Balancing test

for data processing associated with the use of the camera system (electronic surveillance system)
Plazmaszolgálat Kft.
(2045 Törökbálint, Torbágy utca 15/A.)

Plazmaszolgálat Kft. (hereinafter referred to as the data controller) operates an electronic surveillance system at its registered office, premises and centres.

No.	Name of site	Premises address
1.	Plazma Pont (SZM)	20–22 Mikszáth Kálmán Street, 6722 Szeged
2.	Plazma Pont (SZK)	6720 Szeged, Kígyó Street 4.
3.	Plazma Pont (BK)	1082 Budapest, Kisfaludy Street 38, 4th floor
4	Plazma Pont (BC)	1093 Budapest, Czuczor Street 10, 3rd floor
5	Plazma Pont (BÖ)	1106 Budapest, Örs vezér tere 25/B, 3rd floor
6	Plazma Pont (D)	4025 Debrecen, Széchenyi utca 31.
7	Plazma Pont (SZJ)	8000 Székesfehérvár, Jancsár köz 5.
8	Plazma Pont (K)	7400 Kaposvár, Áchim András utca 2.
9	Plazma Pont (GY)	9021 Győr, 36 Bajcsy-Zsilinszky Road
10.	Plazma Pont (SK)	9700 Szombathely, Körmendi út 11.
11.	Plazma Pont (S)	9400 Sopron, Határdomb u. 1–2.
12	Plazma Pont (BB)	1112 Budapest, Boldizsár utca 2.

In designing and operating the CCTV system, the data controller has taken into account Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation, hereinafter: GDPR), Act CXII of 2011 on the right to self-determination in relation to information and freedom of information (hereinafter: Infotv.), as well as Act CXXXIII of 2005 on the rules governing personal and property protection and private investigation activities, and Act I of 2012 on the Labour Code.

The purpose of this document is to define the framework for data processing, to inform data subjects and to carry out a balancing of interests to ensure that data processing is carried out in accordance with the law, taking into account and respecting the data subjects' rights to privacy.

With this document, the data controller informs data subjects about the data processing associated with the use of the CCTV system, its regulation and practical implementation. This information notice and the balancing of interests test are available on the website of Plazmaszolgálat Kft., at the data controller's premises, and in paper form at the data controller's entrance.

The data controller has displayed a brief notice regarding the use of the electronic surveillance system in a clearly visible manner at the entrances. The data controller has placed warning signs (pictograms) at the entrance to the data controller's premises indicating that an electronic surveillance system is in use in that area.

In this notice and in the balancing of interests test, the Data Controller sets out the rules governing data processing and provides information on its data processing activities relating to camera surveillance based on legitimate interests.

1. Data

Controller:

Plazmaszolgálat Kft.
Data Controller: Plazmaszolgálat Limited Liability Company
Registered office: 2045 Törökbálint, Torbágy utca 15/A Company
registration number: 13-09-121293
Tax number: 14380817-2-13
Email: aktualis@plazmaszolgalat.hu
Data Protection Officer: Dr Zsombor Sümegi (gdpr@gdprtanacsadas.eu)

2. Legal basis for data processing

The Data Controller processes personal data on the basis of Article 6(1)(f) of the GDPR; the Data Controller processes data to protect the physical integrity of donors, prospective donors, visitors and employees, the Data Controller's assets, and the physical integrity of donors, prospective donors, visitors and employees, the investigation of accidents and for quality assurance purposes relating to the service. The Data Controller has carried out a balancing test to assess the legal basis.

In the course of data processing, the Data Controller is obliged to comply with the provisions of the following laws:

- Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR) Act I of 2012 on the Labour Code (hereinafter 'Mt.')
- Act CXII of 2011 on the Right to Self-Determination in Information and Freedom of Information
- Act CXXXIII of 2005 on the rules governing personal and property protection and private investigation activities
- Act I of 2012 on the Labour Code
- the National Authority for Data Protection and Freedom of Information's guidance on the basic requirements for data processing in the workplace
- the recommendation of the National Authority for Data Protection and Freedom of Information on the basic requirements for electronic surveillance systems used in the workplace

3. Scope of data processed, purpose of data processing, monitored area, duration

Scope of data processed by the data controller:
The image of any person entering the monitored area (employee, donor, prospective donor, visitor), their activities and movements as visible on the recording. The camera system records the date and exact time the recording was made, as well as the name and number of the camera that made the recording, or the camera's name. The data is recorded in the data processing
. The cameras do not record audio.

Purpose of data processing:
The protection of property, the protection of the life and physical integrity of donors, prospective donors, visitors and employees, and the protection of the data controller's property.
In this context, data processing serves the following specific purposes:

- the protection of persons, life and physical integrity, and the protection of donors, prospective donors, visitors and employees;
- detection and evidence of infringements in order to protect machinery, tools and equipment of significant value;
- prevention, detection and subsequent evidence of infringements, damage, theft and other property offences
- preventing, interrupting and subsequently proving unlawful acts

- furthermore, to ensure that, in this context, the recordings are used as evidence in court or other official proceedings.

The legitimate aim of protecting persons and property cannot be achieved by a solution that does not require the recording of other personal data.
Man-to-man security cannot be implemented cost-effectively in the area due to the size of the data controller's premises and the fragmented nature of the site.

Area under surveillance:
A camera system is necessary to achieve the objective of personal and property protection. The electronic surveillance system monitors the locations specified in the camera appendix, typically the entry points to the site, the internal and external areas of donor, prospective donor and visitor zones, and the areas necessary for operations that are restricted to donors, prospective donors and visitors. The purpose of the placement of the cameras and the monitoring is not to monitor employees, donors, prospective donors or visitors, nor is it for the data controller to draw any conclusions from the behaviour of employees, donors, prospective donors or visitors.
A record of the camera locations and the relevant policy can be requested from the data controller at the entrance. The camera locations are set out in the camera appendix.
The head of the data controller decides on the placement and relocation of the cameras.

Duration of data processing:
The method of camera surveillance is recorded and live. The data controller retains the footage for 14 days. This period is necessary to enable the detection of property offences, administrative offences and legal violations. The recordings are stored for 14 days and then deleted, unless it becomes apparent during the 14-day period that the data recorded on the footage is necessary for the enforcement of the data controller's own or another legitimate interest.
In the event of a suspected criminal offence or administrative offence, the recordings are saved and handed over by the data controller to the law enforcement or administrative offence authority.
The camera system is configured so that, after 14 days, the system automatically overwrites recordings older than 14 days, meaning that recordings older than 14 days are deleted. Deleted recordings cannot be recovered.

4. Rules regarding the review of recordings, and provisions regarding the purposes for which the data controller may use the recordings:

The method of camera surveillance is recorded and live. The recordings are monitored by the data controller on an ad hoc basis; recording takes place 24 hours a day. Authorised employees of the data controller monitor the live feed where justified.
There are no cameras installed in the toilets or changing rooms. The cameras monitor private areas only, not public areas.
Recorded footage may be reviewed by the data controller if there is suspicion of an accident, personal injury, criminal offence, administrative offence or other legal violation.

Rules for reviewing and viewing recordings:
At the data controller's premises, camera footage may only be viewed and reviewed by the centre manager and employees authorised by the data controller (IT manager).
The person reviewing the camera footage logs into the platform enabling the viewing of the recorded footage using a password; the person accessing the data can be identified later, as the system logs their access code, the fact of access, the time and duration of access.
In the event of an incident, the person reviewing the camera footage must record a report in the camera log, noting the reviewer's name, the fact that the footage was reviewed, the location, time and reason for the review, as well as a description of the incident visible in the footage. The viewing of stored footage must be documented. The footage may only be viewed and reviewed by a restricted group of individuals.

Rules for retrieving recordings:
In the event of an accident, personal injury, criminal offence, administrative offence, suspicion of other legal violations, or at the request of an authorised party, the recordings (still images or moving images) shall be saved. The system shall log this. The data controller shall hand over the saved recordings to the law enforcement or administrative offence authority; in the case of a donor, prospective donor or visitor's complaint, or at the request of the data subject, the data controller shall provide the donor, prospective donor or visitor with the opportunity to view the recording.
If the recording is handed over or viewed, the data controller shall blur the faces of all persons appearing in the recording in advance so that the persons in the recording cannot be recognised.
The data controller shall save the extracted recording to a separate data storage medium.
If an unlawful act is detected, the data controller shall retrieve the recording and inform the authority that a video recording of the act has been made. The data controller shall record the retrieval of the recording in the camera log (see the section 'Rules on retrieving and viewing recordings' above).
The data controller keeps a record of data disclosure.
The retrieval and redaction of data are carried out by a company employee.

Rules for the retention of recordings:
If the recordings are not viewed or requested by:

- are not viewed or requested by a donor, prospective donor, visitor or employee,
- or no official proceedings are initiated in the

matter, the recordings will be deleted after 30 days.
In other cases, upon specific request, the data controller shall retain the recordings until a specified deadline (until a specific date or until the records are handed over in response to a request made in connection with official proceedings).

5. Balancing of interests test

When assessing the justification for data processing based on legitimate interest, the company balances its legitimate interest against the interests of the data subjects and, on this basis, determines whether there is a legal basis for data processing based on legitimate interest:

5.1 Step 1: Is CCTV surveillance absolutely necessary to achieve the purpose of the data processing? Justification of the necessity of using the CCTV system.

In their day-to-day work, employees handle equipment and materials that pose high accident and health risks; traceability is of paramount importance due to health and production regulations, so strict rules apply to work activities. An important part of process development is the quality control of individual work processes, as well as long-term traceability and the investigation of questionable procedures. It is not sufficient to define the procedures for each operation before the activity begins; these must also be measured, and compliance with quality and safety requirements must be verified. It would in itself entail disproportionately high costs if we were to employ an inspector for the review of every single work process, who would accompany the operation in question throughout, verify its implementation criteria, and ensure that employees were under constant supervision with regard to quality, accident and disaster prevention, and external parties in terms of property, accident and life protection. Due to the size of the monitored area and the large number of people entering and leaving, employees are unable to carry out the monitoring and supervision of the area. The size of the area would necessitate the employment of more security guards and quality assurance specialists. Even the employment of security guards and quality assurance specialists would not make protection more effective, as they can only monitor a limited area. The legitimate aim to be achieved by the data controller—namely, the protection against accidents, quality control, and the protection of life, persons and property—cannot be achieved cost-effectively by any solution other than the electronic camera system that does not require the recording of personal data.
A further purpose of the surveillance is to monitor the protection of the large number of donors, prospective donors and visitors to the centres against accidents
, life and property, as well as to monitor the appropriate level of service provided to them, which would not be feasible without the use of the surveillance system.

5.2 Step: Determining the data controller's legitimate interest and the purpose of data processing

The data controller's interests include accident, quality, life, personal and property protection; the apprehension of offenders; the prevention and subsequent proof of infringements; and the effective handling of complaints and quality discrepancies. The
camera system assists in achieving this objective.

5.3 Circumstances of data processing

The data controller has established the rules for data processing in accordance with the applicable legislation and has set them out in this policy and information notice.
The data controller retains the recorded footage for 14 days, after which the recordings are deleted. The data controller will retain the recorded footage for a longer period only if this is necessary to safeguard the legitimate interests of the data subject or another person.

5.4 Assessment of the interests of data subjects

The data controller processes the personal data (image) of donors, prospective donors, visitors and employees. On the part of the data subject, issues may arise concerning the right to privacy and its infringement, as well as rights falling within the scope of human dignity, such as the freedom of self-determination or the right to physical and personal integrity and its infringement. Risks may arise from the implementation of data security requirements, data protection, the duration of data processing, and the group of persons with access to the data.
The scope of data processing and the field of view of the cameras may pose a risk.

5.5 Why is the restriction of the data subjects' rights considered proportionate?

To date (including the period since the cameras were installed), no complaints have been received from employees, donors, prospective donors or visitors regarding data protection issues.

The cameras' field of view is directed at the assets to be protected and the areas where people move. Donors, prospective donors, visitors and employees are aware of the cameras' locations. The cameras record the movements of donors, prospective donors, visitors and employees, but the data controller does not use the recordings to monitor employees, nor does it identify behavioural patterns relating to the behaviour of employees, donors, prospective donors or visitors. The monitoring of employees is governed by Section 9 of the Labour Code.
in accordance with the provisions of Sections 10 and 11. The management and protection of recordings ensure that recordings made of donors, prospective donors, visitors and employees may only be used in accordance with the provisions of the GDPR, in the interests of the data controller, the data subject or other legitimate interests. The data controller implements data security measures and protects the data from damage and unauthorised access.
Access to the CCTV recordings is restricted to a very limited group of individuals. Even these individuals may only view the recordings where justified. Any use of the data for purposes other than those specified is prohibited.

Data subjects are informed in advance by the data controller about the data processing; warning signs have been placed on the premises of the data controller and the institution.

The processing of data is strictly necessary and proportionate for the purposes of accident prevention, quality control, and the protection of life, persons and property. The use of cameras may contribute to the personal safety of donors, prospective donors, visitors and employees, as well as to accident prevention, quality control, and the protection of life, persons and property; it may also facilitate the subsequent investigation of infringements and accidents.
The camera system does not use new technology. No special protection applies to the data to be processed. The data processing is not excessive or inappropriate. The data subject cannot influence the data processing activity.

5.6 Outcome of the assessment: Data processing restricts the rights of data subjects to a limited extent; data processing is necessary and proportionate; the legal basis for data processing can be established.

6. Data transfer

The Data Controller transfers data to public authorities solely in accordance with legal provisions and does not transfer data to any other third parties. The Data Controller discloses data at the request of a court, the police or a public authority if required to do so by law.

7. Data security measures:

Location of storage of the recording:

The Data Controller processes data in such a way as to ensure the protection of the data subjects' privacy. The data controller protects the data using information technology solutions, in particular against unauthorised access, alteration, transmission, disclosure, erasure or destruction, as well as accidental destruction and damage, and against becoming inaccessible due to changes in the technology used.

Data security measures relating to the storage of recordings:
Recordings may be viewed online by authorised employees upon entering a password. The system logs access attempts. (see Section 4)

Recordings may only be reviewed for the purpose of detecting or proving accidents or unlawful acts, or for quality assurance purposes.
Access to the video recordings is restricted to a limited group of persons, who must enter a password; the person accessing the data can be identified. The system logs the viewing and saving of video recordings, and a record must be kept of these actions. The rules governing the viewing and saving of recordings are set out in Section 4. Saved recordings are stored on a separate data storage medium. The data controller keeps a record of data provision.

Employees with access to the data are trained by the data controller on data security and on how to handle the data.

We engage data processors in the operation of the cameras, subject to the safeguards set out in the data processing agreement required by Article 28 of the GDPR. You can find out about our data processors through our company's data processing register, using the contact details provided in Section 1.

8. Rights of the data subject, remedies Right of

access:
The data subject may request that the Data Controller provide information regarding the processing of their personal data; they have the right of access to their data, which also means that they may request a copy of their data. The Data Controller is obliged to comply with this request in such a way that no other person is recognisable in the recording.

No other person may appear on the copy provided; it must show only the person whose data has been processed. Other persons appearing in the recording must be obscured so that they are not recognisable.
Any person whose rights or legitimate interests are affected by the recording of the image or other personal data may, within seven days of the recording of the image or other personal data, request, by providing evidence of their rights or legitimate interests, that the data controller does not destroy or delete the data.

Right to rectification:
The data subject may request the rectification of their personal data (right to rectification), which means that the data subject is entitled to have inaccurate data concerning them rectified at the request of the data controller.

Right to restriction of processing:
The data subject may request the restriction of the processing of data relating to them (right to restriction) if they contest the accuracy of the processing, object to the erasure of the data in the event of unlawful processing, the data controller no longer needs the data but the data subject requires it for the establishment, exercise or defence of legal claims, or the data subject has exercised their right to object to the processing. The Data Controller shall inform the Data Subject in advance of the lifting of the restriction. The Data Controller shall inform all recipients to whom the personal data has been disclosed of the restriction.

Right to object:
The Data Subject has the right to object at any time to the processing of data on grounds relating to their particular situation, where such processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Data Controller, or where the legal basis for the processing is the legitimate interests of the Data Controller or a third party.

Right to erasure ("right to be forgotten"):
The Data Subject has the right to request that the Data Controller erase personal data concerning them without undue delay. In the event of a request for erasure, the Data Controller will examine the precise legal basis for the data processing and, if the conditions for erasure are met, will erase the data. In the event of erasure, the Data Controller shall ensure that all parties to whom the data has been disclosed through the Data Controller also erase the data. If the legal basis for the data processing is compliance with a legal obligation, the performance of a contract, or the Data Controller's legitimate interests, the Data Controller shall refuse the erasure.

The Data Controller shall provide the requested information in writing at the data subject's request within the shortest possible time (without undue delay) from the submission of the request, but no later than 30 days. In the event of rectification, the Data Controller shall inform all recipients to whom the data has been disclosed.

The data subject may request information regarding their data, or the rectification or restriction thereof, via the contact details of the Data Controller specified in point 1.

Should the data subject wish to lodge a complaint, they may do so with the National Authority for Data Protection and Freedom of Information (Budapest, Falk Miksa u. 9-11, 1055, postal address: 1530 Budapest, PO Box 5, www.naih.hu, telephone: +36 (1)
391-1400, fax: +36 (1) 391-1410,ugyfelszolgalat@naih.hu), or, at their discretion, to the court with jurisdiction over the Data Controller's registered office, the data subject's place of residence or place of stay.

Törökbálint, 13 October 2025.