

H.M. HOUSEMARKET (CYPRUS) LIMITED

**Information Note about the use of video surveillance (CCTV) systems**

**Introduction**

The company under the name «H.M. HOUSEMARKET (CYPRUS) LIMITED» having its registered seat in Nicosia, at 5, Esperidon Str. (hereinafter referred to as the «Company») shall inform any person coming to its offices and stores (hereinafter referred to as “Subjects” or “Data Subjects") that it makes use of a closed circuit surveillance system (CCTV) under the Regulation EU 679/2016 (hereinafter referred to as the «Regulation» or «GDPR») and the relevant national law 125(Ι)/2018 implementing the above Regulation.

1. Principles governing the processing

The processing of images recorded through the video surveillance system CCTV is governed by the following principles:

**Legality principle:** The CCTV system is operating under the provisions of the national and European legislation, as well as the Directives and Decisions of the supervisory authorities and organs (indicatively mentioned are the Directives of the Data Protection Authority, Guidelines of the European Data Protection Council as well as of the Article 29 Working Party and so on) only for the purposes specified in this information note.

**Confidentiality Principle:** The CCTV system is operating on the basis of the protection of the subjects’ privacy.

**Necessity Principle**: The system has been designed in a way that it records the cases where people moving in the supervised areas or the Company’s property or its customers’ property or its employees’ property is in jeopardy.

**Data minimisation principle:** The data collected through the CCTV system are adequate, related and not excessive for the purpose of their collection. As regards each device a risk assessment has been conducted (in relation to the data safety and protection), as well as an impact assessment (in relation to the personal data protection), aiming at a minimization in the supervision of areas, where this supervision is not necessary. The video surveillance system of the Company has not been designed in such a way so that it can collect sensitive personal data.

**Accuracy, Availability and Integrity Principle:** The personal data collected through the CCTV system are subject to processing in a way that it guarantees the proper safety of personal data, making use of the appropriate and proper technical and organizational safety measures, as these are described in detail below.

1. Purposes and legal base of the video surveillance system (CCTV) operation

The processing is required for purposes of legal interests, which we are seeking as controllers (article 6 par.1.f GDPR). Our legal interest consists of our need to prevent, manage and investigate incidents concerning the safety of the employees, customers and visitors of our premises, as well as their property from risks and, especially:

* In order to assist in the prevention, disclosure, avoidance, management and, when this is necessary, investigation of incidents related to the safety and protection, of possible risks or of the unauthorised physical access, including the unauthorised access to protected areas of the Company’s stores.
* In order to assist in the investigation of the theft of equipment or other property objects of the Company, of the employees, of the lessees, or the visitors as well as in the investigation of threats in the safety and security within the premises.
* In order to monitor the safety and security of the business facilities of the premises.
* In order to ensure compliance with the health and safety regulations.
* In order to ensure the prevention and avoidance of theft, breakage or other illegal act that may cause non-material damage of property in the areas/facilities of the premises.
* In order to secure the protection of the employees’, lessees’, and visitors’ property.
* In order to safeguard the monetary transactions in the business areas of the premises.
1. Installation facilities of the video surveillance system (CCTV)

The cameras of the video surveillance system have been installed in specific areas of the premises, at a visible spot with a suitable warning label, mainly in the entry points (so that the entrants can be informed that they are entering an area covered by a CCTV system) and exit points as well as in areas where financial transactions take place and in areas where supplies and equipment are secured and safeguarded and/ or in the parking area of the premises. The complete display/ mapping of the separate cameras is found in the Annex 1.

The Controller does not take shots of people in areas where the Data Subjects have increased expectations about their privacy, such as, indicatively, a) in WCs and toilet vestibules and gangways; and b) in restrooms for personnel and customers.

1. Technical Specifications of the System

The video surveillance system of the Company is a conventional CCTV system. All TV cameras are operating 24 hours a day / 7 days per week. The quality of the image/picture allows in most cases the identification of persons located within the functioning scope of the cameras but, although the system is recording digital images, the taking of high definition pictures and images containing biometric data is not feasible. We do not use high tech surveillance systems, we do not connect our systems to other systems and we do not use voice recording systems or “CCTV recording systems with a speaking option”. The images/pictures are saved in digital video recording devices which are kept in safe, locked places, to which only the authorised personnel has access, and the technical specifications are kept in full detail in the compliance file.

1. Recording and Maintenance of Images

The data maintenance period, on the basis of the aforementioned processing purposes, is determined in fifteen (15) calendar days. After the lapse of the 15 days, the data saved in a pc-hardware or in external discs such as in DVDs, USB discs are destroyed or erased completely. In case of an incident, accident or theft, in the supervised areas, the Company is allowed to keep the recordings, in which the specific incident has been recorded in a separate file for three (3) months with the purpose of using the data as evidence in court proceedings. In exceptional cases, when the incident requires further investigation, the period for data maintenance may be extended for the necessary period of time for the maintenance of the said recordings.

1. Access to the videos and transfer of data

The maintained material is accessible only by our competent/authorized personnel, who is assigned with the security of the area.

The Controller is obliged to transfer to the competent judicial, public prosecution, police authorities etc. data lawfully requested by them during the execution of their duties. Furthermore, the controller, apart from its specific obligations and rights provided by the Criminal Procedure Code, may transfer to the competent judicial, public prosecution and police authorities data which may constitute evidence of a criminal act (e.g. theft, beating) committed in the area supervised by the video surveillance system and which may contribute in the investigation of the facts or in the identification of the offenders, as well as the victim or the offender of a criminal act, in case of facts which may constitute evidence of the act.

In case of transfer of data collected by the video surveillance (CCTV) system to third parties, the Data Subject is informed in advance, as long as this is possible, except for the case that the relevant notification is prohibited by law. These data, however, may be communicated without the consent of the Subjects after a specially justified request of a third party, when the data must be used as evidence for the foundation, exercise or support of legal claims or in respect of an investigation procedure of a criminal act and may contribute in the investigation of the facts or in the identification of the offenders.

1. Technical and Organizational Measures

The Company has taken the appropriate technical and organizational measures for the protection and recovery of the personal data of the Subjects collected by means of use of the video surveillance systems.

More specifically, the Company cares for:

− the safety of the recorded material and the prevention of its disclosure to unauthorized recipients;

− the control of the access to the central control area, the repository of the recorded material and to any processing system (at a hardware and software level);

− the prevention of uncontrollable use of projection screens;

− the secure transmission of the recorded events to the authorized recipients and the prevention of transfer of the material to unauthorized recipients;

− the selection of appropriate personnel for the handling of the video surveillance system;

− the continuous training of the personnel in data protection matters and the general respect of the regulatory framework;

− the selection of procedures and products supporting the data protection (privacy by design).

More specifically, the films/DVD saved, the recorded videos as well as the surveillance equipment are kept securely in an area of limited and controlled access. The access is limited to specially for this purpose authorised and trained personnel. The Company conducts and keeps a list with the names of the authorised persons with an access right. All persons who have a right to access the video recorded material have received the appropriate training in relation to the obligation for the protection of the said data with the purpose of ensuring that they will not transfer, communicate or otherwise disclose the content of any video recorded material of the undertaking to third parties with the exception of the authorized recipients. Relevant training is provided to each new member of the personnel.

The measures taken are intended to ensure both the safety, security and integrity of the system, that is the protection from a voluntary or forced intervention through the regular functions and the access control as well as the safety of the personal data, and this means confidentiality (the data can be accessed only by those who must have access), integrity (prevention of loss or alteration of data) and availability (the data can be available when required).

In case of data processing by third parties, the processing is performed only in accordance with the express instructions of the Company and provided the third parties have been contractually bound to take the appropriate technical and organizational protective measures and in accordance with the other obligations pursuant to the GDPR for the best possible data protection against any incidental or illegal destruction or loss, alteration, illegal disclosure or access to these data, and in general against their illegal processing, as well as for the purpose of ensuring the recovery option of availability and access to these data.

1. Rights of the Data Subjects

Each Data Subject is entitled to exercise the access rights, information rights, rights to object/correct and erase his personal data, which (rights) will be satisfied provided this is not incompatible with legal obligations of the Company. If the erasure, due to the special nature of the saving mode, is not possible or is possible only after disproportionately great effort and technical measures, our Company may not erase these data, however, it will proceed to a limitation of the processing in accordance with the article 18 of the GDPR. In the event of an objection the Data Subject should declare the objection to the processing either before the entry, or during the stay or upon exiting the supervised area. In this case, the Company shall cease the processing of the data of the individual who raised objections unless there are compelling legitimate grounds superseding the rights and interests of the data subject. Moreover, you have the right to request from us to limit the processing, for example, not to erase/delete data, which you consider necessary for the foundation, exercise or support of legal claims.

As regards the exercise of these rights as well as for more information and assistance in relation to the collection and processing of the data, as well as regarding the prescribed rights of the Subjects, you can contact the Company to the e-mail address dpo@ikea.com.cy or by calling the number +357 22502502. At the same time you should inform us about the date and time of your face recording and provide us with a recent photograph for your identification, if you desire the erasure of the recording. Further, the verification of the identity of the requesting person should be preceded for the purpose of exercise of his rights (by submission of e.g. a driving license/ passport including a photo etc.).

The Company is obliged to respond to the request of the subject timely and in any case within 30 calendar days from the receipt of a valid request and identification of the subject under the aforementioned after full description of the requested information and with the relevant documentation. The Company has the right to dismiss a claim for a copy of the data, especially when this access could impede the prevention, detection of crimes or the arrest or prosecution of the offenders, as well as when in these images other persons are also illustrated, whose consent for the communication of their personal data cannot be obtained, and it is not possible that editing techniques can be used so that the lack of consent can be handled.

In case the access request is dismissed, the data subject shall be informed in writing and justifiably within the same, as above, period of 30 calendar days.

In case the Company does not respond to any request of data subject or the subject is not satisfied with the Company’s response, the subject reserves the right of filing an appeal before the Commissioner for Personal Data Protection (<http://www.dataprotection.gov.cy>) Offices: Iasonos 1, P.C1082, Nicosia, Call Center: +357 22818456, Fax: +357 22304565, email: commissioner@dataprotection.gov.cy.