No. Fax: 11.17.001.010.090 DECISION Closed Circuit Video-Surveillance Installation I refer to the complaint filed in my Office, on May 25, 2022, by the law firm I. CHRISTODOULOU & PARTNERS LLC on behalf of XXX (hereinafter the "Complainant") of KUUTIO HOMES LTD (hereinafter the "Complainant") against the latter, and in all correspondence related to the above matter, which forms part of the case file. After examining the incident, based on the duties and powers conferred on me by Articles 57 and 58 of Regulation (EU) 2016/679 on the protection of natural persons against the processing of personal data and on the free movement of such data (hereinafter the "Regulation"), I note the following: Facts of the case 2.1. As described in the complaint, the Defendant had notified her staff of a Notice regarding the installation and operation of Closed Circuit Video-Surveillance (hereinafter the "CCTV") at her offices. Along with the Notice, the Client had given a consent form to her staff, regarding the placement of the PPE. According to the Complainant, the said form was never signed by him. 2.2. The Notice stated the purposes for which the installation of CCTV was deemed necessary, as well as a general description of the locations of the cameras. Here is a full excerpt of the Notice in English: "The CCTV surveillance is intended for the purposes of: 1. 2. Keeping employees safe and secure by preventing violence or theft; Preventing pilfering, malingering, deliberate damage or other misconduct? 3. 4. Ensuring and recording that health and safety procedures are being followed? Monitoring and improving productivity? Location of CCTV cameras: 1. 2. 3. 4. The CCTV cameras will be sited so they only capture images relevant to the purposes for which they are installed and care will be taken to ensure that reasonable privacy is not violated. The location of the equipment is carefully considered to ensure that images captured comply with the Data Protection Regulations. The management of KUUTIO GROUP LTD has endeavored to select locations for the installation of CCTV cameras which are least intrusive to protect the privacy of individuals. CCTV cameras will not be used in restrooms. » 2.3. As pointed out in the complaint, the Defendant recorded the staff in the workplace, during the exercise of their work duties, throughout the working hours. It is the Complainant's position that the access to the screen where the image captured by the CCTV cameras was displayed was free, with the result that the displayed images could be watched and commented on by third parties. 2.4. The following were also mentioned, to strengthen the Complainant's positions: 2.4.1. Image data is personal data and image capture constitutes personal data processing. 2.4.2. The intended purposes could be achieved by using other measures. 2.4.3. The nature and conditions of the work performed by Kathy do not justify the use of PPE. 2.4.4. The Complainant never gave his consent to the placement of the CCBP. 2.4.5. Even in the case where there was consent, if the operation of the GDPR conflicts with basic principles of personal data processing, then any consents obtained do not make the

processing compliant with the Regulation. 2.4.6. Monitoring the efficiency and personal behavior of staff is not a legitimate purpose. 2.4.7. There is a clear imbalance between, on the one hand, the legal interest of protecting the Complainant from theft and damage, and on the other, the 2 fundamental right to privacy and protection of personal data of the Complainant. 2.5. Attached to the complaint was the Notice and the consent form regarding the installation and operation of the CCCP, as well as the appointment document of the law firm to represent the Complainant. 3. By letter, dated June 16, 2022, my Office requested the positions/opinions of the Complainant regarding the incident described above, asking her specific questions. 4.1. According to the letter, dated June 27, 2022, the Plaintiff had informed all her staff verbally and in writing, of her decision to install the KKBP. Also, after the installation of the CCBP, he sent to all staff a relevant information letter, dated July 23, 2021, via e-mail. Additionally, Ms. confirmed that she provided all of her staff with a consent form for the placement of the CPAP. As he noted, although the Complainant never signed the consent form, he never objected to the installation of the system. 4.2. Kathy emphasized that she is active in the field of land development and due to these professional activities, large sums of money are often traded within her building. Also, as she noted, she is in possession of confidential documents such as agreements, passports, no. bank accounts, but also keys and other personal belongings of customers. Furthermore, it was reported that the complainant's buildings are located in a central part of Paphos, where incidents of violence and vandalism often take place. In the past, Kathy has received complaints from her employees about lost items and using the cameras has helped them find them. Kathy considers the operation of the CCTV necessary to protect her building from break-ins, vandalism and theft. 4.3. As explained, the CCTV consists of 21 cameras, 13 internal and 8 external perimeter of the building. In particular, Kathy attached to the message dated June 27, 2022, as requested, screenshots showing the images captured by the cameras, which are as follows: □ Camera 01 □ Parking Area □ Exit door 3 □ Reception □ Administration □ Accounting □ O Office_2 □ Lobby □ Road_1 □ General Manager □ Road_2 □ Reception Entry □ Office □ Main Entrance □ Living Room Area □ Filio □ Court Entry It is noted that in the said message, Ms. attached 19 areas and not 21 , as he had mentioned. 4.4. As explained, the retention period of the KKBP files is 45 days, with automatic deletion after the end of said time period, without any copying of data. There is no audio recording when the image is recorded and there are two warning signs for the CCTV, which state that the surveillance is 24 hours. 4.5. With regard to the Complainant's claim for free access to the screen where the captured image of the CCTV cameras is presented, it is the position of the Defendant that there is no screen showing a captured image. The download is done via a remote connection, via the IVMS 4500 app on a smartphone. Only Ms. XXX and

the company that had installed the CCBP have access. A relevant report of the company that installed the KKVP, which confirms the positions of the Client, was attached to the relevant response dated June 27, 2022. 4.6. The following were also attached to Ms.'s said response: the letter dated July 23, 2021, the Notice for the installation and operation of the CCTV, consent form, the screenshots of the captured image of the cameras, photographs of of warning signs, 4 reports of the installation company of the KKBP and the technical specifications of the system. 5.1. After studying the above I judged that there are clear violations of the provisions of the Regulation. Based on my Powers, as defined in Article 58 of the Regulation, I issued an Order, dated July 22, 2022, for the Defendant to suspend the operation of the KKBP until the completion of the investigation of the incident by my Office, and issuance of my Final Decision . 5.2. She sent electronically on July 26, 2022, a letter confirming her compliance with my above Order. He also explained that the two cameras, for which he had not sent screenshots, are placed one in the lobby, which is out of order, and the second in the parking lot of Kathi. She stated, among other things, that an effort had been made on her part, following the guidance of her Legal Advisers, to have the cameras not record the staff at all and focus only on the office doors. This, as he noted, was impossible since its offices are small in size. He explained that the recording of sidewalks and public spaces in general was done out of ignorance and there was no intention to violate the Regulation. 6.1. On July 22, 2022, I sent a letter to the law firm representing the Complainant, with which I requested that it send me its positions and any supporting documents it has in its possession, regarding the Claimant's claim that there is no screen in which the image taken by the KKBP cameras is presented, which was also the only one that differed between the two parties. On July 29, 2022, I received the Complainant's positions, in which it was noted among others that "(...) it is noted that there was free, external and unfair access in relation to the said CCBP by third parties, as a result of which it was monitored and commented on between others the time of attendance but also the general behavior and (…) from third parties." Additionally, it was stated that "Appropriate security was not demonstrated in the data illegally collected by the Complainant with the inevitable result of free access to it by third parties." 6.2. According to the Complainant's statements, during his employment with the Complainant, the latter had a screen installed in the corridor of the 1st floor, outside the kitchen, directly above 5 The Complainant is open to any suggestions/suggestions of Kathy had sought legal advice before installing the KKBP, the server tower in public view. It was noted that, to the best of the Complainant's knowledge, access to the content of the said screen was not only provided by XXX of the Complainant, but also by XXX, XXX of the Complainant and XXX. Relevant photos (from Kathy's website), showing the described location and display, are attached. I note that, in the

photos, the screen was not working. 7.1. Subsequently, on July 29, 2022, Ms. XXX contacted an Officer of my Office by telephone, and stated the following: Could my Office arrange an on-site visit, during which A. a satisfactory solution could be found regarding the violations that have been detected. B. My office. C. on the basis of which it requested the consent of its employees for it. The reasons for filing the complaint with my Office are vindictive. D. E. A lot of money has been invested in Cathy's building, and stopping the KKBP could cause problems, as there can't be a complete audit. F. After the PPE was shut down, a door to the building was found to remain unlocked and there was no proper means to check if anyone entered the building. G. security. H. case you need them. 7.2. My Office sent me an email, dated August 3, 2022, related to the above concerns of Ms., in which it was explained that only in the event that it is deemed necessary, my Office will proceed with an on-site visit to her premises. It was also stated, among other things, that her cooperation with my Office and her prompt compliance with my Order is favorably regarded. Furthermore, it was explained that due to the employer-employee dependency relationship, obtaining consent from the employees cannot be considered free, explicit, nor that it can be revoked at any time. Hence it is regarded as unborn. It was also noted that the grounds for filing the complaint will not be considered as they do not change the violations I have identified. Through the KKBP, XXX can easily locate employees in Large amounts are traded within the buildings and the KKBP contributes to 6 7.3. It was also stated that my Final Decision would be issued after the investigation of the incident was completed, at which point the Defendant was asked to take additional measures (e.g. installing alarm systems, having second-person checks to lock the building, security guard, smoke detectors etc.) for the security of its building. It was emphasized that, under no circumstances is it allowed to control the personal behavior, personal contacts and efficiency of employees through KKBP. Finally, the Defendant was requested, if available, the 8. screen shot of the camera that takes an image from the parking lot of the building and which was not previously attached, as sent. In the event that due to the interruption of the KKBP, this possibility does not exist, it was requested as described in the download image. The Defendant, in an email dated August 30, 2022, stated that the camera that was taking an image from the parking lot and was not previously attached, was not taking an image from any adjacent road, sidewalk, other building, etc. Legal Framework Below I list the Legal Framework in which I have based Rationale 9. and my Conclusion. Any marking in the text is my own. 10. Based on recital 47 of the Preamble of the Regulation, "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, under condition 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 7 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. Since it is for the legislator to provide by law the legal basis for the processing of personal data by public authorities, that legal basis should not apply to processing by public authorities in the performance of their duties. The processing of personal data, to the extent that it is strictly necessary for the purposes of fraud prevention, also constitutes a legitimate interest of the controller concerned. The processing of personal data for the purposes of direct marketing can be considered to be carried out for the sake of a legitimate interest." 11. Based on Article 4 of the Regulation, "1) "personal data": any information concerning an identified or identifiable natural person ("data subject"); an identifiable natural person is one whose identity can be ascertained, directly or indirectly, in particular by reference to an identifier such as a name, an identity number, location data, an online identifier or one or more factors that characterize the physical, physiological, genetic, psychological, economic, cultural or social identity of the said natural person, 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, the storage, adaptation or alteration, retrieval, retrieval of information, use, disclosure by transmission, dissemination or any other form of disposal, association or combination, restriction, deletion 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 manner of processing personal data; when the purposes and manner of of this processing are determined by the law of the Union or the law of a Member State, the controller or the special criteria for his appointment may be provided by the law of the Union or the law of a Member State" 8 12. Pursuant to Article 5 of the Regulation, "Personal data: a) are processed lawfully and legitimately in a transparent manner in relation to the data subject ("legality, objectivity and transparency"), b) are collected for specified, explicit and legitimate purposes purposes and are not further processed in a manner incompatible with those purposes; further processing for archiving purposes in the public interest or scientific or historical research purposes or statistical purposes shall not be

considered incompatible with the original purposes in accordance with Article 89(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 measures for the immediate deletion or correction of personal data that are inaccurate, 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 time required for the its purposes processing of personal data; 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 scientific or historical research purposes or for statistical purposes, in accordance with Art. 89 paragraph 1 and as long as the appropriate technical and organizational measures required by this regulation are applied to safeguard the rights and freedoms of the data subject ("restriction of the storage period"), f) are 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 technical or organizational measures ("integrity and confidentiality"). 2. The controller shall be responsible and able to demonstrate compliance with paragraph 1 ("accountability")." 13. "1. The processing is lawful only if and as long as at least one of the following conditions applies: According to Article 6 of the Regulation, 9 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 to take measures at the request of the data subject prior to the conclusion of 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 public authority delegated to the controller, f) the processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party, unless these interests are overridden by the interest or the fundamental rights and freedoms of the data subject that require the protection of personal data, in particular if the data subject is a child. Item f) of the first paragraph does not apply to the processing carried out by public authorities in the exercise of their duties." 14. Based on Article 7 of the Regulation, "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 statement that 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 is required of said contract." 15. Pursuant to paragraphs 1 and 2 of Article 58 of the Regulation, "1. Each control authority has all the following powers of investigation: a) to instruct the controller and the processor and, where appropriate, the controller's representative processing or the processor to provide any information it requires for the performance of its tasks, b) to conduct investigations in the form of data protection checks, c) to review the certifications issued in accordance with article 42 paragraph 7, d) to notify the controller or the processor of an alleged violation of this regulation, e) to obtain, from the controller and the processor, access to all personal data and all information required for the performance of its duties, f) to have access to the facilities of the controller and the processor, including any equipment and means of data processing, 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) to 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, d) to instruct to the controller or the processor to make the processing operations comply with the provisions of this regulation, if necessary, in a specific way and within a certain period, e) instruct the controller to notify the personal data breach to the subject of data, f) to impose a temporary or definitive restriction, including the prohibition of processing, 11 g) to order correction or deletion of personal data or restriction of processing pursuant to articles 16, 17 and 18 and an order to notify recipients of these actions in whose personal data was disclosed pursuant to 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 certification, if the 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, j) to order a suspension of data circulation to a recipient in a third country or an international organization. " 16. Based on Article 83 of the Regulation, "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(2)(a) to (h) and Article 58(2)(j). When deciding on the imposition of an administrative fine, as well as on the amount of the administrative fine for each individual case, the following shall be duly taken into account: a) the nature, gravity and duration of the infringement, taking into account the nature, extent or purpose of the relevant processing, as well as the number of data subjects affected by the breach and the degree of damage suffered by them, b) the fraud or negligence that caused the breach, c) any actions taken by the controller or the processor to mitigate the damage suffered by the data subjects, d) the degree of responsibility of the controller or the processor, taking into account the technical and organizational measures they apply pursuant to articles 25 and 32, e) any relevant previous violations of the controller or processor, f) the degree of cooperation with the supervisory authority to remedy the violation and limit its possible adverse effects, g) the categories of personal data affected by the violation, 12 h) the way in which the supervisory authority was informed of the violation, in particular if and to what extent the controller or processor notified the violation, i) in case the measures referred to in Article 58 paragraph 2 were previously ordered to be taken of the controller involved or the processor in relation to the same object, the compliance with said measures, j) compliance with approved codes of conduct in accordance with Article 40 or approved certification mechanisms in accordance with Article 42 and k) any other burden or a mitigating factor arising from the circumstances of the particular case, such as the financial benefits obtained or damages avoided, directly or indirectly, from the infringement. 3. In the event that the controller or processor, for the same or related processing operations, violates several provisions of this regulation, the total amount of the administrative fine does not exceed the amount set for the most serious violation. 4. Violations of the following provisions shall attract, in accordance with paragraph 2, administrative fines of up to EUR 10 000 000 or, in the case of undertakings, up to 2 % of the total worldwide annual turnover of the previous financial year, whichever is higher: a) the obligations of the controller and the processor in accordance with Articles 8, 11, 25 to 39 and 42 and 43, b) the obligations of the certification body in accordance with Articles 42 and 43, c) the obligations of the monitoring body in accordance with Article 41 paragraph 4. 5. Violations of the following provisions shall attract, in accordance with paragraph 2, administrative fines of up to EUR 20 000 000 or, in the case of undertakings, up to 4 % of the total global annual turnover of the previous financial year, depending whichever is higher: a) the basic principles for the processing, including the conditions applicable to the authorization, in accordance with Articles 5, 6, 7 and 9, b) the rights of the data subjects in accordance with Articles 12 to 22, c) the transmission of personal data to a recipient in a third country or an international

organization in accordance with articles 44 to 49, d) any obligations under the law of the Member State established pursuant to chapter IX, e) non-compliance with order or to temporarily or permanently limit the processing or to suspend the circulation of data imposed by the 13 supervisory authority pursuant to Article 58 paragraph 2 or not providing access in violation of Article 58 paragraph 1." According to Guidelines 3/2019 on the 17. processing of personal data through video devices, which were issued on January 29, 2020: "3.1 Legitimate interest, Article 6(1)(f) 17. The legal assessment of Article 6(1) (f) should be based on the following criteria in accordance with 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. The existence of a legitimate interest, as well as the necessity of monitoring should be re-evaluated at regular intervals (eg once a year, depending on the circumstances). (…) 22. Legitimate interest can also constitute situations of imminent danger which are located in banks or shops selling valuable 14 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 be appropriate, relevant and limited to what is necessary for the purposes for which they are processed ("data minimization"), see Article 5 paragraph 1 item 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 off 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 works at night, as well as outside of normal business hours, meets the need of the controller to prevent any danger that threatens his property. 27. As a general rule, the need for video surveillance to protect the premises of the controller ends at the boundaries of the property. However, there are also cases in which video surveillance of the property is not enough to effectively protect the property. In some individual cases, it may be necessary to extend video surveillance to areas 15 adjacent to the premises. In this case, the controller should use physical and technical means, removing e.g. from the video material the areas not relevant to the purpose of the surveillance or presenting said areas with pixels. (…) 29. Questions concerning the necessity of the processing are also raised about the way in which the data is preserved. 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." 18. Based on Guidelines 5/2020 on consent under Regulation 2016/679, issued on 4 May 2020, “21. of employment. Imbalance Given 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 his refusal. It is unlikely that the employee will be able to freely respond to the requestpower also exists in the context reliance that entails considering 16 his employer's consent to, for example, the activation of surveillance systems such as workplace camera observation, or the completion of assessment forms, without feeling pressured to give consent. 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. 22. However, this does not mean that employers can never use consent as a lawful basis for processing. There may be circumstances in which the employer can demonstrate that consent is indeed freely given. Taking into account the power imbalance between the employer and his staff members, employees may freely give their consent only in exceptional circumstances, when giving or not giving consent would not have any negative consequences." 19. I also took into account the following Decisions, Instructions and Announcements related to the incident: Cyprus Supervisory Authority - Office of the Commissioner for Personal Data Protection: 10/2/2011 – Decision to remove CCTV cameras in Bank of Cyprus offices, 25/04/2016 – Decision to uninstall CCTV inside the employees' offices and invalidity of the consent in the work context, 24/05/2018 – Investigation of a complaint about the installation and operation of Closed Circuit Video-Surveillance, which also records sound in offices of the company GAN DIRECT INSURANCE LTD, 31/03/2022 – Operation of Closed Circuit Video-surveillance in the area of the children's clinic and dental office Announcement of date 28 June 2019 for the Installation of Closed Circuit Video Surveillance (CCTV) in areas accessible to the public Announcement dated October 26, 2021 for the Installation of Closed Circuit Video Surveillance (CCTV) and the role of Management Committees and Management Companies, in apartment buildings for data processing 17 - Personal Data Protection Authority Greek Supervisory Authority Nature: Decision 23/2021 Decision 24/2021 Directive 1/2011 Rationale 20. According to Article 4 of the Regulation, image/video data if they refer to natural persons constitute personal data. Collecting, storing, retrieving, searching for information, using personal data is processing. Therefore, downloading and storing video via CCB is processing. The Complainant, like any other person, whose data was processed through the KKBP, are the data subjects. The Complainant, specifying the purpose and method of personal data processing, recommends the data controller. 21. As mentioned by the Defendant in the complaint, the reason for the establishment and operation of the KKBP was the safety and smooth operation of the business, as well as the safety of its personnel. Kathy, considering her financial and other activities as well as the

location of her building, determined that she was at high risk of burglary. He therefore considered that to ensure the desired protection, the video-surveillance circuit was the appropriate measure to be taken. 22. Based on the Guidelines 3/2019 but also on Article 6(1)(f) of the Regulation, processing through GDPR, which is necessary to protect the legal interests of the data controller, from a real risk condition (e.g. . robbery, theft or vandalism), may be legal, if it does not override the interests or fundamental rights and freedoms of the data subjects. As noted, GDPR should only be chosen if the purpose of the processing could not reasonably be fulfilled in another way, such that the fundamental rights and freedoms of the data subjects would be affected to a lesser extent. 23. Employees, coming to their workplace, still enjoy the right to their private life. The reception and processing of personal data with a CCB that operates permanently, inside offices, meeting and waiting areas, offends the personality and privacy of the staff, encroaching on their rights and freedoms. In the present case, I judge that the legal interest of the Client does not prevail over the rights of the data subjects, so the receiving and processing of personal data through the KKBP in the interior of the building is not legal, as it does not meet any of the conditions of Article 6 of the Regulation. 24. In the present case, the Defendant had installed cameras in 21 places, recording images from the inside and outside of the company. In no case, the recording of the interior spaces of the offices, the waiting areas and also the meeting rooms, cannot be considered as a measure commensurate with the purpose that the Defendant wanted to fulfill, i.e. the protection of her property. On the contrary, the recording of staff throughout their work, but also of customers/partners during meetings, is deemed excessive and inconsistent with the principle of data minimization (Article 5 of the Regulation). 25. Next, I emphasize that Ms. XXX was able to monitor the staff in real time. This feature allowed XXX to intrude into the privacy of staff to a greater extent than it would have been allowed if there was no projection screen and the material was stored directly. 26. In no case can securing the consent of the staff make legal the processing carried out by the Defendant through the CCBP. Firstly, as I have explained above, the processing in question conflicts with one of the basic principles of personal data processing as defined in Article 5 of the Regulation, so the consents obtained do not remove this illegality. Secondly, based on Article 7 of the Regulation, the consent of data subjects should be free, explicit and can be revoked at any time. In this case, due to the employer-employee dependency relationship and the significant power imbalance between the two, obtaining consent cannot be considered free. 27. In reviewing the snapshots of the 8 exterior cameras, I found that the CCTV was capturing images from public areas (streets/sidewalks, etc.), in addition to Kathy's private property. As explained in recital 47 of the Preamble of the Regulation, the existence of a legitimate interest is assessed, among other things, in terms of whether the 19 data subject,

at the time and in the context of the collection of the personal data, can reasonably expect that for this purpose processing is carried out. 28. People who pass through adjacent streets, buildings and sidewalks, of Kathy's building, do not expect to be recorded by the cameras she had installed. As above, the video recording of passers-by is deemed excessive and irrelevant to the purpose the Defendant sought to achieve, thus violating the principle of data minimization as defined in Article 5 of the Regulation. Also, under no circumstances does the Defendant's right to protect her legal interests legitimize the taking of images of a public space and the video recording of passers-by, with the result that its operation does not meet again any of the conditions of Article 6 of the Regulation. 29. As stated by the Defendant, the illegal recording of public spaces was due to ignorance of the law. However, ignorance of the law is no defense for any person. All of us must know the legal framework that defines our actions and not act contrary to it. property 30. I emphasize that, in order to achieve the desired purpose, i.e. the protection of security and the smooth operation of the business, the Complainant should first of all take alternative security measures, such as installing alarm systems, fencing her, hiring security staff, installation of security locks, control of entry/exit by staff in the waiting area, etc. 31. After the application of the above and if the Court considered that these were not sufficient, in which case the installation of the KKBP was also necessary, then the image capture should be limited to very specific points which would be in accordance with the purpose she sought to achieve. achieve. In particular, it could be allowed to take a picture at the entrance/exit of the building, in the parking lot of the building, above the safe or the cash register.is recorded. Therefore, she should be able to use them

suitable physical and technical means that will allow it to focus,

such as for example the removal from the video footage of non-

relevant to the purpose of monitoring areas or presenting them with

pixels.

32. I point out, that the evaluation of the necessity of the use of the CCBP

it is not done arbitrarily and vaguely, but after a thorough examination of the circumstances

which mandate it as compulsory. Each controller must

such as, investigates in depth the need to install a PPE, conducts an Assessment

Impact in advance when required, is always able to account

to the competent supervisory authority presenting sufficient evidence for this

need, and re-evaluates the need to use the CCCP periodically

intervals.

33. Access to the

video footage, but also its retention period. In

in this case, the preservation of the material for 45 days and the

real-time personnel tracking by XXX, no

was sufficiently justified by the Defendant, as it should have been, based on Article 5(2) of

Regulation, in which case it is deemed disproportionate to the purpose.

34. As I have observed, in the staff notification form for the

installation of the KKBP, it was mentioned, among other things, that its operation would

helped in "Monitoring and improving productivity". Although in the written positions

of Kathy this purpose was never mentioned, I consider it very important to

draw her attention and mention that no one is allowed

occasion to control personal conduct, personal contacts and

employee efficiency through HRD.

35. Regarding access to the screen where the image was displayed

reception of the cameras of the KKKP, I judge that there is not sufficient evidence to

document further violations than the ones above that I have already identified.

I take into account the reports of the installation company of the KKBP, which

confirm Ms.'s positions, and I note that, access to images

receiving a CCPP should have a specific and specifically authorized

staff, which will be deemed necessary for the fulfillment of

purposes served by said installation and operation.

36. The Complainant had posted 2 warning signs for

the operation of the KKBP. Number which I consider was not sufficient for the

number of cameras that were placed inside and outside the building. As I have

formulated in my previous Announcements, dated June 28, 2019

21

and October 26, 2021, which are also posted on his website

My office, the use of warning signs for the CCBP operation

is mandatory. Warning signs should be prominently displayed

places, sufficient in number and clearly visible to the persons recorded. At

said signs must state that video recording is being done, the purpose

of the video recording and data of the data controller.

the full cooperation of Ms. the complaint with my Office and

the absence of malice or intent to violate on the part of the Defendant,

the number of previous decisions and announcements they have

compliance with my Order dated July 22, 2022;

the non-existence of another, previous, incident on the part of Ms.

Conclusion

37.

On the basis of the above findings and on the basis of the powers given to me

provided by Articles 58 and 83 of Regulation (EU) 2016/679, I find

violation of Articles 5 and 6 of the Regulation.

38. Based on the provisions of Article 83 of the Regulation, insofar as

apply in this particular case, I consider them below

mitigating (1)-(4) and aggravating (5)-(7) factors:

(1)

the submission of data with complete transparency,

(2)

(3)

her,

(4)

(5)

issued by my Office, relevant to the subject of this complaint,

(6)

of the data,

(7)

the operation of the KKBP for a period of approximately one year and the

video recording of a crowd of people inside and outside the building

of Kathy.

39. In exercising the remedial powers conferred on me by Article 58(2)(b)

and (d) of the Regulation, pursuant to which:

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

(b) to address reprimands to the data controller or the executor thereof

processing when processing operations have violated provisions herein

regulation

d) instruct the controller or processor

to make the processing operations in accordance with the provisions hereof

regulation, if necessary, in a specific manner and within a certain period

deadline".

the non-detection of the violation by the Defendant, but by the subject

22

40. I decided,

at my discretion and subject to the above provisions, to address:

Reprimand to the Complainant for the violation of Articles 5 and 6

of Regulation (EU) 2016/679,

Ordering the Complainant to completely disable the cameras

of the CCBP that take an image inside the offices, the waiting areas

and meetings,

Ordering the Complainant to completely deactivate them

outdoor cameras that take an image from public places and spaces

outside of her private property,

Order to the Complainant as in the case of receiving additional

alternative security measures and deems it necessary to operate PPE,

apply appropriate technical and organizational measures, as described in

Legal Framework and Reasoning of this Decision, so that the cameras

of the KKBP that may be put into operation to be in accordance with its provisions

Regulation (EU) 2016/679.

Irini Loizidou Nikolaidou Nicosia, September 2, 2022

Data Protection Commissioner

Personal Character