No. Fax.: 11.17.001.010.052 No. Tel: 22 818456 No. Fax: 22 304565 Email: commissioner@dataprotection.gov.cy

DUPLICATED AND BY ELECTRONIC MAIL January 16, 2023 DECISION in the form of Orders regarding a complaint against A&A HOTELS SHOPS 1. Facts / Positions of Parties 1.1 On 21/3/2022 we received a complaint against of XXXXXX regarding the operation of Closed Circuit Video Surveillance (CCV) at the XXXXXX store at METROPOLIS Mall in Larnaca. According to the claim of the complainant, she was being monitored by KKKP with constant observations and pressures by phone and very few times in writing. He added that the surveillance system was by video and voice and that he was fired from the job by calling for CCTV footage. 1.2. With our email dated 11/4/2022 we informed about the receipt of the complaint and the positions of the complainant. We also requested that we have the positions of Professor until 25/4/2022 as well as the relevant supporting documents for these positions. 1.3. On 4/29/2022 we received your letter via e-mail where you mentioned that: i. Acting at the behest of your customers XXXXXXX. ii. You have received our email on 11/4/2022. iii. We do not mention the name of the complainant but it is obvious that it is iv. for their employee. The PPE was installed by a licensed company. 1 The CCTV was intended for store security The CCTV does not have an audio recording system, according to a certificate from the company that installed it (you have attached a certificate). v. vi. vii. The complainant was aware of the existence of the KKKP. viii. The complainant controlled the KKBP. ix. The video recorder was located next to the cash register where the complainant was working and monitoring. x. The complainant broke a figurine in the store. He concealed and denied the fact by quoting to us a conversation dated 19/3/2022 which took place between the complainant and Mr. Antonis (store owner). You added that it appears from the conversation that the complainant herself urged the Professor to see what was done through the CCCP. xi. The Defendant has not violated any provision of the legislation on the protection of personal data. 1.4. With our email dated 13/5/2022, we requested that you notify us of an appointment document to represent the Professor before my Office, since as you mentioned in your email dated 29/4/2022 acts on the order of the Professor. 1.5. On 7/6/2022 you notified us of the requested appointment document. 1.6. With our email dated 4/7/2022 we reported that the complainant after submitting her complaint shared with us a video where she had audio. In particular, the video in question contained part of the interior of the store, while music is playing, showing that it is possible to receive audio. We mentioned that we have communication (screenshots) showing an exchange of messages, in the first case between the complainant and a certain Mr. XXXXXX and in the second case between the complainant and a certain Ms. XXXXXXX. Specifically, in the first case, the communication was as follows: "Mr. XXXXXX: Watch it and tell me Complainant: XXXXXX I'm waiting for the video to have a complete picture and

get you when you comment so we can talk Mr. XXXXXX: XXXXXX I prefer you to come now that we are in Larnaca to us you bring the key and we will stop the cooperation and talk about whatever you want. Complainant: Ok I'll bring you the keys, we don't need to discuss anything else. Thank you" In the second case, the communication was apparently in two different records, as follows: First record "Mrs XXXXXX: Is there anyone? Complainant: Yes, there are people today, I entered the store, many people were excited, ok...I have 123 euros. I think there will be more people in the afternoon Ms. XXXXXX: Did you have foreigners? Complainant: Not many one got earrings and one who wanted the bag I asked price for...but she didn't get it Ms. XXXXXX: Did you check the bag for its price? She who was with a baby were strangers?' 2 the sound Second recording "Ms. XXXXXX: XXXXXX I just happened to be watching the cameras. It is not right for him to have a client and you to be holding a wing. He saw the gourds, you could explain what they are. Complainant: She was a stranger if you look further I talked to her I told her her skirt is nice she told me it's from wrinkles I told her she has a nice style and I thought it was right that she doesn't feel like I'm watching her or that I'm doing something...my mistake" We added that , in your e-mail dated 29/4/2022 you listed your positions: i. That the closed surveillance system, which was installed by a licensed company, was intended for the security of the store, which does not have an audio recording system. In this regard, you have attached a relevant certificate from the syncview company. ii. You stated that the complainant was aware of the system in question, which she controlled, adding that the image recording device was located next to the cash registers that she monitored and worked on. iii. You quoted a conversation between the complainant and Mr. XXXXXX where the complainant was urging your clients to look on CCTV for what was done regarding an incident of a statuette being broken. We have requested that by 19/7/2022 we have your positions regarding the allegations of: i. Monitoring the complainant's movements that appear to take place during her work. The proven ii. the CCTV and which you have assured us otherwise. iii. The legal basis for the installation and operation of Closed Circuit Video Surveillance (see article 6 of the Regulation). Conducting an impact assessment. iv. v. The total number of cameras and where they are located. vi. The shooting angle of said cameras (attach screenshot). vii. The posted informational/warning signs regarding the operation of the Closed Circuit Video Surveillance. How many and in which places. Which persons have access to said system in any way. viii. ix. Communicate with us in support of your positions. 1.7. On 8/31/2022 we received your letter via e-mail stating that: i. Apologies for the delay in sending your reply. ii. As we send you the screenshots. iii. Explain how the messages were exchanged. iv. Who printed the screenshots and under what circumstances. v. We are sending evidence to show our claim that 'proven vi. You sent 10 photos and a letter from the

company XXXXXXX where as a closed video surveillance system it has sound.' you mentioned "the contents of which speak for themselves". 1.8. With our email dated 7/9/2022 we reported to you that: i. The Office of the Commissioner does not usually share information received during the examination of a complaint. However, the administrative file is available for inspection. possesses which 3 ii. You failed to answer the questions we asked you and we are waiting to receive your positions on the 8 questions we raised in order to have a complete picture in relation to the complaint. iii. Taking your positions as well as the legal basis of the establishment of a PPE are part of the process of examining a complaint and failure to cooperate with a Supervisory Authority is a criminal offence. 1.9. In your email dated 9/9/2022, you suggested that a meeting/inspection be arranged at the store in the presence of our Office, in the presence of a representative of the company that installed the PPE and a representative of your customers for an on-site inspection and to answer our questions. You have added as we set a date and time for inspection of the administrative file. 1.10. On 14/9/2022 we sent an email informing you that: i. Inspections by our Office are carried out as scheduled and in any case if and when deemed necessary. We also mentioned that we will judge whether we need to conduct an inspection after receiving your answers to the questions we asked you. ii. We added that Article 58(1)(a), of Regulation (EU) 2016/679 states that among the Commissioner's powers is to instruct the controller and the processor and, where appropriate, the representative of the controller or processing to provide any information it requires for the performance of its tasks. iii. We have informed you that the inspection of the administrative file could take place on Thursday 22/9/2022 at 10:00 a.m. at our Offices and we will await your written answers to the questions we have asked you as well as the confirmation of the date definition for inspection of the administrative file. 1.11. With your e-mail dated 16/9/2022: i. You informed us that it was impossible to carry out an inspection of the administrative file and suggested that it be carried out on 9/26/2022 at 10:00 am. You requested, as you have in writing, the positions of Ms. XXXXXXX (an employee of our Office) who was invoked by Mr. XXXXXXX (director of the company that installed the KKBP). iii. You mentioned that you will come back to the issues raised at the beginning of October as o manager of your clients was absent abroad to have his positions and the relevant information required. 1.12. On 21/9/2022 with our email we informed you that: i. Your suggestion to conduct the review of the administrative file on 9/26/2022 at 10:00 AM instead of 9/22/2022 was accepted. ii. We added that based on article 43(3) of the General Principles of the Administrative Law Law of 1999 (158(I)/1999) "The right to be heard is exercised either in person or through a lawyer of the choice of the interested party", therefore during the inspection of the administrative file, either the Defendant or the lawyer who represents him could be present. iii. We mentioned that regarding the positions of

Ms XXXXXXX, an officer of my Office, the case has been assigned to another officer of my Office and when the technician/company XXXXXXX contacted my Office he should 4 ii. states that there is a case in progress and should ask to speak to the officer handling the case under review. We added that Ms. XXXXXXX answered general questions and gave general directions, as well as my Office's announcements and Opinions in relation to CCBP, and when the technician subsequently referred to said complaint, Ms. XXXXXXX directed him to contact the officer who he handles it, which he didn't. iv. In addition, we mentioned that we will expect your answers until 7/10/2022 since the questions were originally put to you on 4/7/2022. 1.13. On 9/26/2022 you inspected the administrative file in my Office. 1.14. With your e-mail dated 12/10/2022 you apologized for the delay of a few days, attached a letter from the company that installed the CCTV, photos showing the placement of the cameras as well as warning signs, a diagram regarding the installation of the system, an operation/specification manual of the system in question, and you listed the following: i. You mentioned that following the correspondence between us and the inspection of the administrative file that took place on 26/9/2022, you list the positions of your clients and send us all the relevant ones that answer our questions as raised in our letter dated 7/9/2022. their claims that the complainant was aware of the cameras as it appears from the attached photo that there was a monitor showing the movements in the store next to the till and she had urged your customer manager to view the video and talk and who sent it to her and how to see the electronic messages that were enclosed in the administrative file. Therefore the complainant was aware of the existence of the cameras. iii. Additionally, the video in our possession has download motion and this is due to copying from your customer manager's mobile phone. This cannot be done by the cameras which are fixed. iv. Also the sound heard in the video is not from the cameras but from another device which transmits music. The cameras cannot focus as small as shown in the video but they focus as shown in the photos you sent us. v. You have filled in that the letter from the company that has installed the CCD answers all our questions. ii. You mentioned that your customers repeated 1.15. With our email dated 18/11/2022 we communicated to you my prima facie decision by which you were informed that there is a prima facie violation of articles 5 and 6 of the General Regulation on the Protection of Personal Data (EU) 2016/679. In addition, I have called upon you that within 4 weeks of the decision in question, you provide me with the reasons why you believe that any corrective measure or administrative sanction should not be imposed, prior to the issuance of a decision. I also asked you to inform me about the turnover of the Company and the number of its employees, in relation to the previous financial year. 1.16. On 20/11/2022 you confirmed receipt of my prima facie decision. 5 1.17. On 15/12/2022 by email, you communicated to us

your letter dated 13/12/2022 in which you stated your positions regarding my prima facie decision. Specifically, it was stated that: i. Valuable goods such as gold and silver items are available for sale in your customer's shop providing a legal interest to your customers for the use of PPE as referred to in Guidelines 3/2019 which I refer to in my prima facie decision. In particular, you mentioned that for the existence of a legal interest, situations of imminent risk can also be found which are found in banks or shops that sell valuable goods (e.g. jewellers). Therefore, you have attached a Certificate of Registration in the Register of Jewelers of the Cyprus Precious Metals Marking Organization as well as a number of invoices for the sale of jewellery. You added that it is not possible to hire security guards as customers cannot make a purchase while being watched by security guards. ii. As far as audio recording is concerned, you mentioned that, it is not noticeable if we have made a finding that the cameras have an audio recording system, except that this possibility exists due to the specifications that were sent to us. iii. You added that the data subject, namely the complainant, knew that there was video surveillance which was done with her consent. In addition, your customers apologize for the remark made to the employee but the employee who is paid for his working hours should respect his workplace and perform his duties in the best way and diligence without the need for supervision even physics. You also indicated that the employee's behavior was inappropriate by attaching a copy of text messages between the complainant and your customers. iv. Regarding the observance of the Legislation and the Regulations, you added that your clients entrusted the installation of PPE to a licensed company, which assured them that no formalities were required according to the information received from our Office, but as it turned out, there was misinformation or a misunderstanding . You added that your customers are ready to change the warning signs where you clearly state that there is video surveillance, the controller, how long the data is kept and when it will be deleted. You also mentioned that a relevant form will be delivered to obtain the written consent of the employees regarding their acceptance that the space is video-surveilled and their data will be processed which will not be used for other purposes and will be deleted in due time. v. You stated that there is no reason to impose any administrative penalty considering that your customers intend to immediately take the corrective measures you mentioned unless our service wishes to indicate anything additional to your customers e.g. issuing any permit, sending sample warning signs. 2.1. Based on Article 4 of the Personal Data Protection Regulation (EU) 2016/679, "1) "personal data": any information concerning an identified or identifiable natural person ("data subject"); the identifiable natural person is one whose identity can be ascertained, directly or indirectly, 6 2. Legal Basis the name in particular by reference to an identifier such as a name, an ID number, location data, an online identifier or one or more factors

that attribute to the physical, physiological, genetic, psychological, economic, cultural or social identity of the natural person in question, 2) "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, adaptation or alteration, retrieval, information retrieval, use, disclosure by transmission, dissemination or any other form of disposal, the association or combination, restriction, erasure or destruction,... 7) "controller": the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and the manner of processing personal data; where the purposes and manner of such processing are determined by Union law or the law of a Member State, the controller or the specific criteria for his appointment may be provided for by Union law or the law of a Member State.' 2.2. Based on Article 5 of the Personal Data Protection Regulation (EU) 2016/679, "1. Personal data: a) are processed lawfully and legitimately in a transparent manner in relation to the subject of the data ("legality, objectivity and transparency"), b) are collected for specified, explicit and legitimate purposes and are not further processed in a manner incompatible with these purposes; the further processing for archiving purposes in the public interest or for scientific or historical research or statistical purposes is not considered incompatible with the original purposes in accordance with Article 89 paragraph 1 ("purpose limitation"), c) are appropriate, relevant and limited to what is necessary for the purposes for which they are processed ("data minimization"), d) are accurate and, where necessary, updated; all reasonable steps must be taken to immediately delete or correct personal data that is inaccurate, in in relation to the purposes of the processing ("accuracy"), e) are kept in a form that allows the identification of the data subjects only for the period necessary for the purposes of the processing of the personal data; the personal data can be stored for longer intervals, as long as the personal data will be processed only 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 on safeguarding the rights and freedoms of the storage period"), f) are processed in a way that guarantees the appropriate security of personal data, including their protection against unauthorized or illegal processing and accidental loss, destruction or damage , using appropriate ("integrity and confidentiality"). 2. The controller shall be responsible and able to demonstrate compliance with paragraph 1 ("accountability")." technical or organizational measures of the data subject ("restriction 7 2.3. Article 6 of the Regulation on the Protection of Personal Data (EU) 2016/679, Lawfulness of processing states that, "1. Processing is lawful only if and as long as at least one of the following conditions: a) the data subject has consented to the processing of his

personal data for one or more specific purposes, b) the processing is necessary for the performance of a contract to which the data subject is a party or for to take measures at the request of the data subject before entering into a contract, c) the processing is necessary to comply with a legal obligation of the controller, d) the processing is necessary to safeguard a vital interest of the data subject or another natural person, e) the processing is necessary for the fulfillment of a task performed in the public interest or in the exercise of a public authority assigned to the data controller, f) the processing is necessary for the purposes of the legal interests pursued by the data controller or a third party , unless these interests are overridden by the interest or fundamental rights and freedoms of the data subject that require the protection of personal data, in particular if the data subject is a child…" 2.4. Based on recital 47 of the Personal Data Protection Regulation (EU) 2016/679, "The legitimate interests of the controller, including those of a controller to whom the personal data or third parties may be disclosed, may provide the legal basis for the processing, provided that they do not override 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. Such a legitimate interest could for example exist where there is a relevant and appropriate relationship between the data subject and the controller, such as if the data subject is a client of the controller or is in its service. In any case, the existence of a legitimate interest would need a careful assessment, including whether the data subject, at the time and in the context of the collection of the personal data, can reasonably expect that for this purpose it can be carried out processing. In particular, the interests and fundamental rights of the data subject could prevail over the interests of the controller, when personal data are processed in cases where the data subject does not reasonably expect further processing of his data…". 2.5. Based on article 7 of the Regulation on the Protection of Personal Data (EU) 2016/679 "1. When the processing is based on consent, the controller is able to prove that the data subject consented to the processing of the personal data. 2. If the data subject's consent is provided in the context of a written statement that also concerns other matters, the request for consent shall be submitted in a way that is clearly distinguishable from the other matters, in an understandable and easily accessible form, using clear and simple wording . Any part of this 8 statement which constitutes a violation of this regulation is not binding. 3. The data subject has the right to withdraw his consent at any time. Withdrawal of consent does not affect the lawfulness of processing that was based on consent prior to its withdrawal. Before giving consent, the data subject is informed accordingly. Withdrawing consent is as easy as giving it. 4. When assessing whether consent is given freely, particular consideration is given to whether, among other things, for the performance of a contract, including the provision of a service, consent to the

processing of personal data that is not necessary for the performance of the said contract." 2.6. Based on Article 35(1) of the Personal Data Protection Regulation (EU) 2016/679, Data Protection Impact Assessment, "When a type of processing, in particular using new technologies and taking into account the nature, scope , the context and purposes of the processing, may entail a high risk for the rights and freedoms of natural persons, the controller shall, before processing, assess the impact of the planned processing operations on the protection of personal data. An assessment may consider a set of similar processing operations which involve similar high risks.' 2.7. Pursuant to Article 58 of the Personal Data Protection Regulation (EU) 2016/679, Powers, "1. Each supervisory authority shall have all of the following investigative powers: a) to order the controller and processor and, where applicable, the representative of the controller or processor to provide any information it requires for the performance of of its duties, b) to carry out investigations in the form of data protection audits, c) to review the certifications issued in accordance with Article 42 paragraph 7, d) to notify the controller or processor of suspected violation of this regulation, e) to obtain, from the controller and the processor, access to all personal data and all the information required for the performance of its duties, f) to have access to the facilities of the controller and the processor, including any data processing equipment and means, in accordance with the procedural law of the Union or a Member State. 2. Each control authority has all the following corrective powers: a) to issue warnings to the data controller or processor that intended processing operations are likely to violate provisions of this regulation, b) to address reprimands to the data controller or processor processing when processing operations have violated the provisions of this regulation, c) instruct the controller or the processor to comply with the data subject's requests for the exercise of his rights in accordance with this regulation, 9 d) to instruct the data controller or the processor to make the processing operations compliant with the provisions of this regulation, if necessary, in a specific way and within a certain period, e) to instruct the data controller to announce the data breach of a personal nature to the data subject, f) to impose a temporary or definitive restriction, including the prohibition of processing, g) to order the correction or deletion of personal data or the restriction of processing pursuant to articles 16, 17 and 18 and an order to notify the actions of these to recipients to whom the personal data notified under Article 17(2) and Article 19, h) to withdraw the certification or to order the certification body to withdraw a certificate issued in accordance with Articles 42 and 43 or to order the certification body not to issue a certification, if the requirements certification requirements are not met or are no longer met, i) to impose an administrative fine pursuant to article 83, in addition to or instead of the measures referred to in this paragraph, depending on the circumstances of each individual case,...". 2.8. Based on article 83 of Regulation (EU) 2016/679:

"2. Administrative fines, depending on the circumstances of each individual case, are imposed in addition to or instead of the measures referred to in Article 58 paragraph 2 items a) to h) and Article 58 paragraph 2 item j)..." 2.9. Based on Guidelines 3/2019 on the processing of personal data via video devices state that "3.1 Legitimate interest, Article 6(1)(f) 17. The legal assessment of Article 6(1)(f) should be based on the following criteria according to recital 47. 3.1.1 Existence of legitimate interests 18. Video surveillance is lawful if it is necessary to achieve the purpose of the legitimate interest pursued by the controller or a third party, unless these interests are overridden by the interest or fundamental rights and freedoms of the data subject (Article 6(1)(f)). The legitimate interests pursued by the controller or a third party can be legal, financial or non-material interests. However, the controller should bear in mind that if the data subject objects to the surveillance in accordance with Article 21, the controller may only carry out video surveillance of that data subject if there is an overriding legitimate interest, rights and freedoms of the data subject or for the establishment, exercise or defense of legal claims. 19. If there is a real and dangerous situation, the purpose of protecting property from robbery, theft or vandalism may constitute a legitimate interest for the purposes of video surveillance. 20. The legal interest must actually exist and concern a present matter (ie the interest must not be fictitious or hypothetical). There must be an actual risk situation – such as damage or serious past events – before surveillance can begin. Based on the principle of accountability, it is useful for controllers to record relevant events (date, manner, financial loss) and relevant criminal prosecutions. These recorded events can be a strong presumption of the existence of a legitimate interest. 10 The existence of a legitimate interest, as well as the necessity of monitoring should be re-evaluated at regular intervals (e.g. once a year, depending on the circumstances)... 22. Legitimate interest can also constitute situations of imminent danger which are identified in banks or shops that sell valuable goods (e.g. jewelry stores) or in places where property crimes are known to be frequently committed (e.g. gas stations)... 3.1.2 Necessity of processing 24. Personal data should are appropriate, relevant and limited to what is necessary for the purposes for which they are processed ("data minimization"), see Article 5(1)(c). Before installing a video surveillance system, the controller should always thoroughly consider whether this measure is, firstly, appropriate to achieve the desired objective and, secondly, sufficient and necessary to achieve its purposes. Video surveillance measures should only be chosen if the purpose of the processing could not reasonably be fulfilled by other means, which infringe to a lesser extent the fundamental rights and freedoms of the data subject. 25. If it is assumed that the controller wishes to prevent crimes against his property, instead of installing a video surveillance system, he can take alternative security measures, such as e.g. fence his property, have security personnel

regularly patrol the premises, hire security guards, improve lighting, install security locks, tamper-proof windows and doors, or cover surfaces with anti-graffiti coatings or films. These measures can be just as effective as video surveillance systems in preventing incidents of robbery, theft and vandalism. The controller must assess on a case-by-case basis whether these measures can be a reasonable solution. 26. Before operating the video surveillance system, the controller is obliged to assess when and where video surveillance measures are absolutely necessary. Usually, a video surveillance system that operates at night, as well as outside normal working hours, meets the need of the controller to prevent any danger that threatens his property... 29. Questions concerning the necessity of the processing are also raised about the way in which the which the data is kept. In some cases it may be necessary to use "black box" solutions: audio-visual material is automatically deleted after a certain storage period, and is only accessible in the event of an incident. In other cases, it may not be necessary to retain the video footage at all as it is deemed more appropriate to use real-time monitoring means. The choice between black box solutions and real-time monitoring should also be based on the intended purpose. If, for example, the purpose of video surveillance is to preserve evidence, real-time surveillance methods are usually not considered appropriate. Also, in some cases real-time monitoring can be more intrusive than storing and automatically deleting material after a certain amount of time has passed (e.g. when someone is constantly monitoring the screen it can be more intrusive into people's privacy than ,what if there is no screen at all and the material is stored directly in the black box). In this case the principle of data minimization must be taken into account (Article 5(1)(c)). It should also be taken into account that the controller, instead of video surveillance, sometimes has the option of using security personnel, who can react and intervene immediately." 2.10. Based on Guidelines 5/2020 on consent, “3.1.1. Power imbalance 21. Power imbalance also exists in the context of employment. Given the dependency inherent in the employer/employee relationship, it is unlikely that the data subject will be able to refuse to provide his employer with consent to the processing of his data without fear or without running a real risk of suffering adverse consequences due to of his refusal. It is unlikely that an employee will be able to freely respond to their employer's request for consent in relation to, for example, the activation of monitoring systems such as workplace camera observation, or the completion of assessment forms, without feeling pressured to provide consent of. Therefore, the EDPS considers it problematic for employers to process personal data of their existing or future employees based on consent, as it is unlikely to be freely given. For most of this data processing at work, the legal basis cannot and should not be employee consent [Article 6(1)(a)], due to the nature of the employer-employee relationship." 2.11. Based on Article 4 point 11 of Regulation (EU)

2016/679, consent is defined as: "any indication of will, free, specific, explicit and fully informed, with which the data subject expresses that he agrees, by statement or by clear positive action, to be the subject of processing of the personal data concerning it." 2.12. In addition, in recital 42 you state that consent should not be considered freely given if the data subject does not have a genuine or free choice or is unable to refuse or withdraw consent. In particular you state that "When the processing is based on the data subject's consent, the controller should be able to demonstrate that the data subject consented to the processing act... According to Council Directive 93/13/EEC, a statement of consent should be provided, drawn up in advance by the controller in an understandable and easily accessible form, with clear and simple wording, without abusive clauses. To be considered informed consent, the data subject should know at least the identity of the controller and the purposes of the processing for which the personal data is intended. Consent shall not be deemed to have been freely given if the data subject does not have a genuine or free choice or is unable to refuse or withdraw consent without prejudice." 2.13. Decision 23/2021 of the Hellenic Personal Data Protection Authority is also relevant, regarding the installation of cameras in the workplace and monitoring of employees. 2.14. Based on the announcements of our Office dated 28/6/2019 and 26/10/2021 regarding the legality of installing CCTV in places accessible to the public such as shops, shopping malls, businesses, leisure centers state that, 12 "Image and audio data are personal data . The recording of image and sound constitutes processing of personal data, which in order to be legal must comply with the provisions of GDPR 2016/679 as well as the National Legislation Law 125(I)/2018. Capturing an image using CCD is only permitted if there is no less intrusive way to accomplish the purpose. Examples where it is allowed to take an image using CCD: - Building entrance/exit - Outside an elevator, focusing only on it - Above a card/cash register machine, focusing only on it - Parking area Examples where it is not allowed to take an image with the use of CCTV: - Corridors - Inside elevators - In waiting areas - Restrooms - Indoor/outdoor dining areas of cafeterias, restaurants, etc. In general: It is not allowed to control the personal behavior, personal contacts and efficiency of individuals through such systems. People should be informed by means of warning signs, which should be clearly visible, sufficient in number and in a prominent place. The sign must state (a) that it is being videotaped, (b) the controller and (c) the purpose of the videotaping. The data subject can exercise the right of access in the event of registration by KKKP. Regarding the right to erasure, the data is kept for a reasonable period of time, always in relation to the purpose it serves. In the cases where the installation of PPE may pose a high risk to the rights and freedoms of natural persons, an Impact Assessment is required prior to processing, in order to assess the effects of the planned actions..." 3. Rationale 3.1. With our daily emails.

11/4/2022, 4/7/2022, 7/9/2022 and 21/9/2022 we requested as we have the positions of the Professor as well as the relevant supporting documents of these positions are sent to us. We have also raised the following questions awaiting answers on: Monitoring the movements of the complainant who appears to i. took place during her work. The ii. the Closed Circuit which appears to be Video Surveillance and for which we received confirmation to the contrary. iii. The legal basis for the installation and operation of Closed Circuit Video Surveillance (Article 6 of the Regulation). Conducting an impact assessment. iv. v. The total number of cameras and where they are located. 13 has sound and is a legal basis The shooting angle of the cameras in question (as attached screenshot). vi. The posted information/warning signs regarding vii. operation of the Closed Circuit Video Surveillance. How many and in which places. vii. Which persons have access to said system in any way. 3.2. Through your e-mail dated 4/29/2022 you stated that the CCTV was for store security and was installed by a licensed company. You failed to answer us about what is the legal basis for the installation and operation of the CCCP. From your above reference, we can guess that it is considered that the article 6(1)(f), that is, the processing/installation and operation of the GDPR is necessary for the purposes of the legal interests pursued by the controller, i.e. Prof. u. And your reference that the CCBP was installed by a licensed company does not provide the legal basis for the CCBP installation, nor does it legitimize the installation of the system in question. 3.3. In addition, you stated that the complainant was aware of the existence of the CCCP, controlled the CCCP, and that the video recording device was located next to the cash register that the complainant operated and monitored. The reports in question indicate that the complainant is aware of the operation of the KKBP, they do not legitimize the existence and operation of the KPBP nor negate the obligation of the data controller to demonstrate compliance with Article 5(1) that the personal data is submitted to lawful and lawful processing. The submission of the complaint demonstrates that the processing in question was not lawful. In addition, the above references to you imply that the data subject has provided his consent for the operation of the CCCP. Keep in mind that the employer-employee relationship that existed in this particular case reveals the existence of a power imbalance in the context of employment. That is, when there is an employer-employee relationship, it is unlikely that the employee will be able to refuse the operation of a GDPR without fearing any negative consequences due to his refusal, since any processing cannot be characterized as legitimate. 3.4. In addition, the screenshots in our possession showing the written communication between Ms XXXXXXX and the complainant show that the complainant's movements were being monitored during her work. In both of these communications, Ms. XXXXXXX monitored the recordings in the CCBP and through them made observations/checks of the complained action, which is prohibited. In particular, workplace surveillance is

prohibited and a PPE should not be used to monitor workers. The recording of personnel throughout their work is considered excessive as it interferes to a large extent in the private life of the employee and is not consistent with articles 5 and 6 of the Regulation. Additionally, CCTV recording should be limited to entry and exit areas, checkouts or areas with safes, electromechanical equipment, etc., provided that the cameras focus on the asset they are protecting and not on employee areas. 3.5. Regarding your reference in your email dated 4/29/2022 that the KKBP does not have a sound recording system according to the certification of the company that installed it, please note that in your email dated 12/10/2022 you have attached us an operation/specification manual of the system in question. From the 14 technical specifications it is not proven that there is no sound as the specific system provides this possibility. In any case, it is not only considered a violation of the existence of sound in the KKBP due to the sound (music) heard in the video we have in our possession, but also the monitoring of the employee through the KKBP, as can be seen from point 3.4. above. 3.6. In addition, in our e-mails you were asked questions about the total number of cameras, where they are located, what is the shooting angle of said cameras and how to attach screenshots. In your email dated 12/10/2022 you shared with us a letter and blueprint from the company that installed the CCPP stating that the company's letter answers all our questions. Please note that we have not addressed, nor have we sought the company's positions on the complaint, but the Professor. In any case, the letter in question states that 4 cameras were installed in the 4 corners of the store in question. Also, the photos shared with us in your email show the placement of cameras in points/corners of the store. 3.7. Regarding the installed informational/warning signs regarding the operation of the Closed Circuit Video Surveillance, how many and in which places, you indicate in the company's letter that warning signs were placed at the cash register and at the entrance of the store. Also, through the photos that were sent to us, their existence can be seen. Note that subjects should be informed by means of warning signs, which should be conspicuous, sufficient in number and placed in conspicuous places. Signs must state (a) that video recording is taking place, (b) the controller and (c) the purpose of the video recording. In the photos that you shared with us through your e-mails on 31/8/2022 and 12/10/2022, it appears that points (b) and (c) are not recorded on the warning signs, but the name and contact details of the company that installed the CCD. 3.8. In relation to our question, as far as which persons have access to the KKBP, you have not answered, except that you mention in your letter d. 29/4/2022 that the video recording device was next to the cash register which the complainant herselfhe was working and watching. In addition, in the company letter you mention that the recording monitor is located next to the cash register so that the respective employee can

to have full control of the store.

3.9. Regarding your reports:

i.

that in the video we have in our possession there is movement of the download and this was done

due to the copying from the cell phone of your customer manager and

that this cannot be done by the cameras, which are fixed.

that the sound heard from the video is not from the cameras but from another

device, which transmits music.

that cameras cannot focus on such a small size as shown in

video but focus as seen in the photos you sent us.

As already mentioned in paragraph 3.5. above, we do not only consider

existence or not of the sound function in the CCB but its very legality

ii.

iii.

installation and operation of the KKBP as well as its monitoring

employed through the KKBP.

3.10. Please note that as far as carrying out an impact assessment before the

KKBP installation, this has not been communicated to us nor has anything been reported to us

on this matter.

3.11. In relation to your reference in your e-mail dated 15/12/2022, that

it is not possible to hire security guards because in such a case the customers

they cannot make a purchase while being monitored by security guards,

keep in mind that hiring security guards is not the only measure which

can be taken to protect against theft of sale items that

your customers have (gold and silver valuables). Measures such as

placing these valuable items in display cases where they have a lock,

opening them at the customer's request, installing an anti-theft alarm in the

due goods etc.

3.12. Regarding your reference to the same email that it will be delivered

relevant form to obtain the written consent of the admissions officers

of the fact that the area is video-surveilled, cannot be considered as a measure of its legalization

establishment of the CCPP, as the employer relationship has already been mentioned to you –

employee reveals the existence of an imbalance

of force in its context

of employment. The employee, fearing any negative effects at work

due to refusal to grant consent, he cannot freely give the

his consent. In general, the term "free consent" implies that the subject

of data has real choice and control. If the data subject,

i.e. employees, have no real choice or feel forced to

consent, the consent is not valid.

3.13. Keep in mind that employees coming to their workplace,

they still enjoy the right to their private lives. His recording

staff during his work is considered excessive and offends her

personality and private life of employees by violating the rights

and their freedoms. So obtaining consent from employees is considered a no

arising and cannot be taken into account.

3.14. Note that in the prima facie case I asked as me

inform about the turnover of Kathy and the number of

of its employees, in relation to the previous financial year, a fact which also

you skipped

4. Conclusion

4.1. Bearing in mind all the above facts as they have been quoted, and based on them

powers granted to me by Articles 58 and 83 of Regulation (EU) 2016/679,

I judge that there is a violation of articles 5 and 6 of the General Regulation on

Personal Data Protection (EU) 2016/679.

4.2. Based on the provisions of article 83 of Regulation (EU) 2016/679 and

taking into account the mitigating factors (a-b) and aggravating factors (c-d) below

factors:

16

your cooperation with my Office,

the non-existence of a previous incident by the Defendant,

the monitoring of the employee through the KKBP,

the absence of appropriate warning signs,

a)

b)

c)

d)

exercising the corrective powers conferred on me by Article 58(2)(d) of the Regulation

(EU) 2016/679 pursuant to which:

"Each control authority shall have all of the following remedial powers:

d) to instruct the controller or processor to

make processing operations comply with the provisions of this regulation,

if necessary, in a specific manner and within a specific period,'

I have decided to address the following Orders to the Professor as follows:

Commandment 1: Cameras to focus and capture only the objects you judge

that they have value.

Order 2nd: The placement of informational/warning signs regarding the

CCBP operation to be in accordance with the Guidelines of my Office.

Order 3rd: Records obtained outside the legal framework are deleted immediately,

and a relevant receipt is sent to us.

Order 4th: Notify my Office within an exclusive period of 2 weeks

from the receipt of this all actions to implement the Orders.

Irini Loizidou Nikolaidou

Data Protection Commissioner

Personal Character

MI

17