NJORD Estonia: Can a smart house be a “backdoor” to your personal data?

Smart houses became a reality a long time ago. Smart house solutions are used for production, commercial and residential buildings. The “smartness” of such houses means that it is possible to regulate, through sensors, detectors, and other devices, the indoor climate of the house and control equipment based on the changes in the external environment or wishes of the user and provide recommendations for users of the building.

Modern solutions can also be managed from a distance, e.g. via a mobile phone. Accordingly, it is possible to control various systems in a building: heating and ventilation systems, lighting, security equipment, closing or opening of doors and windows. Today buildings have systems that show an employee who has arrived at the office car park the way to the vacant parking place with the most convenient location or, by remembering the preferences of employees, a coffee machine offers the employees their favourite coffee or tea.

Smart solutions are developing strongly to make people’s life much more comfortable. Challenges related to the transfer from manual control to automatic and centralised control of devices are of great interest to start-ups as well as large corporations. For instance, Sleepace, a Chinese start-up, has developed a monitoring system that makes it possible to switch off an iron or a TV set left switched on, regulate the temperature and humidity in the bedroom or simulate dawn for a cosier awakening from a distance. In addition, devices can analyse the quality of sleep and provide recommendations for the users of the device for the improvement of the quality of sleep. There are autonomous systems for watering flowers and feeding pets in the world. Thus, the array of functions of smart solutions may be unlimited.

A building is not “smart” only as a result of the devices installed in the building but as a result of the ability to collect and use the data, including the data about the users and residents of the building. Depending on the content of the data, the data may also include personal data, i.e. data by which a natural person can be directly or indirectly identified. As a result, the application of smart technologies may entail risks in the area of ensuring data privacy and cybersecurity, which must be considered by the developers, providers and end users of smart systems. Personal data collected may include data about the personal preferences, habits, and conduct of users of a smart building. For instance, the data of the automatic number-plate recognition system installed in a parking area or garage can reveal the exact time when a car user leaves work or when a resident stays at home. If a personal key card or proximity tag issued to an office employee is also a means for using functions of a smart house, the organisation that has issued the card may ultimately also have access to the personal data of the employee generated as a result of the communication between the smart house and the employee. Modern buildings may provide possibilities as a result of which, upon collection of data, special categories of personal data (i.e sensitive personal data before the entry into force of the EU General Data Protection Regulation) may also be included in the personal data, e.g. if buildings have ceremonial premises for different religions, the data describing the religious and philosophical beliefs of a user of the building can be obtained. Biometric data, such as fingerprints, have been used on door lock systems for years. It is important that employers having offices in smart houses take into account that the monitoring of employees is only allowed in exceptional cases, e.g. if the purpose of such activities is the protection of people and property. As a general rule, monitoring of a specific employee is not allowed.

Processing of personal data is any act performed with personal data, including the collection, recording, organisation, storage, alteration, disclosure, granting access to personal data, consultation and retrieval, use of personal data, communication, cross-usage, combination, closure, erasure or destruction of personal data or several of the aforementioned operations, regardless of the manner in which the operations are carried out or the means used. If data to be processed is personal data, the EU General Data Protection Regulation and the Estonian data protection regulation apply. Based on the data protection regulation, a real estate owner must, among other things, consider that people have rights, incl. the right of access to the data collected about them, the right to have the data rectified and to have personal data concerning them erased. Various parties contribute to the development and operation of the systems of a smart house: those creating and developing the respective technologies, those who help to implement the solutions and those who use the solutions in their real estate. All the aforementioned parties can potentially collect and use personal data either as a controller or a processor or in both roles. The main task and challenges arising from smart houses are establishing the roles, obligations and responsibilities of various parties within the context of data protection. This is crucial to duly comply with the data protection regulation and to prevent violations of rules of processing of personal data.

If the responsibility and obligations of different parties in the field of data protection are undefined and unclear for the parties themselves, there is a risk that the application of measures required in data processing and the performance of the respective obligations is inadequate. This may lead to the violation of personal privacy, insufficient protection against cyber-attacks and commencement of state supervision and offense proceedings. If the roles and responsibilities have been determined, the obligations must be clearly specified in contracts entered into between the corresponding parties. In addition, people must be properly notified of the processing of their personal data, and lawful consents related to data processing must be obtained from people if the consents are required. The providers of such systems and personal data processors must also be able to take relevant technical and organisational measures to ensure the level of security appropriate for the data.

It is recommended that the users of smart houses start with an inquiry to the manager or systems operator of the smart house concerning whether and which data are collected for users and how the security of data collected is ensured.

RAIMO KLESMENT
ASSOCIATE

(+372) 66 76 440
RAIMO.KLESMENT@NJORDLAW.EE