

Privacy Policy
on the camera surveillance performed by MÁV-START Zrt.

1. The identity and contact details of the data controller

Name: MÁV-START Vasúti Személyszállító Zártkörűen Működő
Részvénytársaság
Headquarters: 1087 Budapest, Könyves Kálmán krt. 54-60.
Company reg. no.: 01-10-045551
Tax number: 13834492-2-44
E-mail: kamerainfo@mav-start.hu
hereinafter: Data Controller.

Contact details of the Data Protection Officer:

E-mail: adatvedelem@mav-start.hu
Postal address: 1087 Budapest, Könyves Kálmán krt. 54-60. – please mark the following on the envelope: „for the Data Protection Officer”.

2. The identity and contact details of the data processor

Name: MÁV Szolgáltató Központ Zártkörűen Működő Részvénytársaság
Headquarters: 1087 Budapest, Könyves Kálmán körút 54-60.
Company reg. no.: Cg. 01-10-045838
Tax number: 14130179-2-44
E-mail: helpdesk@mav-szk.hu
hereinafter: Data Processor.

Based on the contract the Data Processor provides a full IT service for the Data Controller, which includes the operation of communication applications (e.g. mail system and other registration systems) as well as the server services of computer equipment.

3. The data subject: the natural person whose image is recorded by the Camera Surveillance and Recording System (hereinafter: camera system) and image and voice by body cameras (hereinafter: data subject).

4. Information about the „Data processing”

Camera surveillance by the Data Controller as data processing:

Brief description of the data processing: the Data Controller shall carry out camera surveillance in the territory owned or lawfully used for the purpose indicated below, in particular in the place open to public traffic and in the vehicles used for the purpose of passenger transport services [Section 8 (5) of the PTS Act]. As part of this, the Data Controller shall record video recordings by surveillance cameras deployed in the areas under its management, by on-board cameras in its vehicles and shall record video and audio recordings by body cameras attached to the data controller's employee clothes, if necessary to achieve the purposes specified by law and below [Section 8 (3) of the PTS Act]. When recording by the body camera, the Data Controller ensures that the wearer of the body camera can start or stop recording. During the recording, the events occurring 30 seconds before the start of the factual recording shall be stored in a manner appropriate to the data processing purposes specified below, in particular for the investigation the damages to life, integrity, person and property of the employee or agent wearing the camera and detection of an infringement against them. The body camera provides sound-based information about starting and ending the recording, and indicates the recording with a light.

Purpose of the data processing: detection of accidents and damages affecting the data controller's property (vehicle, equipment and other property), life, person, physical integrity and property (eg luggage) of the service provider's employees, agents and passengers, as well as national property, and investigation and proof of the infringements against them, as well as the investigation of complaints made by passengers regarding the service of the Data Controller.

Legal basis of the data processing: according to the point (e) of the Article 6(1) of the GDPR, data processing is necessary for the performance of a task in the public interest, which is authorized by the 8.§ of PTS Act.

Categories of the personal data: in the case of recordings made by on board cameras an image of the data subject and in the case of recordings made by body cameras an image and voice of the subject.

Period of the data processing:

- a) the storage period of the image and voice recorded by the body camera before the factual recording and storage of the recording shall be 30 seconds, which shall be deleted at the same intervals, unless the data controller employee starts the factual recording and storage.
- b) Pursuant to Section 8 (9) of the PTS Act, the recording will be cancelled (erased) on the 16th day after the camera recording, in the absence of a request for preservation. If the recording is necessary for the conduct of an investigation initiated by the Data Controller or an authority or court, the camera recording – in accordance with Section 8 (15) of the PTS Act – shall be deleted on the 15th day following the date on which the decision taken in the proceedings becomes final.

Method of the data processing: electronically.

Persons entitled to access the data: in the event of accidents and injuries, the persons conducting an internal investigation by the Security Directorate of MÁV-START Zrt. and the investigation of the received passenger complaint in the given area.

Recipients of the data: pursuant to Section 8 (11) and Section 8/A of the PTS Act. the Data Controller shall forward the camera recording – in order to fulfil official requests received – to an authority, court or other public authority for the purpose of adjudicating the individual case.

The Data Controller shall transmit the camera recording to the railway infrastructure manager for the purpose of investigating the accident in the event of a railway accident involving the railway vehicle, if the accident also affects the railway infrastructure manager.

5. Information on data security measures

- The Data Controller, with the assistance of the Data Processors, shall take the technical and organizational measures:
 - (a) which are necessary for the operation of the electronic systems in accordance with the IT Security Code (ITSC) and operate in accordance with the internal instructions;
 - (b) ensuring that authorized users access the systems, its functions and data in accordance with their level of authorization;
 - (c) to ensure archivation of the data.
- The Data Controller shall comply with the procedural rules necessary to enforce the provisions of the legislation on data processing specified in Section 7. The Data Controller also expects the Data Processors to comply with these laws on the basis of the data processing contract concluded between them pursuant to Article 28 (3) of the GDPR.
- The Data Controller shall subject the electronically processed data files to virus scanning;
- The data controller shall ensure the protection of the security of data processing with technical and organizational measures that provide a level of protection appropriate to the risks related to the data processing, select the IT tools used and operate in such a way that the processed data:

- (a) be accessible to those entitled to it (availability);
- (b) its authenticity and authentication are ensured (authenticity of data processing);
- (c) its integrity must be verifiable (data integrity);
- (d) be accessible only to the rightholder and be protected against unauthorized access (data confidentiality).

6. Rights of the data subject and method of enforcement

6.1. The right to be informed

The data subject may request information from the Data Controller, request the correction of his or her personal data and restrictions on data processing. Upon request, the Data Controller shall provide information on the personal data processed by the Data Controller, the purpose, legal basis, duration of the data processing, the name, address (headquarters) of the data Controller or the Data Processor and the activities related to data processing, about who and for what purpose will receive or have received the personal data of the data subject and the rights in relation to the processing. The Data Controller shall provide the information in writing in a comprehensible form as soon as possible after the receipt of the request, but not later than within one month. If necessary, taking into account the complexity of the application and the number of applications, this period may be extended by a further two months. If the request for information is unfounded or, in particular due to its repetitive or excessive nature, the Data Controller may refuse to act on the request. The Data Controller may refuse to comply with a request to exercise the data subject's rights until the Data Controller can not identify the data subject beyond doubt.

6.2. Right of access

The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

- the purposes of the processing;
- the categories of personal data;
- where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
- the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- the rights of the data subject;
- the right to lodge a complaint with a supervisory authority;

At the request of the data subject, the Data Controller shall provide a copy of the personal data subject to data processing, provided that this does not adversely affect the rights and freedoms of others. The Data Controller may charge a fee for any additional copies requested by the data subject.

The exercise of the right of access does not include the case of the request for recording provided for in Section 8 (10) of the PTS Act, when a person who is not considered as data subject submits a request to the Data Controller not to delete the camera recording. In this case, the person requesting the camera recording must prove a legitimate interest which is the basis for not deleting a camera recording. The Data Controller shall assess the existence of a legitimate interest on a case-by-case basis and, if it considers that the person requesting the camera recording has a legitimate interest, shall, in accordance with Article 6 (1) (f) GDPR, forward the recording to the person requesting the camera recording, or waive the cancellation of the camera recording pursuant to Section 8 (10) of the PTS Act.

6.3. Right to rectification

The data subject may request the amendment (correction) of inaccurate personal data concerning him or her or may request the addition of incomplete personal data through the contact details provided in point no. 1. The Data Controller shall notify the data subject of the rectification. The Data Controller shall refrain from notification if this does not harm the legitimate interests of the data subject with regard to the purposes of the data processing.

6.4. Right to erasure ('right to be forgotten')

The data subject may request the deletion of his or her personal data if the purpose of the processing has ceased, if the data subject withdraws his or her consent, if the processing of the data is unlawful, if the specified retention period has expired and if the deletion has been ordered by a court or authority. The data controller shall notify the data subject of the deletion of the personal data. It shall refrain from notification if this does not harm the legitimate interests of the data subject with regard to the purposes of the data process. The Data Controller shall not delete personal data if they are necessary for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or for the establishment, exercise or defence of legal claims.

6.5. Right to restriction of processing

The data subject may request at any contact of the Data Controller that the Data Controller restrict the processing of his/her personal data on the camera recordings - e.g. may request that the camera recording not be cancelled after the expiry of the period specified in Section 8 (9) of the PTS Act - if:

- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

The restriction shall last as long as the reason given by the data subject requires. In this case, the camera recording shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State. The Data Controller shall not delete the camera recording for as long as the reason indicated by the data subject's request, but for no longer than six months. The Data Controller shall inform the data subject in advance of the lifting of the restriction at the request of the data subject.

6.6. Right to object

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, which is based on point (e) of Article 6(1). In this case, the controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims. If the data subject objects to the camera surveillance, the Data Controller shall examine the feasibility of the request on a case-by-case basis.

6.7. Remedies

In case of violation of the rights of the data subject or if the data subject does not agree with the Data Controller's decision, the data subject can file a complaint at the following contacts of the Hungarian National Authority for Data Protection and Freedom of Information

Name: Hungarian National Authority for Data Protection and Freedom of Information
Headquarters: 1055 Budapest, Falk Miksa utca 9-11.
Postal Address: 1363 Budapest, Pf. 9.
Telephone no.: +36 (1) 391-1400 / +36 (30) 683-5969 / +36 (30) 549-6838
Telefax: +36 (1) 391-1410
E-mail: ugyfelszolgalat@naih.hu
Website: <https://naih.hu/about-the-authority>

In the event of a breach of your rights, or if you do not agree with the Data Controller's decision, you may, within 30 days of being notified, bring a direct action against the Data Controller in the court of the Data Controller's domicile.

If you require further information in addition to that contained in this Privacy Policy, you may request information through the contact details provided in Section 1. If the data subject has any remarks or objections regarding the processing of his/her personal data, or would like to request information on the processing of his/her data, he/she can do so by e-mailing the Data Protection officer at adatvedelem@mav-start.hu. If you would like to find out more about the rights of the data subjects provided by MÁV-START Zrt., and about how to exercise the rights of the data subjects please visit the website: <https://www.mavcsoport.hu/en/mav-start/introduction/rights-data-subject-and-their-enforcement>.

7. Legislation applied in connection with data processing

- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation or GDPR);
- Act CXII of 2011 on Informational Self-Determination and Freedom of Information ("Privacy Act");
- Act XLI of 2012 on passenger transport services (PTS Act).

Budapest, 13 January 2022.

MÁV-START Zrt.
Data Controller