on data protection, (b) the Opinion of the Article 29 GDPR Working Party entitled "Opinion 2 /2017 on data processing at work", (c) paragraph 9 of Article 35 of the GDPR, in which it is stated that "Where appropriate, the data controller requests the opinion of the data subjects or their representatives

on the planned processing, with the reservation of the protection of commercial or public interests or the security of processing operations" (d) the Opinion 2/2018 issued by the Commissioner for the Protection of Personal Data under Article 58(3)(b) of the GDPR on Video-surveillance in the premises work and the use of biometric systems and (e) Directive 1/2011 issued by the Greek Personal Data Protection Authority for the Use of video surveillance systems for the protection of persons and goods. 9. In Article 35(9) of the GDPR regarding the Data Protection Impact Assessment and which states that "Where appropriate, the data controller shall seek the opinion of the data subjects or their representatives on the planned processing, subject the protection of commercial or public interests or the security of processing operations'. 10. The 2012 Law on Limitation of Transferable Rights, as amended (hereinafter Law 66(I)/2012). 11. In Article 12.(10A) of the Annual Leave with Benefits Law of 1967 (hereinafter L. 8/1967) it is stated that "An application to the Labor Disputes Court shall be submitted within twelve months from the date on which the matter to be submitted arose right of application or within nine months from the response of the Fund for redundant staff..." C. Commentary: 12. It is the position of the lawyer of the Complainant that for the replacement and installation of the card system as well as for the processing of the data, apply, at least one of the following cases of Article 6 of the GDPR: "b) Processing is necessary for the execution of a contract to which the data subject is a contracting party [.....] f) processing is necessary for the purposes of legal interests pursued by the controller or a third party...". 12.1. In order for item b) of Article 6(1) of the GDPR to be used as a legal basis, an express provision should be included in the employment contract signed between Defendant 9 in the complaint and the data subjects (employees). No such evidence was produced before me. 12.1.1. However, even if there was an express provision in the employment contract, this would be examined in the light of Article 7(4) of the GDPR and whether the consent of the data subject (employee) is freely given. As mentioned in the letter from my Office dated 12/30/2019, the employer is considered to have a dominant position in the employment relationship, therefore the employee's consent is not considered free. 12.2. With regard to Article 6(1)(f) of the GDPR, I accept that it could be used as a legal basis, provided that the processing of the subjects' (employees') data, i.e. the taking and storage of their photograph, obeys the Principles of proportionality, limitation of the storage period and accountability and in any case does not override the interests or fundamental rights and freedoms of the data subjects. 13. Accordingly, in the present case, I am required to consider (a) whether the installation of a camera by the Plaintiff for the purpose of taking a low-resolution photograph of the data subject (employee) to identify that the employee swiping the card is its owner and not a third party, as a control measure, obeys the Data Minimization Principle and (b) whether the retention time of employee entry/exit data

(employee card number, date and time of entry/exit) for a period seven years, for the purposes of resolving labor disputes or for the exercise of conductive rights, is subject to the Principle of the Limitation of the Storage Period. 14. Regarding question 13(a), I take into account the following: 14.1. In the Impact Assessment carried out by the Complainant, on page 5, in the paragraph entitled STEP 3: Consultation process, it is stated that: "The advice of the subjects was not sought, nor of their representatives, as the recording and time data management has always existed as part of Personnel Management.' 14.2. In the letter of the lawyer of the Complainant dated 11/18/2019, on page 2, it is stated that: ".... In any case, KEO used the card swipe system in the past, collecting through this device the employee's card number, date and time of entry/exit. That is, the only substantial change in the card swipe system is the collection and storage of the employee's low-resolution photo, and therefore KEO has limited the photo retention time to one month in contrast to other data that needs to be retained for longer period of time..." 14.3. In the Impact Assessment carried out by the Complainant, on pages 5 and 6, in the paragraph entitled STEP 4: Proportionality and Necessity Assessment, it is stated that: "1. The time recording devices are necessary for the Company to execute the contract together with its employees and for the protection of its legal interest or that of a third party. Bearing in mind the conditions of the Company there does not seem to be any other way of processing by which the Company can adequately monitor and evaluate the observance of working hours and detect any disciplinary offences. It is noted that in the past there have been incidents where people swiped another colleague's card. In any case, we consider that through the devices only the data that is necessary to serve the stated purposes is collected and stored. 14.4. In addition, in the letter of the lawyer of the Complainant, dated 18/11/2019, on page 3, it is stated that: 10 (facial recognition "… We also consider it appropriate to refer to Opinion 2/2018 which was issued by the Office of the Commissioner for Personal Data Protection under Article 58(3)(b) of the General Data Protection Regulation (Regulation (EU) 2016/679) for Video-surveillance in the workplace and the use of biometric systems. Although the present case does not concern video-surveillance and the use of biometric systems but concerns photo collection low resolution of the employee, we consider it appropriate to refer by analogy to the reference below contained in the document in question: "Therefore, the use of biometric recognition systems or fingerprinting) by employers, for the purpose of checking the time of arrival and departure of employees at the site their work, is prohibited. The controller must choose other means less intrusive/burdensome to human dignity than those entailed by the collection and use of fingerprints. As such means are, for example, the card swipe system, frequent/unannounced checks by the Manager/Supervisor in the card system, the presence of a supervisor in the area where the system operates, or alternatively,

the placement of a surveillance camera above the card machine” . Therefore, we consider that the collection and processing of the employee's low-resolution photo in conjunction with the card machine as a whole as implemented by our customers, cannot be considered an excessive measure (as opposed to, for example, a surveillance camera which would continuously videotaped the specific points and would not be limited only to the moments when an employee taps his card) to achieve the above-mentioned purposes of the KEO. This measure is therefore consistent with the provisions of the General Data Protection Regulation...". 14.5. Additionally, in the letter dated 2/14/2020, the Plaintiff's attorney states that: "... our clients wish to clarify that the low-resolution photo associated with the system in question does not constitute biometric data. In other words, the system in question does not collect biometric characteristics, which are unique, measurable, physical features used to identify a person. It is therefore not considered necessary to find other ways since the system used is not a biometric data collection and processing system...". 14.6. All of the above references contained in the Impact Assessment and the Complainant's solicitor's letters explain that taking a low-resolution photograph of the data subject was the only practical solution for the purposes the Complainant sought to serve. I do not rule out that, in some cases, taking a photo or video, as I mention in Directive 2/2018, when the card is swiped, may be mandatory. However, in such cases, based on the Principle of Accountability, the employer should be able to demonstrate that there is no other less intrusive way to achieve the intended purpose, namely the effective control of employees. 14.7. In the present case, the Defendant has not substantiated the complaint, nor has it emerged at any stage that other methods and measures were applied on her part, e.g. the frequent/unannounced checks by the Manager/Supervisor on the card system, the presence of a supervisor in the area where the system works or even the camera, which would focus on the hands of the employees when they tap the card and not on the face , and be judged as ineffective or as inappropriate or insufficient, so as to confirm the choice of taking a low-resolution photo, as the most appropriate measure to serve the purposes pursued by the Complainant. In the employment context, monitoring measures that capture employee behavior must be proportionate to the risks they face and implemented in the least intrusive manner. 14.8. Therefore, in relation to the question (a) that I ask in paragraph 11 above, the position of Ms. that, the installation of a camera for the purpose of taking a low-resolution photo of the data subject (employee) to identify that the employee who taps the card is its owner and not a third party, as a control measure, it obeys the Data Minimization Principle, 11 is rejected, since the Defendant did not take or consider taking other less intrusive measures, before implementing measure of this. 15. Regarding question 13(b), I took into account the following: 15.1. In the Impact Assessment carried out by the

Complainant, on page 2, in the paragraph entitled Nature of Processing, it is stated that: "... The data in relation to the employee card number, the time and date of entry and exit to the workplace may be kept for a period of up to seven (7) years from the date of their collection unless there is a pending legal proceeding and/or contractual dispute where the data will be kept for a longer period for the purposes of establishing, exercising and defending legal claims..." 15.2. On page 5, of the same Impact Assessment, in the paragraph entitled STEP 3: Consultation process, it is stated that: "The consultation of the data subjects was not sought, nor were their representatives as well as the recording and management of time data existed always as part of Personnel Management…". 15.3. Additionally, on page 7 of the same Impact Assessment, in the paragraph entitled STEP 4: Proportionality and Necessity Assessment, it is stated that: "7. … The rest of the data was deemed appropriate, at least at this stage, to be kept for a period of 7 years bearing in mind the limitation periods that apply to breach of contractual relationship under Cypriot Law. As explained below the issue of retention time will be re-evaluated in the near future and in particular after the appointment of a DPO". 15.4. In the letter of the lawyer of the Complaint dated 18/11/2019, on page 3, it is stated that: "... In terms of the retention of the remaining data, the retention period has at this stage been set at 7 years taking into account the limitation periods applicable under Cypriot Law regarding contractual disputes. However, as explained in the Impact Report (Appendix C), this issue will be re-evaluated and amended if deemed necessary. We also note that the range of data kept is limited to what is absolutely necessary, i.e. the data concerning the employee's card number, the date and time of entry/exit and the employee's low-resolution photo. In addition, we note that, as explained in Appendix C, access to specific data has been restricted..." 15.5. Additionally, in the letter dated 14/2/2020, the lawyer of the Plaintiff states that: "... Regarding the retention of the data concerning the time and date of entry and exit to the workplace, it is noted that the retention period has at this stage been set at 7 years taking into account the limitation periods under Cypriot Law regarding contractual disputes (6 years) and civil offenses (3 years). From what we understand, it is possible in relation to an employee that legal disputes may arise regarding issues for which the limitation period for transferable rights according to Cypriot Law amounts to 6 years. Entry and exit records may be relevant evidence in such cases. That is, in relation to an employee, a case may arise other than those included in the jurisdiction of the Labor Disputes Court for which the limitation period is shorter. It is for this reason that we have advised our clients to keep such data for a period of 7 years except of course in the cases where a case arises and such data should, if relevant, be kept for as long as the litigation is pending.Finally, with regard to this issue, we consider that objectively speaking the maintenance of suchof data for 7 years is not an excessive period as the data containing

the time

entry and exit to the workplace is not of such a nature as to create a serious

12

risk to the rights and freedoms of subjects (emphasis mine).

But at the same time we remain at your disposal to discuss and adjust

depending on this detail in the future as the system has only recently been put into

application…".

15.6. In summary, Kat'is claims that, the period of storage of the data of its employees

for a period of seven (7) years is absolutely necessary because it may arise between the Defendant and

of its employees a conductive right, which, based on Law 66(I)/2012, as amended, provides

limitation periods of six (6) years for contracts and three (3) years for civil offences. On the contrary, the

lawyers of the complainants claim that any difference between the Accused and the

of its employees will be of a labor nature, which will have to be resolved before the Court

Labor Disputes, meaning, in accordance with the provisions of article 12(10A) of Law 8/1967, as

amended, which, inter alia, provide that: “Application to the Labor Court

submitted within twelve months from the date on which the matter to be submitted arose

right of application or within nine months from the response of the Fund for redundant personnel".

15.7. I am of the opinion that both positions suffer because neither Law 66(I)/2012 nor Law 8/1967

is a legal basis for determining the storage period of the data in question. And the

two Acts provide for periods within which respective rights may be exercised, however

they do not, at the same time, create an obligation to maintain any data for the purpose of exercising them

of the rights. Besides, if I accepted the positions that, these Laws could constitute

criterion for determining the storage time of the data in question, I would arrive at

paradoxical conclusion that, all data collected by all controllers who

fall within the scope of the GDPR, they should be stored for periods commensurate with them

provided by their national laws for the resolution of labor and civil disputes, respectively,

which circumvents both the letter and the spirit of the GDPR.

15.8. The data in question, i.e. employee card number, date and time of entry/
exit of each employee, are stored in the system installed by Kat'is, for a long time
specific purposes, namely time control and payroll and, based on
the Beginning of the Storage Period, sole factor/criterion for determining the period
of their storage, in a form that allows the identification of employees, must be the time
required to fulfill these purposes. Their storage for longer periods,
it can only be done for archival purposes in the public interest or for scientific purposes
or historical research or for statistical purposes. In this case, these purposes do not
are applicable, or at least, the Court has not put them before me. Hence her position
the Defendant that the data storage period of its employees for a period of seven (7) years is
absolutely necessary, it is rejected.

16. Furthermore, it should be taken into account that the decision of the Complainant to establish
low-resolution camera and its decision to retain employee data for a period
seven (7) years, were taken without having previously been consulted with the employees or
their guilds.

16.1. The lawyer of the Complainant in the impact assessment he sent states that no
the advice of neither the employees nor their representatives was requested as well as the recording and
time data management has always existed as part of Personnel Management. The fact that the
According to the complaint, it previously collected and kept data without justifying the time
guarding them, this does not mean that he can continue to do so and furthermore, he could at
in the context of this system upgrade to carry out a consultation with the stakeholders,
so as to correct any distortions of the past.

16.2. In addition to the fact that, based on Article 35(9) of the GDPR, the Defendant, when preparing the complaint
impact assessment was appropriate to seek the opinion of its employees or their representatives,
for measures he intended to take, this was also imposed by the Principle of Transparency.

16.3. For the purposes of transparency, the participation of employee representatives (e.g.

guilds) during the discussions that take place before taking measures involving the

13

control and/or supervision of staff through the processing of their personal data.

The following excerpt from the Opinion of the Article 29 Working Group, "Opinion

2/2017 on data processing at work»:

"6.3 Transparency

Effective communication should be provided to employees regarding any monitoring that takes place

place, the purposes for this monitoring and the circumstances, as well as possibilities for employees

to prevent their data being captured by monitoring technologies. Policies and rules concerning

legitimate monitoring must be clear and readily accessible. The Working Party recommends

involving a representative sample of employees in the creation and evaluation of such rules and

policies as most monitoring has the potential to infringe on the private lives of employees."

D. Conclusion – Conclusion:

17. In light of the above and exercising the powers granted to me by the provisions of the Article

58(1)(d) I inform the Defendant of the complaint that:

17.1. In relation to the question (a) I ask in par. 13 above, the installation of a camera by

Each for the purpose of taking a low-resolution photo of the data subject (employee)

to identify that the employee who taps the card is its owner and not a third party, as

control measure, without considering or considering the adoption of other less intrusive ones

measures, before the implementation of this measure, violates the Data Minimization Principle

and therefore cannot be accepted.

17.2. In relation to the question (b) I ask in par. 13 above, the data retention time

entry/exit of employees (employee card number, date and time of entry/exit) for

period of seven (7) years, for the purposes of exercising conductive rights, violates its Authority

Limitation of the Storage Period.

17.3. Pursuant to Article 58(2) of the GDPR, I have the power to impose an administrative sanction on the Defendant for above violations, which includes the possibility of imposing an administrative fine based on Article 83 thereof. However, taking into account:

(a) all the factors set out in Article 83(2) of the GDPR,

(b) that, at all stages of the examination of this complaint, the Complainant had the complaint cooperation with my Office,

(c) that, the case could have been avoided if the Plaintiff had consulted the measures taken with its employees or their representatives;

(d) that the Complainant has taken sufficient measures to comply with the GDPR, in particular as regards concerns the obligation to inform its employees and

exercising the powers granted to me by the provisions of Article 58(2).(d) of the GDPR, I consider more appropriate in the first phase, to give the complainant the following order:

(a) suspend the installation of the upgraded card swipe system which includes the installation of a camera and to destroy the material it has collected, if the receipt of this and inform my Office of the actions and

(b) to choose through transparent procedures, with the participation of their representatives of employees, differentiated measures/solutions which are appropriate and sufficient and the which ensure the guarantees of legality, transparency, conservation, proportionality and security of personal data and as a draft of art due to procedures until 4/12/2020.

17.4. In the event that the Complainant does not comply with the above order within the above mentioned deadlines, I will consider the necessity of taking stricter administrative measures against her.

Irini Loizidou – Nikolaidou

Protection Commissioner

Personal Data

15