PRIVACY PROTECTION AND STATE TRANSPARENCY Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 PRESCRIPTION-WARNING in the case of personal data protection no. 2.1.-1/21/3177 Prescription author of Data Protection Inspectorate lawyer Raiko Kaur Time and place of issuing the injunction 31.01.2022, Tallinn Addressee of the injunction responsible person Vipex AS (10170170) info@vipex.ee Board member RESOLUTION: § 56 subsection 1, subsection 2 clause 8, § 58 subsection 1 of the Personal Data Protection Act (ICS) and According to Article 58 paragraph 1 point d and paragraph 2 points d, e and f of the General Personal Data Protection Regulation (GPR), as well as taking into account Articles 5, 6, 12 and 13 of the GPR, the Data Protection Inspectorate issues a mandatory order for Vipex AS to comply with: 1. Remove Vipex AS- i audio recording from the customer service center (see points 2 and 3.1 of the inspection's reasons); 2. Notify employees of the violation related to the use of audio recording (see point 3.4 of the inspection's reasons). Send the inspection a copy of the letter that was sent to the employees regarding the violation. 3. Provide the inspection with a clear and comprehensible legitimate interest analysis that meets the conditions set forth in Article 6(1)(f) of the IKÜM, that is, by reading it, it is possible for both the inspection and the data subjects to clearly understand the following (see points 2.1 and 3.2 of the inspection's reasons and its subsections): a) what are the specific legitimate interests of Vipex AS; b) for what reason is the use of video surveillance and video recordings actually necessary for the realization of the legitimate interests specified in point a; c) what are the rights and freedoms of employees that are violated when video surveillance is used; d) how do the legitimate interests of Vipex AS (points a and b) outweigh the interests and fundamental rights of the data subject (point c). 4. To transmit the locations of all cameras used in Vipex AS and excerpts of their camera images (see point 3.2.3 of the reasons for the inspection); 5. Submit a sample of the camera recordings/viewing live image log showing who and Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 when (date, time (period)) viewed the camera recordings (see point 2 of the inspection's reasons); 6. Send confirmation to the inspection that the video recordings will be deleted immediately, but no later than after 72 hours (see points 2 and 3.3 of the inspection's reasons). A longer storage period is allowed if Vipex AS has substantiated the need for a longer storage period and the inspection has given a corresponding confirmation; 7. Submit data protection conditions that fully meet the requirements set forth in Articles 12 and 13 of IKÜM (see points 2.2 and 3.5 of the inspection's reasons). We set the deadline for the execution of the injunction to be 22.02.2022. Report compliance with the order to the e-mail address of the Data Protection Inspectorate at info@aki.ee by this deadline at the latest. REFERENCE FOR DISPUTES: You can contest this order within 30 days by

submitting either: - an appeal in accordance with the Administrative Procedure Act to the Data Protection Inspectorate or - an appeal in accordance with the Administrative Court Procedure Code to the Tallinn Administrative Court (in this case, the appeal in the same matter cannot be reviewed). Challenging a precept does not stop the obligation to fulfill it or the implementation of measures necessary for fulfillment. EXERCISE MONEY WARNING: If the injunction has not been complied with by the specified deadline, the Data Protection Inspectorate will impose a fine of 15,000 euros on the addressee of the injunction based on § 60 of the Personal Data Protection Act: Extortion money for each unfulfilled injunction point. A fine may be imposed repeatedly - until the injunction is fulfilled. If the recipient does not pay the penalty, it will be forwarded to the bailiff to start enforcement proceedings. In this case, the bailiff's fee and other enforcement costs are added to the enforcement money. MISCONDUCT PUNISHMENT WARNING: Failure to comply with the prescription under Article 58 (1) of the Personal Data Protection General Regulation may result in a misdemeanor proceeding based on § 70 of the Personal Data Protection Act. For this act, a natural person may be fined up to EUR 20,000,000, and a legal person may be fined up to EUR 20,000,000 or up to 4 percent of its global annual turnover of the previous financial year, whichever is greater. The out-of-court procedure for a misdemeanor is the Data Protection Inspectorate. FACTUAL FACTS: On 13.10.2021, the Data Protection Inspectorate (inspection) initiated a self-initiated supervisory procedure regarding Vipex AS, within the framework of which we wanted to know, among other things, the following: 1. If the cameras are used, among other things, on the basis of IKÜ Article 6(1)(f) (legitimate interest), then submit a comprehensive legitimate interest analysis, based on which the inspection would be able to assess the legality of the use of cameras. 2. Forward all documents that regulate the use of cameras and that have been introduced to employees. If the document is not only related to the use of cameras, refer to the specific points in the document that specifically regulate the use of cameras. 4.1. If the prepared documents and notification do not meet the requirements set forth in Articles 12 - 13 of the IKÜM, prepare the correct data protection conditions without delay, but no later than by the response deadline, and forward them to the inspection. Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 On 26.10.2021, the representative of Vipex AS sent a reply, in which, among other things, the analysis of legitimate interest was forwarded. In terms of data protection conditions, it was noted: The document "Use of surveillance cameras in AS Vipex" has been prepared in accordance with articles 12 - 13 of the IKÜM. In the following, we assess the compliance of the above with the requirements of IKÜM. REASONS FOR THE DATA PROTECTION INSPECTION: 1. Processing of personal data Personal data is any information about an identified or identifiable natural

person. An identifiable natural person is a person who can be directly or indirectly identified (see Article 4 point 1 of the General Regulation on the Protection of Personal Data (GPR)). With the help of cameras, a person (especially an employee) can be identified in any case. Vipex AS also stated: Surveillance cameras are simple devices that can be installed around if necessary, 1 of which has audio recording (located in the cash handling area of the customer service center). The voice is also a personal gift, by which it is possible to identify a person. In the case of video and audio surveillance (audio recordings), it is a matter of personal data processing, which must comply with the requirements set forth in the General Regulation on the Protection of Personal Data (GPR). 2. Principles of personal data processing The controller of personal data is obliged to comply with the principles set forth in Article 5, paragraph 1 of the IKÜM. The responsible processor himself is responsible for the fulfillment of these principles and must be able to prove their fulfillment (see IKÜM Article 5 paragraph 2). To the extent that data processing does not fully comply with the principles set forth in Article 5, paragraph 1 of the IKÜM, data processing is prohibited. The use of cameras must be based on, among other things, the following principles of personal data processing: - Legality, fairness and transparency (IKÜM Article 5(1)(a)) Any processing of personal data must be fair and legal, i.e. fully in accordance with all applicable legislation (including IKÜM and IKS). Data processing must also be transparent. The principle of transparency requires that all information related to the processing of personal data is easily accessible, understandable and clearly formulated for the data subject. This primarily concerns the notification of data subjects in order to ensure fair and transparent processing (see Recital 39 of the IKÜM). Informing people is more precisely regulated by articles 12 - 14 of the IKÜM. Articles 13 and 14 of the IKÜM state what the information given to a person must contain as a minimum. The use of cameras must be based on the requirements of Article 13 of IKÜM. - Purpose and retention limitation. Collection of as little data as possible (IKÜM Article 5(1) points b, c and e) In order to assess whether the use of cameras complies with the principle of goal limitation and collection of as little data as possible, it is necessary to: 1. state all specific purposes; 2. assess whether the use of cameras is necessary for the fulfillment of the stated objectives or whether there are other measures that are less intrusive to the data subject. It is forbidden to monitor employees with cameras during the entire working time, and the cameras must be directed to specific security risks. The processing of personal data must be stopped and the data must be deleted or transferred to a non-personalized form as soon as the legal basis ceases and/or the purposes for which they were collected have been fulfilled. The time for processing personal data must be strictly limited to the minimum. In order to ensure that personal data is not processed longer than necessary 

Registry code 70004235, the data controller must determine the deadlines for deleting personal data and for periodic review (see also IKÜM justification point 39 ). Regarding the storage of camera recordings, the European Data Protection Board has stated the following in its guidelines 3/2019 on the processing of personal data in video devices1: Taking into account the principles set out in points c and e of Article 5 (1) of the General Regulation on Personal Data Protection, namely the collection of as little data as possible and the limitation of storage, personal data should in most cases (e.g. to detect vandalism) to be deleted - ideally automatically - after a few days. The longer the prescribed retention period (especially if it is longer than 72 hours), the more the legitimacy of the purpose and the necessity of retention must be justified. If the controller uses video surveillance not only to monitor its premises, but also intends to store the data, the controller must ensure that the storage is actually necessary to achieve the purpose. If storage is necessary, the storage period must be clearly defined and established separately for each specific purpose. The controller is responsible for determining the retention period in accordance with the principle of necessity and proportionality and for proving compliance with the provisions of the General Regulation on the Protection of Personal Data. Therefore, in a situation where a storage period longer than 72 hours does not follow from the special law, the responsible processor must clearly and comprehensibly justify the need for a longer storage period of the recordings. However, the inspectorate does not agree that the necessity of the recording retention period can be measured in months. The longer the retention period, the greater the burden on data subjects, especially employees, because longer time means more data. - Personal data is processed in a way that ensures the appropriate security of personal data, including protection against unauthorized or illegal processing (Article 5(1)(f) of IKÜM) In order to be able to check who, when and which camera recording has been viewed, a logging system must be created. According to the inspection, logging is the only possible way to check that the camera's live image or recordings have not been viewed illegally, including without reason. 2.1. Preparing a legitimate interest analysis If the data processor relies on a legitimate interest in the processing of personal data, it is legal if the processing of personal data is necessary for the legitimate interest of the data controller or a third party, unless such interest is outweighed by the interests of the data subject or the fundamental rights and freedoms of which personal data must be protected on behalf of (IKÜM Article 6(1)(f)). Thus, IKÜM article 6 paragraph 1 point f stipulates three conditions, all of which must be met in order for the processing of personal data to be permitted: - the controller or the third party or third parties receiving the data have a legitimate interest in data processing; - the processing of personal data is necessary for the exercise of a legitimate interest; - the legitimate interests of the data controller and/or third party outweigh the interests, fundamental

rights and freedoms of the protected data subject. In order to understand whether it is possible to process personal data on the basis of Article 6(1)(f) of the IKÜM, it is first necessary to find out exactly whether and what the specific legitimate interests of the data processor are. Legitimate interests must be formulated clearly enough. This requires a real and present interest – something related to an activity currently taking place or a benefit expected to be received in the near future. In other words, interests that are too vague or speculative are not enough. If the legitimate interests are not formulated clearly enough, it is not possible to balance said interests with the interests and fundamental rights of the data subject. 1 https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_et.pdf page 28 p 121 Tatari st 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 Therefore, it is first of all important that the legitimate interest is in accordance with the current legislation, formulated clearly enough (ie sufficiently specific) and real and present at the moment (ie not speculative). Secondly, it is necessary to analyze and consider what are the possible interests or fundamental rights of the data subject - and freedoms that may be harmed by the processing of personal data. Thirdly, the legitimate interests of the data processor must be balanced with the interests and fundamental rights of the data subject. In doing so, the possible impact on the data subject from the processing (collection, transfer, disclosure) of personal data is compared with the legitimate interests of the controller and/or third party, and it is assessed whether and to what extent the legitimate interest of the controller and/or third party outweighs the interests of the data subject. We emphasize that the legitimate interests of the controller or a third party do not automatically outweigh the interests related to the fundamental rights and freedoms of the protected data subjects. If the data processor fails to perform one of the previous steps correctly, data processing is not permitted on the basis of Article 6(1)(f) of the IKÜM, and the inspectorate has the right to prohibit further processing of personal data. It must be possible for every data subject (both customer and employee) to familiarize themselves with the legitimate interest analysis. 2.2. Drafting of the data protection conditions The following must be reflected in the data protection conditions, among others (see IKÜM article 13 paragraphs 1 and 2): - the name of the data controller and his contact details; - purposes and legal bases of personal data processing; - if the processing of personal data is based on a legitimate interest, information about the legitimate interests of the controller; - information about recipients or categories of recipients of personal data; - term of personal data storage; - information on the data subject's right to request: a) access to personal data concerning him (both customers and employees have the right to receive records about themselves); b) deletion of personal data; c) restriction of personal data processing. - information about the right to object to the use of cameras; -

information about the rights to file a complaint with the supervisory authority. However, each data controller must draw up data protection conditions based on their own business activities and check their compliance with the requirements set forth in Articles 12 - 13 of the General Data Protection Regulation. In addition, we explain the following: - data protection conditions must be drawn up in accordance with the actual data processing. The conditions cannot be limited to examples, but the list must be exhaustive. The use of the words "for example, in particular, among others" is not allowed. If the content or purposes of data processing change over time, the data protection conditions must be updated accordingly. - In the case of customers, the legitimate interest analysis must either be included in the data protection conditions, or must be highlighted in the conditions, so that an e-mail can be sent to a specific e-mail address to view the analysis. However, employees must be able to consult the legitimate interest analysis at any time (e.g. in the break room or in the institution's internal information system). Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registry code 70004235 3. Compliance with IKÜM requirements 3.1. Vipex AS's legal basis for using audio surveillance We explain that it is theoretically possible to use audio surveillance only if a correct legitimate interest analysis has been prepared and it shows that the legitimate interests of the company outweigh the interests of the data subject. Such an analysis has not been prepared by Vipex AS regarding audiovalve. Based on IKÜM, the inspection has analyzed the use of audio surveillance. There are certainly situations where audio recording is useful. However, accepting the permissibility of using audio surveillance to ensure security, resolve customer disputes, detect possible fraud, etc. leads to the same situation we are in with video cameras. It would become a new reality at every turn. But video surveillance has not always been the normality of everyday life either. Over time, video surveillance is exploited more and more, while the functionalities and quality of video surveillance improve. Over time, people have accepted the inevitability of video surveillance being used on such a large scale. Starting to use audio surveillance for the same purposes, step by step at first in some companies, it spreads indiscriminately everywhere. Furnishings and the sale of finishing materials in the salon are not so special in nature that audio surveillance can be considered permissible only there. You provide a civil law service in exactly the same way - you sell goods like any other civil law service provider (shop, service point). Therefore, the Data Protection Inspectorate does not consider audio surveillance inherently permissible in companies engaged in the provision of goods and services. Only very exceptional circumstances that do not exist elsewhere could justify the use of Audiovalve. The European Data Protection Inspector has already stated in 2010 that the use of audio recordings in the workplace is prohibited.2 This is also confirmed in the guidelines of the European Data Protection Board, which state that

monitoring devices should not offer functions that are not necessary (e.g. audio recordings). Therefore, unnecessary functions must be deactivated or monitoring devices with no additional functions must be used. 3 Since the use of audio surveillance in the workplace is prohibited by its very nature, and Vipex AS has not pointed out exceptional circumstances, due to which it would still be necessary to use audio recordings in the workplace, the inspection is of the opinion that in the representative office of Vipex AS audio surveillance is not allowed due to IKÜM. 3.2. Vipex AS legitimate interest analysis in the use of video surveillance 3.2.1. Legitimate interests of Vipex AS and their necessity Vipex AS has stated that video surveillance is used for the protection of persons and property, for the detection of legal violations, for finding out the circumstances of accidents at work, and for checking the employee in a situation where the customer makes a claim that the goods have not arrived or that the goods have been issued in less quantity. Regarding the necessity of checking the employee, the following is stated: It is necessary to monitor the process of receiving and handing over the goods with a video camera to avoid later disputes. There are several cases where we have received a claim regarding the quantity of delivered goods. Claims have also been made that a particular shipment was not among the goods that arrived. The camera recording allows you to check, among other things, whether the ordered goods were delivered correctly. 2 European Data Protection Supervisor, Video-surveillance Guidelines, 2010, p 6.12. 3 European Data Protection Board, Guidelines 3/2019 on the processing of personal data in video devices, 2020, point 129 Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 According to the inspection, the legitimate interest of Vipex AS in the use of cameras is understandable in the warehouse, i.e. the protection of the materials in the warehouse, possible accidents at work and control of the delivery of goods. However, Vipex AS has justified the necessity of using cameras only in the part that concerns the reception-handover process. However, the factual circumstances and how often the aforementioned situations occur or have occurred have not been identified. Perhaps the inspection is not clear: 1. How often thefts occur or have occurred in the warehouse (state how many thefts are committed, e.g. per month/year) and what has been stolen; 2. How often have occupational accidents occurred (specify, for example, how many occupational accidents have occurred per year) and which ones; 3. How often do employees make mistakes with the quantity when handing over goods (specify, for example, how many mistakes there are per year) and what kind of goods have been made wrong when handing over, and in what large quantities. 4. How often has it been necessary to use camera recordings for the protection of persons and in which cases. It must also be explained why cameras are necessary to check/assess the above and why other and less intrusive measures cannot be used. However, the use of cameras in the

showroom remains unclear. If Vipex AS considers that the use of cameras in the sample room is necessary for the realization of the aforementioned legitimate interests, then the above four questions must also be answered taking into account, among other things, the special features of the sample room, i.e. the fact that there are samples in the sample room. 3.2.2. Interests or basic rights and freedoms of the data subject In this point, it is important to thoroughly analyze the possible interests or basic rights and freedoms of the data subject that may be harmed by the use of cameras. This point has not been fulfilled by Vipex AS. We explain that the possibility of monitoring employees during the entire working time leads to a very high level of interference. It is not possible for the employee to make any movements in such a way that his actions cannot be monitored (except in the daily life and rest rooms). This, in turn, can cause stress, anxiety and other mental problems in employees. The inspection has also received an appeal, where it was stated that Vipex AS as an employer monitors the activities of employees through cameras, and it is not about identifying anything, but monitoring employees. 3.2.3. Balancing the legitimate interests of Vipex AS and the interests, fundamental rights and freedoms of data subjects As Vipex AS has not formulated its legitimate interests sufficiently clearly and comprehensibly (there are no factual circumstances and these are speculative interests) and the interests of the data subject, which may be harmed by the use of cameras, have not been assessed, it is not it is possible to balance interests. However, we reviewed the explanations of Vipex AS and submit our comments. Vipex AS stated: Employees' workplaces that are within the camera's field of view are covered by a privacy fee so that employees' privacy is fully guaranteed. The inspection does not understand what Vipex AS meant by this. On the website of Vipex AS, it is possible to take a virtual tour of the furnishing salon (https://vipex.ee/kontakt/virtuaaltuur/), during which it is also possible to identify the locations of the cameras. The inspection found that Vipex AS has installed cameras in such a way that they are aimed directly at employees' workplaces, including computer screens. The use of cameras in this manner is not permitted. In order to assess the extent of the use of cameras, the inspection wants the locations of all cameras and excerpts of their images. Vipex AS stated: Although it is not always possible to foresee all activities in the processing of personal data during work, because business activity sometimes requires quick responses and therefore quick changes in work processes, AS Vipex adheres to the principle of minimality when processing personal data: Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 as little as possible and only as much as necessary. It remains unclear what such a sentence means in the analysis of legitimate interest. If Vipex AS has in mind that the cameras can be used for any purpose, if it is necessary for changing business activities and work processes, then this is not correct. The goals must be established before

using the cameras, and if the goals should change over time, an additional legitimate interest analysis must be performed and the data subjects (employees, customers) must be informed of the change in goals. We agree that the use of cameras is not based on consent, but regulating this in a legitimate interest analysis is unnecessary and gives the wrong impression. We emphasize that the analysis of legitimate interest is intended for data subjects (employees, customers), therefore it must be so clear and understandable that every data subject can understand, by reading the analysis of legitimate interest, what are the legitimate interests of the company, which interests of the data subject have been assessed when using video surveillance, and how in the balancing of interests, it was reached that the use of video surveillance is necessary and outweighs the interests of the data subject. Considering that the security risks in the sample cabin and in the warehouse are likely to be different, the need to use cameras must be evaluated accordingly. 3.3. Time limit for storing video recordings Vipex AS noted: Recordings are not stored for a long time, they are automatically deleted after four months. Firstly, Vipex AS has not explained why it is necessary to store the camera recordings for four months, and secondly, it is a very long storage period. The longer the retention period, the greater the burden on data subjects, especially employees, because longer time means more data. It is also not very realistic that Vipex AS will review four months of recordings (reviewing this would take a huge amount of time) to identify a possible violation that may have occurred during that time. Since Vipex AS has not justified the necessity of the storage period for camera recordings (four months) and the inspection does not see that such a long storage period can be legitimate, Vipex AS must in the future delete the recordings immediately, but no later than after 72 hours. In the opinion of the inspectorate, in order to protect the rights of employees, it is necessary to establish a limitation on the processing of personal data (limit the term of storage of video recordings) until Vipex AS has proven to the inspectorate that the storage of video recordings for longer than 72 hours actually complies with the principles of personal data processing (see IKÜM Article 5(1)(b, c) and e) and the inspection has confirmed the legality of the longer storage period. 3.4. Notifying employees of a violation The use of an audiovalve represents a very intense invasion of privacy, therefore it is particularly important that in a situation where the audiovalve has been installed illegally, i.e. the installation did not comply and does not comply with the principle of personal data processing (the principle of legality), the audiovalve is immediately removed and employees are also informed of the violation (see IKÜM Article 34 paragraph 1). The breach notification describes in clear and simple language the nature of the breach related to personal data and provides at least the following information (see Articles 34 paragraph 2 and 33 paragraph 3 of IKÜM): 1. Name and contact details of the contact person, through which it is possible to obtain more detailed information

about the breach; 2. Describe the possible consequences of a breach of personal data; 3. Describe the measures taken or planned to be taken to resolve the personal data breach. Therefore, Vipex AS must convey the above information to the employees and confirm to the employees that the audio surveillance has been removed. Tatari tn 39 / 10134 Tallinn / 627 4135 / info@aki.ee / www.aki.ee Registration code 70004235 3.5. Data protection conditions of Vipex AS Vipex AS stated: The document "Use of surveillance cameras in AS Vipex" has been prepared in accordance with articles 12 - 13 of the General Data Protection Regulation. We clarify that the form of the mentioned document is not correct data protection conditions. First of all, sentences have been copied there, which makes reading difficult and the content incomprehensible, and secondly, the content of the document has not been based on Article 13 of the IKÜM (see also point 2.2 of the inspection's reasons for the mandatory content). Based on the above, the submitted document does not meet the requirements stipulated in IKÜM (IKÜM Article 5(1)(a), Article 12(1) and Article 13(1) and (2)). SUMMARY: In summary: 1. Vipex AS has no legal basis (legitimate interest) to use audio surveillance, and the audio surveillance must be removed immediately. Since the audio surveillance has been used illegally, the employees must be informed of the violation. 2. In order to use video surveillance, a correct legitimate interest analysis must be prepared. We emphasize that the analysis of the legitimate interest must be so clear that the employee can understand why the employer actually uses cameras and what he has done to ensure that the employee's rights are not excessively harmed. 3. Cameras must be installed (directed) only at the security risk and ensure that the employees are actually in the field of view of the camera to a minimum. 4. Vipex AS did not justify the necessity of the term for storing the camera recordings, therefore it is not justified to store the recordings for more than 72 hours. 5. Data protection conditions must be drafted that fully meet the requirements set forth in Articles 12 - 13 of the IKÜM. Given that the use of video surveillance in Vipex AS is not legal (there is no correct legitimate interest analysis), a correct legitimate interest analysis must be submitted to the inspection by the deadline or the cameras must be removed (e.g. from the sample salon) and a corresponding confirmation sent. In accordance with § 58 (1) of the Personal Data Protection Act and Article 58 (2) points d, e and f of the General Regulation on Personal Data Protection, the inspectorate has the right to establish a temporary or permanent restriction on the processing of personal data, including a processing ban, and to order that: - the data controller conducts the processing of personal data to certain comply with IKÜ requirements in a manner and within a certain period of time; - the data controller would inform the data subject of a violation related to his personal data. Taking into account the factual circumstances and the fact that in a specific case personal data is processed illegally (data processing does not meet

the requirements set forth in Articles 5, 6, 12 and 13 of the IKÜM), the inspection considers that issuing a mandatory injunction in this case is necessary to end the offense as soon as possible and ensure the protection of the rights of employees. /signed digitally/ Raiko Kaur lawyer under the authority of the Director General