4.6 Data processing for security purposes: operation of entry control systems, camera systems, breathalyser test, baggage and cabinet control

Future Security Zrt. (registered seat: 1148 Budapest, Fogarasi út 5.; telephone number: (1) 267-6706; email address: mail@future-security.hu) provides personal security and property protection services to Egis in relation to Egis facilities. Services include reception (entry), guarding (breathalyser test and baggage/locker inspection) and technical on-call services (monitoring cameras, providing access to camera recordings). In doing so, it has access to the personal data of individuals for the purposes of the data processing for the following purposes.

Purpose of data processing	Legal basis of data processing	Scope of processed data	Data retention period, access rights, recipients of data transfers
1. Operating the entry control system: recording the times and places of entering and leaving the Egis headquarters, sites, branch, including the individual buildings by means of registered entry cards.	Article 6 (1) (f) of the GDPR – legitimate interest of Egis. Legitimate interest is the protection of the property of Egis and the protection of the life and bodily integrity of the persons staying in the premises of Egis in accordance with the provisions concerning the application of an electronic entry system under Section 32 (1) of Act CXXXIII of 2005 on Security Services, Property Protection and the Activities of Private Investigators ("**Property Protection Act**").	Relevant individuals: persons entering the registered seat, sites, branch of Egis. Scope of data in the case of single entries: movement data linked to the registered entry card, (date and place of entry/exit), name of the persons entering, presentation of an identification document with a photo for the verification of identity without recording any data. Scope of data in the case of regular card use: movement data associated with the registered entry card, (date and place of entry/exit), name of the persons entering, name of the organization unit where he/she performs work in the territory of Egis and the name of the company employing him/her. In the event of a security problem that may arise (e.g. theft, burglary),	**In the case of single entries** (by means of a guest card - the guest card is validated for one day, at 18:00 that day the card authorization expires) Egis deletes the movement data 24 hours after the departure. Egis keeps the data recorded upon entry for 1 month. **In the case of regular card use**, (any card that authorises access for a period longer than a given day, e.g. to external construction workers) Egis deletes the movement data after 6 months (Sections 32 (2)-(3) of the Property Protection Act or 24 hours after the card authorization expires. Egis deletes the name and card number recorded upon entry upon the expiry of 8 years after the card deposit fee

Purpose of data processing	Legal basis of data processing	Scope of processed data	Data retention period, access rights, recipients of data transfers
		Egis may inspect entries to offices and other premises. In addition, in the event of any emergency (e.g. fire alarm), Egis will also gather information through this on the actual location of persons who entered Egis' territory.	is refunded (Sections 168-169 of the Accounting Act). **Persons who have access within Egis:** In Budapest, the employees of the Security Department General, the competent officers of the property protection service provider and for operating purposes, the staff of the Automatization and Instrumentation Department General. At the Körmend branch of Egis, security technical officer of the Operational Security Group and the head of the Operational Security Group.
2. Operating an electronic surveillance system (cameras) for the protection of property and for the protection of life and bodily integrity. Data processing related to cameras is governed by a detailed Privacy Notice and rules of procedure: CEO's Order No 18/2016: Operation of the Security Camera System and Drug Technology	Under Section 30 (1)-(2) of the Property Protection Act the security guard may make and process video recordings through the operation of the electronic surveillance system within the scope of his/her agreement that specifies his/her obligations, in order to perform his/her obligations arising out of his/her agreement, enforcing data protection rights under the Act on the Right of Informational Self-determination and Freedom of	Relevant individuals: Recordings made of the persons entering the Egis headquarters, sites, branch and in the areas indicated in the separate notice, the conclusions that can be drawn from the recordings. Scope of data: video recordings of the electronic surveillance system, time of recording.	**If the recording is not used,** maximum 3 business days from the time when the recording is made, in the event of keeping hazardous substances, 30 days. **If the recording is used,** until the final and binding completion of the procedure related to the use. **Persons who have access within Egis:** Security Department General,

Purpose of data processing	Legal basis of data processing	Scope of processed data	Data retention period, access rights, recipients of data transfers
Camera System. Available at the reception of the Egis premises and in the guard's container.	Information in adherence to the restrictive provisions set out in the Property Protection Act. The security guard may use the electronic surveillance system only in private areas or in the public part of the private area, if the private individual explicitly consent thereto. The consent may be given by implicit action. Implicit action in particular means the case where the private individual staying in the public part of the private area enters the area despite the notice displayed there, unless clearly the contrary follows from the circumstances.		security technical on-call service of the security service provider, for operational purposes, the staff of the Automation and Instrumentation Department and employees authorized to have access under the Egis internal regulations, CEO's Order No 18/2016.
3. Operating a drug technology camera system to ensure the protection of consumers' life, bodily integrity and health. Data processing related to cameras is governed by a detailed Privacy Notice and rules of procedure: CEO's Directive No 18/2016: Operation of the Security Camera System and Drug Technology Camera System. Available at the reception of the Egis premises and in the guard's container.	Under Section 30 (1)-(2) of the Property Protection Act the security guard may make and process video recordings through the operation of the electronic surveillance system within the scope of his/her agreement that specifies his/her obligations, in order to perform his/her obligations arising out of his/her agreement, enforcing data protection rights under the Act on the Right of Informational Self-determination and Freedom of Information in adherence to the	Videos recorded by cameras, the time of recording and the conclusions that can be drawn from the recordings	Storage period of video recordings: maximum **2 years** from the recording. Generally, **2 years** is the period within which cases of mixing up medicinal products and complaints can be dealt with reasonably. The recordings (if any) confirm or refute the operating and other accompanying documentation generated in the case. **Persons who have access within Egis:** Security department general,

Purpose of data processing	Legal basis of data processing	Scope of processed data	Data retention period, access rights, recipients of data transfers
Egis has a legitimate interest in ensuring the protection of consumers' lives, bodily integrity and health in the context of a high-risk technological process or activity carried out in the monitored areas. It is indispensable to have a Drug Technological Camera System in place in order to comply with the rules on product liability of Act V of 2013 on the Civil Code (Sections 6:550-6:559), to detect any wrong data that may be generated in the quality assurance system operated by Egis and to comply with national and international pharmaceutical manufacturing regulations.	restrictive provisions set out in the Property Protection Act. The security guard may use the electronic surveillance system only in private areas or in the public part of the private area, if the private individual explicitly consent thereto. The consent may be given by implicit action. Implicit action in particular means the case where the private individual staying in the public part of the private area enters the area despite the notice displayed there, unless clearly the contrary follows from the circumstances.		security technical on-call service of the security service provider and employees authorized to have access under the Egis internal regulations, CEO's Order No 18/2016.
4. Conducting breathalyser tests for the protection of property and for the protection of life and bodily integrity. With regard to that checking whether the individual complies with Egis regulations on alcohol consumption. In a pharmaceutical/chemical environment, because of highly flammable and explosive materials and technological processes, anyone entering the Egis area under the influence of alcohol is a	Article 6 (1) (f) of the GDPR – legitimate interest of Egis. Legitimate interest: to protect the property of Egis and the life and bodily integrity of the persons staying in the territory of Egis. Article 6 (1) (c) of the GDPR: compliance with a legal obligation to which Egis is subject. In the case of health data (personal data related to the physical or mental health of an individual, including the provision of healthcare services to	Relevant individuals: persons entering the Egis headquarters, sites, branch, witnesses involved in the test and persons carrying out the test. Scope of data: name, date of birth, signature of the person subject to a breathalyser test, findings of breathalyser test, and, if so requested by the person tested, blood test result, names, registration numbers and signatures of assisting	Data retention period: 5 years from the issuance of the protocol (under Section 6:22 of Act V of 2013 on the Civil Code civil law claims lapse in 5 years). Then the data processed are deleted. The purpose of data retention is to make the documentation of cases with a positive breathalyser test available during the 5-year retention period, providing necessary information for official proceedings, lawsuits, etc. initiated as a follow-up to positive

Purpose of data processing	Legal basis of data processing	Scope of processed data	Data retention period, access rights, recipients of data transfers
particularly dangerous hazard, as such a person can suffer or cause an accident. In the territory of Egis there are sewage treatment and sedimentation technologies in operation which are also highly dangerous, especially for people under the influence of alcohol.	the individual): Article 9 (2) (b) of the GDPR: processing is necessary for the purpose of carrying out the obligations and exercising specific rights of Egis in the field of employment. Basis of the legal obligation: Section 2 (2) of Act XCIII of 1993 on Safety at Work. Egis, as an employer, is responsible towards its employees for meeting the requirements of working in a safe environment not hazardous to health and, with that in mind, it imposes safety measures on outsiders entering its territory. Pursuant to Article 9 (2) (f) of the GDPR, the processing of data of an individual concerning health may also be necessary for the establishment, exercise or defence of legal claims in connection with the test, either by Egis or by the data subject.	witnesses, name and signature of person carrying out the test.	breathalyser test. In the case of tests with negative results, the duration of data processing is 1 year from the issuance of the protocol. The purpose of data retention is to make the documentation of cases with a negative breathalyser test available during the 1-year retention period, providing necessary information for official proceedings, lawsuits, etc. initiated as a follow-up to negative breathalyser test. **Persons who have access within Egis:** In Budapest, the Security Department General, at the Körmend branch of Egis, Operational Security Group, assisting witnesses and specialised institutions that carry out the analysis of the blood alcohol test. In the case of a positive test result, the competent officer of the Legal Department General.
5. Baggage and cabinet inspection for the protection of property and for the protection of life and bodily integrity.	Sections 25 (2), 26 (1) b-c) and 28 (1) of the Property Protection Act. Accordingly, when guarding any non-public facility of Egis, the security guard is entitled to request	Relevant individuals: persons entering the Egis headquarters, sites, branch, witness involved in the inspection and persons carrying out the inspection.	Until the final and binding completion of the legal proceedings initiated as a result of the inspection (for example civil court proceedings, criminal

Purpose of data processing	Legal basis of data processing	Scope of processed data	Data retention period, access rights, recipients of data transfers
In a pharmaceutical/chemical environment, because of highly flammable and explosive materials and technological processes, anyone entering the Egis area with an instrument capable of causing accident in such an environment is a particularly dangerous hazard, as such a person can suffer or cause an accident. For example, in the territory of Egis there are sewage treatment and sedimentation technologies in operation which are also highly dangerous. In this environment it may be important to inspect the baggage carried by persons entering the premises or the cabinets used by them (that may contain their baggage) from the aspect of fire protection, prevention of accidents and safety at work.	any person entering or exiting the premises to present his/her baggage or delivery documents. The security guard is also entitled to request any person being on or exiting the premises to present the contents of his/her baggage, vehicle or freight consignment as set out below. The security guard may demand to see the contents of baggage, a vehicle, or a consignment with a view to discharging his/her contractual obligations regarding security, upon stating the reason and objective of the proposed action, if a) there are reasonable grounds to believe that the person is carrying on him/her any article obtained by a criminal act or misdemeanour and that article falls within the security guard's scope of contractual liability for safeguarding; b) the person fails to surrender this article when so instructed; and c) it is necessary for the prevention or stopping of the illegal conduct. In case of exercising the above rights, out of the means available for achieving the purpose, the least injury to personal freedom and personal rights shall be chosen.	Scope of data: the name, date of birth and signature of the person subject to the inspection, the findings of the inspection, the action taken based on the findings of the inspection, any comment(s) of the person concerned on the inspection and the action taken as a result, the name, registration number and signature of the assisting witness, the name of the inspector, his/her position, the name of the organizational unit in which he/she is employed and his/her signature, as well as the place and date of the protocol taken (including the conclusion therein).	proceedings. In the absence of such proceedings, 5 years from the issuance of the protocol. Under Section 6:22 and Section 6:533 (1) of the Civil Code claims lapse in 5 years. The rules on limitation are applicable to compensation with the deviation that in the case of damage caused by a criminal offense, the claim will not expire after 5 years until the criminal offense ceases to be punishable. Then the data processed are deleted. The purpose of data retention is to make the documentation of the inspection available during the data retention period, providing necessary information for official proceedings, lawsuits, etc. initiated as a follow-up to the inspection (if any). In the case of inspections with negative results, the duration of data processing is 1 year from the issuance of the protocol. The purpose of data retention is to make the documentation of cases with a negative result available during the 1-year retention period, providing necessary information for official proceedings, lawsuits,

Purpose of data processing	Legal basis of data processing	Scope of processed data	Data retention period, access rights, recipients of data transfers
	Article 6 (1) (c) of the GDPR: compliance with a legal obligation to which Egis is subject. Basis of the legal obligation: Section 2 (2) of Act XCIII of 1993 on Safety at Work. Egis, as an employer, is responsible towards its employees for meeting the requirements of working in a safe environment not hazardous to health and, with that in mind, it imposes safety measures on outsiders entering its territory. Article 6 (1) (f) of the GDPR – legitimate interest of Egis. Legitimate interest: to protect the property of Egis and the life and bodily integrity of the persons staying in the territory of Egis.		etc. initiated as a follow-up to the cases with a negative result. The processing of the data of the assisting witness recorded in the protocol is subject to the above retention periods. **Persons who have access within Egis:** In the Budapest premises of Egis, the Security Department General, the Operational Safety Group at its branch in Körmend, and at each place the competent officer of the security service provider, and if an inspection ends with a positive result (i.e. if there is a strong suspicion that the person in question keeps a thing with him/her that originates from a criminal offense or misdemeanour, but is the property of Egis or keeps a thing with him/her which endangers or threatens the life or physical integrity of others) a competent member of the Legal Department General.
6. Recording the data of van and truck drivers entering the Egis sites and branch for freight	Section 26 (1) a) of the Property Protection Act. Accordingly, when guarding any non-public facility of	**Relevant individuals:** data of drivers entering the Egis headquarters, sites, branch	1 year from the recording of the data.

Purpose of data processing	Legal basis of data processing	Scope of processed data	Data retention period, access rights, recipients of data transfers
transport.	Egis, the security guard is entitled to request any person entering or exiting the premises to verify his/her identity, to give the purpose of his/her entry or stay and verify his/her authorisation. Article 6 (1) (b) of the GDPR – performance of the agreement Article 6 (1) (f) of the GDPR – legitimate interest of Egis. Legitimate interest: it is necessary to record the data of carriers with regard to the value of a shipment in the event of the protection of the property of Egis and transportation of highly valuable shipments of medicinal products, pharmaceutical raw materials.	employed by a company that carries out freight transport for Egis on the basis of an agreement. Scope of data: name of the driver and the type and number of his/her identification document.	In the case of a crime that can be related to transportation, the period is usually 1 year, during which the investigating authority may request information from Egis. **Persons who have access within Egis:** In the Budapest premises of Egis the employees of the Security Department General, the competent officers of the security service provider, at the Körmend branch of Egis, the Operational Security Group, and at each place the competent staff member of the security service provider.