Video Surveillance Policy

EY Bulgaria

Building a better working world

Building a better working world

Contents

Building a better working world

1. Who is responsible for video surveillance

1.1. EY in Bulgaria is represented by three entities: Ernst & Young Bulgaria EOOD, Ernst & Young Audit OOD, Ernst & Young denktsatt EOOD, EY Regional Services EOOD and Ernst & Young Law Partnership, having its registered seat and address at Polygraphia Office Center, 47A, Tsarigradsko Shosse Blvd., floor 4, with one office located in Sofia, Bulgaria (jointly referred to as "EY Bulgaria").

1.2. Each of the five legal entities is a data controller and for the purposes of video surveillance, the three entities act as joint data controllers. Ernst & Young Bulgaria EOOD is the data controller, jointly appointed by all EY entities in Bulgaria, to have overall responsibility for the video surveillance in the offices.

1.3. Ernst & Young Bulgaria EOOD is responsible for receiving and responding to data subject requests and claims in relation to video surveillance and for providing concerned individuals with detailed information about personal data processing as required by the General Data Protection Regulation (GDPR) and the applicable Bulgarian legislation.

2. Physical security at EY offices

2.1. The physical security of the EY offices is of fundamental importance. EY relies on overlapping controls to provide a diversity of defense. That is, if one control, such as the biometric access control system fails or is compromised, an overlapping control, for example, CCTV is available to provide real-time and investigative controls.

2.2. The EY offices house both EY and client information (including personal data). This includes information that EY is under both contractual and legal responsibility to protect from disclosure. Protecting confidential information obtained from, or related to our clients or third parties, as well as personal information about our people, is one of EY's key values embedded in the EY's Global Code of Conduct.

2.3. The EY offices host a connection to the EY Global WAN and although a reasonable level of controls has been applied to network resources, one of the primary controls is segregation of physical access. Having physical access to the EY offices reduces the level of protection to both physical and network resources.

2.4. Finally, EY has a duty of care to protect the life and health of EY people and visitors who come to the EY offices. CCTV provides a critical portion of the overall security controls protecting the EY premises.

3. Objective of the video surveillance system

3.1. The objective of video surveillance is to ensure safety of the property, premises, employees and visitors of EY Bulgaria, and to protect the property, health and life of employees or visitors of EY Bulgaria. The data obtained through the video surveillance systems will be used only for these purposes.

3.2. EY Bulgaria uses CCTV cameras where it has a compelling legitimate interest which overrides the interests, rights and freedoms of the individual.

3.3. Cameras are a necessary component of the overall security controls in EY premises. In addition to the deterrent effect of having visible cameras covering key areas of EY premises, cameras allow EY to investigate past events and to validate current

conditions. However, CCTV-recorded video footage is reviewed only if the security of the EY's premises, assets, people and visitors could not reasonably be fulfilled by other means which are less intrusive to the privacy of the individuals who are being recorded.

3.4. Cameras are predominantly used to investigate incidents after they have been reported to office management or directly to security. Cameras allow the security team to positively identify who has entered the EY offices (e.g., when tailgating or otherwise not using valid access means to enter) and to better understand what was happening in the EY offices at the time of an incident.

3.5. Cameras allow EY investigators to identify the location of missing items, such as laptops and office equipment, verify the time of delivery (such as client files) and validate the functioning of other controls.

3.6. Cameras also function as a secondary security device, that is, cameras can be used to validate that no one entered an area if the primary access control system was down for a period of time or if a door was left unlocked or propped open outside of business hours.

4. Positioning of cameras

4.1. CCTV cameras at the EY offices are positioned and configured to capture and record usable and relevant video. The video surveillance devices are placed in the common use areas: entrances and exits from the premises of the office, reception hall, corridors and lounges. Cameras are carefully positioned to exclude the areas with heightened privacy expectations. Areas where EY people and visitors have a reasonable expectation of not being monitored (e.g., closed offices, conference rooms, leisure areas, toilet facilities, etc.) are not monitored by video surveillance cameras.

4.2. The purpose of installing cameras is not to monitor the work of EY people, working hours or tasks done, or to purposelessly collect private data. As far as possible, the cameras' field of vision excludes the areas of usual activity of the people, such as the working stations and desks. The goal is to monitor areas in which incidents jeopardizing the security of people, property and information are likely to occur.

5. Operation of cameras

5.1. Video surveillance operates twenty-four hours per day, seven days per week and stores all movements in the monitored areas.

5.2. In general, cameras in EY are not directly monitored by a dedicated guard. Life viewing of images is enabled at reception. The screen showing the images is placed in such a way so as not to be visible to unauthorized third parties passing nearby. Images may be viewed remotely, in a control room by authorized personnel only.

6. Notifying data subjects

6.1. Data subjects are notified about video surveillance by the respective signs placed in the area where video surveillance devices are installed. All EY employees are served privacy notices, which describe the details of processing their personal data, including through the video surveillance system.

7. Storage and disclosure of video data

7.1. The video data files are stored in the recording devices, which are located in the limited-access premises that are locked at all times and may be accessed only by the authorized personnel.

7.2. The video data is stored for twenty-one days from the day on which it was recorded. If necessary, images that may be used for investigation purposes or as evidence following a security incident may be retained for a longer period.

7.3. The video data might be disclosed to relevant state or municipal authorities (law enforcement authorities, courts) upon binding order or to such other third parties, which are appointed by EY Bulgaria to provide and maintain the video surveillance technology or otherwise process the data and who will be bound by strict confidentiality obligations by virtue of a data processing agreement. No surveillance data will be disclosed to any other third party.

8. Access to video data

8.1. The data from the video surveillance systems is used only by the authorized persons in the IT and Facility department, who need to access the information in order to perform their professional duties.

8.2. If necessary, the data might be made available to the Country Managing Partner or other members of the EY Bulgaria leadership, all of whom are bound by confidentiality obligation and understand that they might use the video data only in accordance with this policy.

8.3. The transmission of CCTV footage to third parties for a purpose other than the one for which the data has been collected, for example, to law enforcement agencies, is only allowed with the prior approval of the country Data Protection Officer (DPO). The country DPO shall assess whether EY Bulgaria is under a legal obligation to hand over the data and if no such legal obligation exists, whether EY is otherwise allowed to share CCTV footage outside the EY organization.

9. Data subject rights

9.1. All data subjects, including all EY employees, have the rights established by the General Data Protection Regulation (GDPR), the EY Binding Corporate Rules Policies (available at www.ey.com/bcr) and the Bulgarian Personal Data Protection Act.

9.2. To exercise their rights, the data subjects shall address their request to DPO@bg.ey.com. Any request received otherwise must be forwarded to the country DPO or the latter should otherwise be involved as soon as a request or a complaint from a data subject is received in relation to the video surveillance.

Right to access to footage data

9.3. An EY employee, client, supplier, visitor or passer-by who entered into the range of one or more cameras may exercise their right to view the images directly concerning them. However, this right must be strictly limited by the protection of personal data of third parties who also appear in these images. Therefore, if it is not possible to isolate the images in which the requestor alone appears, using standard means and

without a disproportionate investment, it might be impossible for EY to provide the images, for which the latter will be duly informed.

9.4. An access to a CCTV-footage request should, where possible, be in writing (for record-keeping purposes). The requestor must identify themselves with personal identification document or alternative identification proof.

Timeline

9.5. EY will respond to data subject requests within one month, with an additional two months permitted where there is a high level of complexity or numerous requests from the same individual. Where an extension is needed, the reasons for this will be communicated to the individual making the request within one month of receiving the request.

Protection of third parties' rights

9.6. EY will ensure that access, deletion or other rights exercised by an individual do not adversely affect the rights of others.

10. Complaints and appeals

10.1. Any complaints for violation of this policy or the law can be submitted to the EY data protection officer at DPO@bg.ey.com.

10.2. Everybody has the right to have recourse to the Bulgarian Data Protection Commission.

11. Final provisions

11.1. Upon adoption, this policy will be communicated to all employees and placed on the local server (BG Share) for continuous access by EY people. The policy is available in both Bulgarian and English version, online at: https://www.ey.com/en_bg/legal-and-privacy and in paper form – upon request at EY reception.

Date of last update: 29.07.2024