# Helsinki Regional Transport Authority

# Data Protection Policy

17 April 2018

Version 1.1

Contents

## 1 PURPOSE AND BACKGROUND

This Data Protection Policy contains descriptions of the objectives, responsibilities and policies for data protection at HSL. HSL acknowledges the importance of protecting the data and privacy of data subjects as part of its operations and commits to ensure data protection in the manner described in this Data Protection Policy. Data protection forms a part of operational compliance, information security and risk management.

The key elements of data protection culture at HSL are defining and documenting the objectives and concept of data protection and the policies for data protection work, as well as communicating them to HSL's employees. This Data Protection Policy document and the specific instructions based on it are used to communicate the data protection principles of HSL to its employees and partners. High-quality information security work also plays a part in the achievement of the objectives set for data protection. HSL Information Security Policy defines the principles of information security and information security work.

## 2 APPLICABLE LAW AND DEFINITIONS

### 2.1 Legislation

Data protection and the processing of personal data are governed by the EU's General Data Protection Regulation (2016/679), the Finnish acts and decrees on personal data, and other applicable special provisions. Furthermore, data protection work at HSL is guided by the charter, strategy, administrative regulations and internal guidelines of HSL, and with regard to information security, the HSL Information Security Policy, the ISO/IEC standards 27001 and 27002, and the best practices of the sector.

The provisions on publicity and protection of privacy in administration of the Constitution of Finland are observed in all HSL operations. These basic rights are coordinated by HSL in accordance with the law.

### 2.2 Definitions

The definitions of the EU's General Data Protection Regulation are used in this Data Protection Policy as follows.

**Personal data** means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Processing** means any operation or set of operations which is performed on personal data or on sets of personal data, whether by automated means or manually, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**Processor** means a natural or legal person, public authority, agency or other body, which processes personal data on behalf of the controller.

**Data file** means any structured set of personal data, accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis.

**Controller** means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

**Consent of the data subject** means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

**Personal data breach** means a breach of information security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

**Profiling** means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

## 3 DATA PROTECTION PRINCIPLES

The processing of personal data is guided by the principles set out in the provisions of the EU's General Data Protection Regulation so as to ensure the fulfilment of the Regulation's requirements and safeguard the rights of the data subject. All the principles listed below must be observed when processing personal data. Data protection principles must be observed throughout the entire lifecycle of the processing of personal data.

### 3.1 Lawfulness, fairness and transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject. The means in which personal data is collected and processed shall be communicated to the data subjects. The information and any communications relating to the processing shall be provided in an intelligible and easily accessible form. Data subjects shall be provided with the identity of the controller and the purposes of the processing. The controller must be able to provide the data subjects with information on the processing of their personal data and the means that the controller uses to ensure fair and transparent processing.

### 3.2 Purpose limitation

Personal data shall be collected for specified, explicit and legitimate purposes. The collected data shall not be further processed in a way incompatible with those purposes.

Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) of the EU's General Data Protection Regulation, not be considered to be incompatible with the initial purposes.

### 3.3 Data minimization

Personal data shall be appropriate, relevant, adequate and limited to what is necessary in relation to the purposes for which they are processed. Personal data shall be stored for as short a period as possible. Personal data should only be processed if the purpose of processing cannot be reasonably achieved by some other means. The controller must set time limits for the erasure of personal data. If exact time limits cannot be set, the controller shall set criteria on how to determine time limits for the erasure of personal data.

### 3.4 Accuracy of data

Personal data shall be accurate and, where necessary, kept up to date; the controller shall take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay, for example, after the appeal period has ended. The data subject shall have the right to have incomplete personal data completed, for example, by means of providing a supplementary statement.

### 3.5 Storage limitation

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Notwithstanding this, personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

### 3.6 Integrity and confidentiality

Personal data shall be processed in a manner that ensures appropriate security of the personal data, i.e., the integrity, confidentiality and availability of the data. Personal data shall be protected against unauthorized or unlawful processing and against accidental loss, destruction or damage.

### 3.7 Accountability of the controller

Accountability means that the controller must be able to demonstrate to the data subjects and data protection authorities that processing is performed in accordance with data protection principles. The means of demonstrating compliance include the preparation of privacy statements, the provision of information to data subjects, and the use of carefully documented processes and the organization’s internal instructions when processing personal data. The controller shall regularly assess adherence to data protection principles in its operations.

## 4 DATA PROTECTION MANAGEMENT MODEL

According to the Administrative Regulations of HSL, the Executive Board is responsible for data protection at HSL and appointing the Data Protection Officer of HSL. The Data Protection Officer is responsible for the tasks defined in the General Data Protection Regulation and in the data protection management model.

The data protection tasks and responsibilities of HSL are defined in the data protection management model in accordance with the Administrative Regulations and Data Protection Policy. The data protection management model of HSL is approved by the Executive Director of HSL.

The directors of the departments are responsible for ensuring that data protection is implemented in accordance with the Data Protection Policy, including any outsourced personal data processing services. The outsourcing of personal data processing is always subject to a written agreement in which the parties agree on the responsibilities and obligations relating to the processing of personal data in accordance with what has been specified in the EU's General Data Protection Regulation. Department directors are responsible for carrying out data protection impact assessments on the processing of personal data. A data protection impact assessment must be carried out when the processing poses a high risk to the rights and freedoms of data subjects. Where necessary, advice on performing an impact assessment is provided by the Data Protection Officer.

The Executive Director and department directors shall ensure the availability of the sufficient resources needed to carry out data protection work.

Data protection obligations cover all the personnel and partners of HSL.

Data protection at HSL is assessed regularly in accordance with the data protection management model. The Data Protection Officer reports to the department directors about any data protection deviations, as well as regularly to the department directors and Executive Board, in accordance with the principles of the data protection management model.

The personnel and partners of HSL are obliged to notify their immediate supervisor and the Data Protection Officer of HSL when they detect any deficiencies or errors in data protection practices or other comparable threats to data protection.

## 5 APPROVAL AND UPDATING OF THE DATA PROTECTION POLICY

The Executive Board of HSL has approved the content of this Data Protection Policy. The policy content is reviewed and updated as needed. The Data Protection Officer of HSL is tasked with assessing the need to update the Data Protection Policy and presenting the proposed updates for approval to the Executive Board of HSL.

Approved by the Executive Board on 17 April 2018.