TRAFICOM
Finnish Transport and Communications Agency

Data Balance Sheet 2019

Contents

Traficom publications
10/2020
ISSN 2669-8757 (online)

1. Foreword by the Director of Security

The year 2019 was the first year of operations of the Finnish Transport and Communications Agency Traficom. We have overhauled our operating practices during the year and have also learned a great deal during the process. The organisational reform has required coordination of processes and the introduction of new operating models. The reorganisation has prompted us to take a broader look at public information services and to give priority to data protection and information security in the overall development process.

As our Director-General Kirsi Karlamaa noted in spring 2019, we now need the courage and capability to understand the enormous speed of technological progress so that we are not overcome by speed blindness and are able to support businesses and provide opportunities for competition, while at the same time making their benefits available to consumers and society at large. We are now using this principle as the basis for developing our operations.

The concept of privacy protection is constantly changing and evolving. At the same time, the changes taking place in society are reflected in the way in which the concept of data protection is viewed and we must keep up with these changes. How can we achieve balance between publicity and data protection? Protecting and respecting privacy has now been adopted as the key principle guiding our operations.

The journey has not been an easy one as processing and publishing personal data has been and remains a challenging task. Our services are used millions of times every year. In all our activities, we must take into account how our decisions impact public trust in the authorities. Secure processing of the data collected for the performance of statutory tasks must be ensured.

We must also keep in mind the customer perspective and ensure that it is reflected in our services. We are essentially a service-oriented expert organisation with decision-making powers that needs to know the impacts of its services and what people expect from them. Along the way, we realised that our services should also be tested by people who are not involved in planning and development.

We overhauled our online enquiry services during 2019. We worked to enhance data protection and information security by, for example, minimising unnecessary personal data, limiting the number of searches, and introducing the identification requirement for a number of services containing personal data. Consideration of data protection is built into the overhauled development model introduced by the agency.
In accordance with a well-proven model, this data balance sheet highlights both successes and development priorities while at the same time fulfilling its purpose as an information source. Traficom is a responsible and dynamic expert on transport and communications that promotes the safety and functioning of the Finnish transport system and ensures high-quality, secure and reasonably priced communications networks and services in Finland. In cooperation with other actors, we boost innovations and experiments in the digital society and support sustainable development to protect our living environment.

The Finnish Transport and Communications Agency has its sights boldly and decisively set on the future. We want to be open in a secure manner.

Director of Security
Jari Ylitalo

2. Comprehensive security management in the agency

The comprehensive security management model is part of the agency's management system. The model is based on the ISO 27001 information security standard. Management of security was a key priority in the planning of the merger of the agencies. The management model adopted by Traficom is based on commonly used and well-proven operating practices and it combines operating models used by the former agencies.

Every Traficom employee is responsible for security and we are able to enhance security in our agency through our roles. Comprehensive security in Traficom is the responsibility of the Director-General who manages the agency's security using the strategies and principles adopted by the agency. The agency's executive group monitors the security situation by means of regular reporting. In accordance with the annual clock, the executive group reviews the reports relevant to comprehensive security in the agency and approves key security development projects and security policies for the agency. As a member of the executive group, the Director of Security is responsible for developing comprehensive security in the agency. In 2019, the security function was established as a new function in the agency.

The main task of the security function is to develop the agency's security culture, to ensure that the operations are in compliance with all requirements and to produce a situational picture of comprehensive security in the agency. We encourage our personnel to take part in security management through networking.

The security function steers the agency's

- Data protection
- Information security
- Premises security
- Personnel security
- Risk management
- Preparedness
- Continuity

Security is managed through networks

Management

Traficom's management is responsible for security in the agency. With the help of situational pictures, the management is able to review the state of security and development needs, which facilitates security-conscious decision-making.

Internal auditors

Persons from individual competence areas and functions perform internal audits in accordance with an annual plan. The auditors form a network of auditors.

Risk-management network

Management of the future is based on risk management and active identification of new risks. The purpose of the network is to make risk-management competence part of the day-to-day work and to support the development of a security culture throughout the organisation.

Data protection network

The data protection network coordinates data protection work in the agency. As a channel for exchanging messages, it helps to make data protection as part of the day-to-day work and facilitates the creation of joint practices.

You and me

Each of us is an important link in the chain of ensuring security. We identify security incidents, report on them and prevent more serious damage.

2.1 Risk management

Management of security in our agency is based on risk management. The agency has adopted a risk management policy that sets out its risk management principles and objectives. In risk management, activities are examined from an anticipatory perspective and it is part of the process of preparing matters. It covers all activities, both the organisation's own activities and the activities that the organisation is responsible for by law or under agreements or under other obligations. Performance targets, projects and resources are the areas evaluated by our agency as part of its risk management. The evaluated areas are owned by the agency's executive group, which enhances the risk awareness of the senior management and allows quick focusing of resources when problems arise.

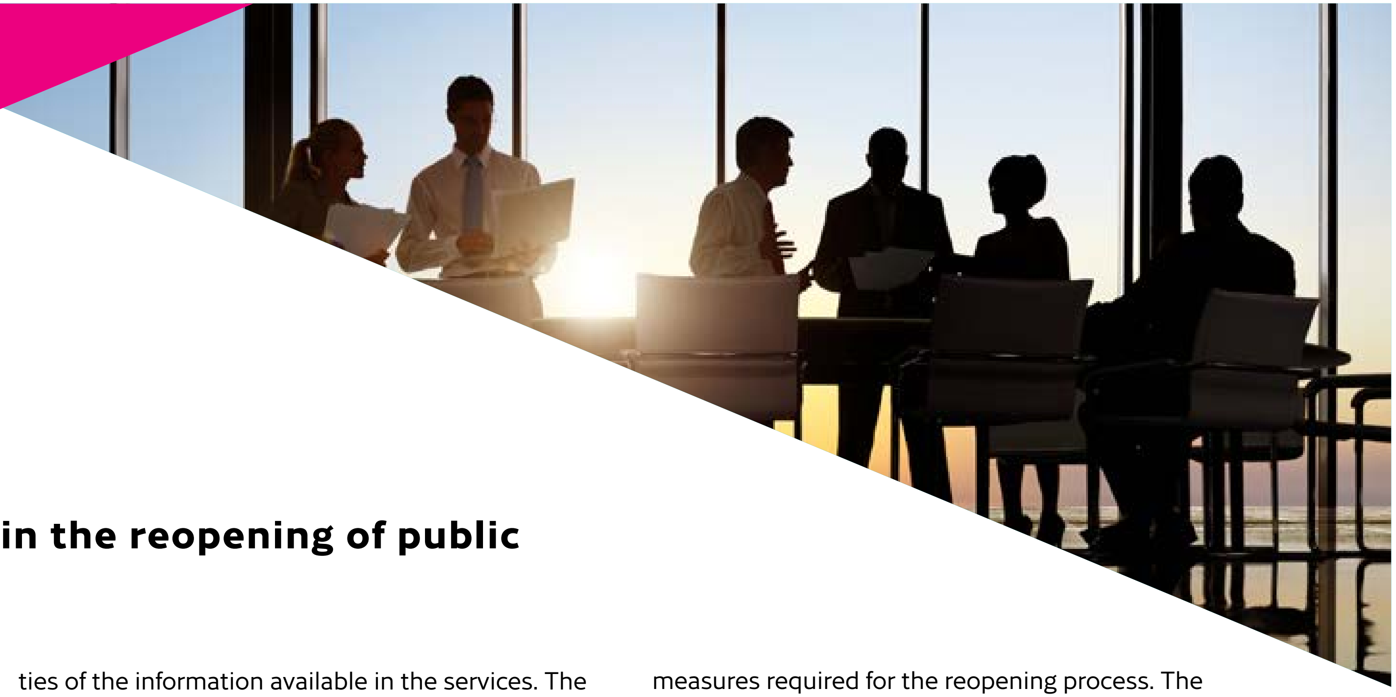
2.2 Information security

During the first year of operations, information security in our agency was reviewed at many levels and through a variety of different frameworks. The way in which our agency assesses its own activities through internal audits is based on the ISO 27001 information security standard. During the summer and autumn, internal audits were carried out by audit teams that were comprised of the agency's employees. We also used external information security experts to evaluate our operations. The audits have helped us to identify development priorities and they have also provided the senior management and the security organisation with a more in-depth view on the level of security in the agency.

Because of the merger of the agencies and the certificate deadline, an external audit covering the ISO 27001 information security standard was carried out in the agency. The purpose of the audit was to produce a single information security certificate for the agency, combining the former certificates of the Finnish Transport Safety Agency and the Finnish Communications Regulatory Authority, and to incorporate the functions transferred from the Finnish Transport Agency into the certificate. The audit revealed minor deviations and development priorities but there were also many positive findings. We prepared plans to correct the deviations and our agency was granted the ISO 27001 certificate on 11 October 2019. According to the audit, our agency should develop its security culture and security awareness of its personnel and assess its risks comprehensively and on a regular basis.

During 2019, information security in our agency was also assessed as part of the updated model for developing services and systems. Information security audits of public information services were carried out in the agency during the year, and they were performed by an accredited assessment body on the basis of the KATAKRI 2015 framework. These audits were also connected with the request for action issued by the Ministry of Transport and Communications, which instructed the agency to carry out information security audits of its key services. Several areas for development in the agency's services were identified in the audits, and we have prioritised the correction and change measures highlighted in the priority and medium level findings, taking into account the life cycle of the services and the feasibility of the measures. The services were made available only after the corrective measures deemed as urgent had been carried out and tested so that the information security risks to the services could be brought to acceptable levels.

During 2019, we also performed ordinary information security audits in about twenty different systems in accordance with the agency's operating practices model.



Case: Comprehensive security in the reopening of public information services

The Finnish Transport and Communications Agency Traficom, which started its operations in early 2019, had to decide on the reopening of the transport enquiry services closed in December 2018. We wanted to ensure that the data protection and information security risks of the services are identified and brought to acceptable levels. The challenge was to identity the key areas where corrections were needed so that individual information services could be made available again in a controlled manner. The key issue was to build a process for reopening the services that would promote trust between the agency's internal stakeholders and openness in development work and decision-making and enhance transparency when decisions on residual risks are made.

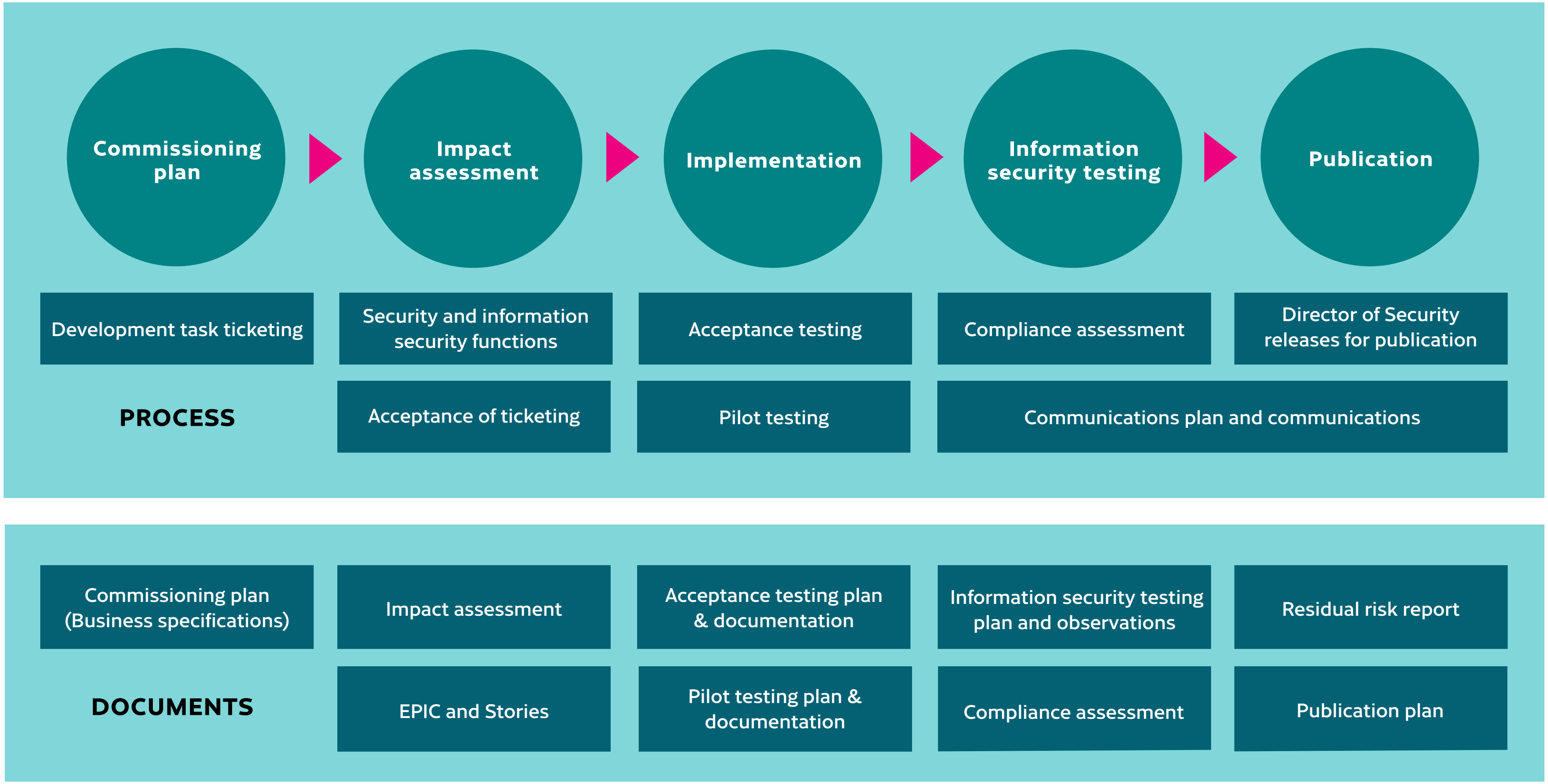
In order to ensure impartiality and transparency, we also used external experts to evaluate the information security, data content and the legal aspects of the processing of personal data. The findings presented by the external experts were used in the redefinition of the properties and content of the services. In their findings, the experts stated among other things that consideration should be given to the search properties of the information available in the services. The agency's executive group received regular reports on the progress made in the reopening of the closed services. The Director of Security supervised the implementation of the information security requirements before the services were reopened.

Separate data protection impact assessments (DPIA) were prepared for the services. The assessments described the processing of personal data, examined the need for processing such data, the proportionality of the processing, the risks arising from the processing of personal data, and the measures that should be used to address the risks. The evaluators drew attention to the data protection principles laid down in the General Data Protection Regulation, such as minimising the processing of personal data. Using the impact assessment as a basis, it is easier for us to comply with the requirements of the data protection legislation, to document them and to ensure accountability.

To reopen the services, the agency prepared separate commissioning plans describing the development measures required for the reopening process. The agency has adopted many of the above operating models in the field of information security, data protection and development as part of its joint development model and daily routines. Furthermore, each of the services that will be reopened will go through the same process, which will ensure uniform and high-quality implementation of the development tasks. Compared with the previous development model, there is now more attention on data protection, information security and risks.

Traficom's enquiry services are extensively used and the information available in the services plays an important role from the perspective of public-sector reliability. For example, private individuals rely heavily on the vehicle information when selling and purchasing vehicles. In fact, in the evaluations preceding the reopening of the services, we had to achieve balance between data protection and information security as well as between the accessibility and appropriateness of the services. The end result is a service that aims to achieve optimum balance between different requirements.

Operating model prepared for the reopening of services



Commissioning plan

Impact assessment

Implementation

Information security testing

Publication

PROCESS

Development task ticketing

Security and information security functions

Acceptance of ticketing

Acceptance testing

Pilot testing

Compliance assessment

Director of Security releases for publication

Communications plan and communications

DOCUMENTS

Commissioning plan (Business specifications)

Impact assessment

EPIC and Stories

Acceptance testing plan & documentation

Pilot testing plan & documentation

Information security testing plan and observations

Compliance assessment

Residual risk report

Publication plan

3. Data protection

3.1 Incorporating data protection competence into day-to-day work

Roles, responsibilities and organisation

Roles, responsibilities and organisation of data protection are set out in the data protection policy of our agency. In accordance with this policy, Traficom, in its capacity as the controller, is responsible for ensuring that the personal data in its possession is processed in a lawful manner in the organisation's operations. Implementing data protection in the agency is the responsibility of Traficom's management. At the same time, the agency's policy functions are responsible for ensuring that they take the data protection requirements into account in their own work. The requirements also apply to data processing carried out on behalf of the agency, in which register data compiled by the agency is used. Each Traficom employee must process personal data in an appropriate manner in their own work tasks. The data protection officer provides employees with advice and guidance in all data protection issues, manages the data protection network, and coordinates the work of the data protection team. The network helps to integrate data protection principles into the agency's day-to-day operations.

The data protection officer provides employees with advice and guidance in all data protection issues, manages the data protection network, and coordinates the work of the data protection team.

In addition to the data protection officer, the data protection team and the data protection guidance and advisory service also support and assist Traficom employees in matters related to the processing of personal data and prepare data protection instructions to support practical work.

The data protection team steers, supervises, guides and trains personnel in data protection matters, and maintains and develops the agency's security culture. In this work, it is assisted by the data protection network.

Data protection network

The data protection network of our agency was launched in October 2019 and the network currently has about 40 members. Data protection ambassadors, employees working in different parts of the organisation who have volunteered to work in the network, play a key role in the data protection network. Supported by the network, they help their own functions in data protection matters. The network does not make any data protection decisions concerning the agency as these are made in accordance with the rules of procedure.

The main task of the network is to promote the sharing of information on data protection matters throughout the organisation and to support continuity management in data protection competence.

The network works to enhance awareness and capability in the use of data protection methods. The network produces information on the state of data protection in our agency to supplement the situational picture produced as part of comprehensive security. The network also reviews phenomena involving data protection impacts at general level and the agency's policies and guidelines in the field of data protection and supports the efforts to incorporate them into day-to-day work.

The network is working to create a positive attitude towards data protection. This is not an additional administrative burden but work to ensure high operational quality and a high level of data protection. It has been noted in the agency that a networked approach to data protection is an excellent way to ensure continuity of competence.

The data protection network works to promote a positive attitude towards data protection

- The network was established in October 2019.
- It has about 40 members from different sectors of the agency.
- It shares information on data protection matters, enhances data protection capabilities in the agency and produces information on the state of data protection.

Data protection training

Traficom arranges both general and tailored data protection training for its personnel. A data protection seminar for all employees was held in November 2019. We have also launched information security/data protection online training for all employees to strengthen each link of the chain as part of the comprehensive development of the information security culture. The contents of the tailored training are planned in accordance with the needs of each policy specialist group. We have noted that such training is an effective way to promote data protection competence.

The data protection instructions and tools are available to all employees on the agency-internal website where new instructions are regularly added as new needs are identified. In these instructions, the requirements set out in data protection regulations are translated into an easier-to-understand language and they are also illustrated with examples from Traficom's operations. The agency is in the process of updating the data protection content of its internal and external websites. By updating our external website, we want to make the information intended for data subjects easier to understand and easier to find.

3.2 Data protection guidelines as tools verifying accountability

Service development manual

The legal framework of data protection is founded on the general data protection legislation and the special legislation supplementing it. We have identified the need for clear and simple guidelines suited for operational use in our day-to-day work. For this reason, the agency has decided to prepare a service development manual as part of the service life cycle.

All agency employees will be familiarised with the contents of the service development manual through training and networks. The publication is also a key element of the development model and serves as a tool for agency employees developing services when data protection is integrated into services.

Service development manual

The service development manual is part of the security management model and its documentation, while at the same time it also supports the model. The manual describes the data protection requirements for the agency's services, which include the prerequisites set by the data protection principles and data protection by design and by default laid down in the General Data Protection Regulation.

These are described as follows:

1. As requirements derived from data protection regulations: guidelines for assessing the roles of different actors in the processing of personal data.
2. As concrete measures in service development: the measures required in the agency's e-services to meet data protection requirements and the rules for processing personal data subject to orders of non-disclosure.

Instructions for service providers

Some of the services coming under the agency's responsibility are provided as outsourced services. The service providers act as processors under the General Data Protection Regulation and on behalf of the agency under commission contracts. These services include the registration of vehicles and watercraft as well as the advisory service.

The processor may only process personal data for the purposes and in the manner specified by the agency in its capacity as the controller. Data protection regulations impose direct obligations on the processor but an agreement on the processing must also be concluded between the parties concerned. The minimum content of the agreement is laid down in the General Data Protection Regulation. In addition to the agreement, the processor must also follow the instructions on the processing of personal data issued by the controller.

At the end of 2019, the agency launched a review of the guidelines applying to the service providers processing personal data on behalf of the agency. The purpose of the guidelines, which are binding on the service providers, is to harmonise the practices of processing personal data. They also serve as an accountability tool and manual and provide a more detailed and concrete basis for processors' obligations. The guidelines will contain a general description of the agency's operations and their regulatory framework. The purpose of the guidelines is to support proper application of the General Data Protection Regulation, taking into account the special characteristics of the sector.

It has been noted in Traficom that sharing successful data protection practices with both private-sector and public-sector actors is a useful and necessary operating model in the development of the agency's own operations. Harmonised operating models in the public administration help to strengthen customer trust and lead to more uniform practices in the processing of personal data used for similar purposes.

Data access control

In addition to issuing guidelines and instructions, we also supervise the use of the data contained in the Transport Register. In order to provide a clearer description of data access control, the agency is in the process of preparing a new control plan, and during the preparations of the plan, we have also worked to identify uniform and optimum central government practices for the planning and implementation of the control. The data access control plan is a comprehensive and cross-cutting description of the overall data access control exercised by the agency each year. The measures to develop data access control will also be described in the plan.

The control plan is one of the instruments used to implement the controller's accountability obligation laid down in the General Data Protection Regulation. The purpose of the control plan is to ensure that the data protection principles set out in the regulation are implemented in all processing of the personal data kept in the Transport Register and to prevent any misuse of the data. The aim is also to ensure that the service providers acting on behalf of the agency and the service providers acting as recipients of data only use the data for the purposes specified in the agreements between them and Traficom and comply with the terms and requirements of the agreements in all processing of personal data. The control plan is prepared for each year and the measures to develop data access control are also detailed in the plan.

3.3 Dealing with personal data breaches in the agency

The agency has a process for dealing with personal data breaches. Traficom employees have been instructed to report any security incidents (including data protection incidents) on a low threshold basis: a mere suspicion of a possible incident must be reported. The agency has produced a set of questions to support the description of personal data breaches and to assess the potential risks to the rights and freedoms of natural persons arising from these breaches. The set of questions helps the parties reporting the breaches to document the incidents. Properly prepared and comprehensive documentation helps to assess the risks arising from personal data breaches.

If the requirements laid down in the General Data Protection Regulation are met, a notification of the incident is made to the Data Protection Ombudsman and, if necessary, to the data subjects affected by the breach. The agency may send a notification to the data subject affected by the breach as part of the corrective measures even though the criteria laid down in the General Data Protection Regulation did not require such a notification.

If, on the basis of a risk assessment, a need for development measures is identified, the measures, the person responsible for them and the implementation timetable are documented. The implementation of the development measures is monitored on a centralised basis. All personal data breaches are reported to the agency's management on a regular basis and using specific procedures.

Lessons learned from personal data breaches

The personal data breaches that have occurred in the agency have allowed us to identify personal data processing operations that may require more effective management measures so that the risks to the rights and freedoms of natural persons can be mitigated. These measures have been documented and the parties responsible for their development have been designated. Operating processes and models have also been developed and measures analysed in cooperation with the agency's policy functions in situations where the root cause of the incident lies in the data subject's own actions, such as giving a wrong email address or inaccurate contact information.

The agency has identified the need for different types of documentation templates, depending on the nature of the personal data breach. At the moment, the agency has two different risk assessment templates the purpose of which is to speed up the risk assessment process and to make it more effective but also to ensure that the accountability obligation is met in the manner set out in the General Data Protection Regulation.

The agency has worked to ensure better identification of security incidents by arranging training and introducing guidelines and by actively communicating on the topic, using such tools as blogs. The aim has been to create a safe atmosphere for reporting incidents and to encourage employees to actively report potential security incidents. In addition to reporting security incidents, employees are also encouraged to produce development proposals and security initiatives.

3.4 Assessing data protection risks

In Traficom, data protection analyses are used to assess data protection risks. The agency utilises data protection analyses when developing services, systems and processes and when implementing programmes and projects.

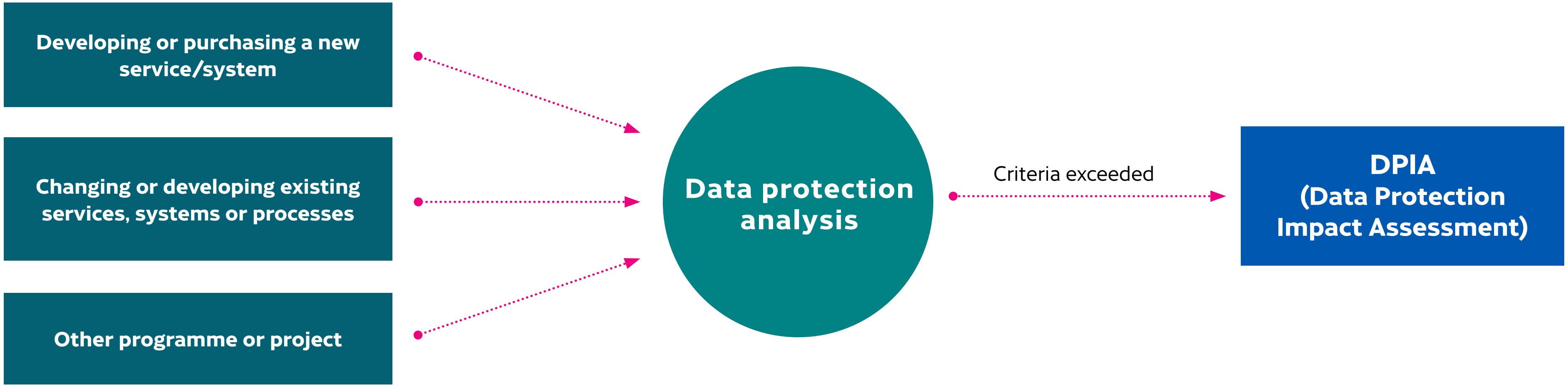
A data protection analysis describes the subject (what is being done and why), the processing in question, and the parties and their roles, and answers questions about the processing, data protection principles, data subjects' rights, and the assessment of data protection risks. The data protection analysis is prepared in multiprofessional groups, which also consider, where necessary, how the case relates to information security issues and the assessment of residual risks.

The purpose of a data protection analysis is to assess whether the case involves processing of personal data and whether a data protection impact assessment should be carried out. If it is determined that the processing of personal data involves a high risk, the data protection analysis is terminated and a more detailed impact assessment of the processing personal data is started. If, however, it is concluded that there is no need for an impact assessment, the preparation of the data protection analysis will continue. The data protection analysis is reviewed and approval for the residual risks is obtained before the commissioning.

The broader impact assessment to be carried out when a high risk is identified helps to understand and analyse factors affecting the processing of personal data, including the necessity and proportionality of the processing, and to identify risks involved in the processing of personal data and risk mitigation measures.

The impact assessment work is part of the planning of the processing of personal data in our agency as well as an integral part of compliance with the requirements for the processing of personal data and the implementation of the controller's accountability as laid down in the General Data Protection Regulation.

Compared with the practices of the predecessor agencies, the current operating model produces more comprehensive and informative documentation of the way in which personal data of the area under development is processed. The documentation templates used in the data protection analysis and impact assessment help to identify early on the personal data processing activities that may involve risks affecting the rights and freedoms of the data subject. The measures used to manage these risks and the residual risk that may remain after the introduction of the management measures will also be appropriately addressed and responsibilities for them will be properly allocated.



Developing or purchasing a new service/system

Changing or developing existing services, systems or processes

Other programme or project

Data protection analysis

Criteria exceeded

DPIA (Data Protection Impact Assessment)

4. Information management

4.1 The Information Management Act will bring changes to architecture work

During 2019, our agency made preparations for the Act on Information Management in Public Administration (906/2019; Information Management Act), which entered into force on 1 January 2020. The new act contains provisions and guidelines on information management, interoperability of data resources and information systems as well as data protection and information security. The new act replaced the Act on the Governance of Data Administration in Public Administration, which contained provisions on enterprise architecture work in public administration.

With the Information Management Act, priority in enterprise architecture work has shifted to describing the current state of the agency (description of the information management model) and to the architecture work carried out as part of the development process (assessment of change impacts). In our enterprise architecture work, we have thus focused on producing descriptions of the current state of the agency and participated in the construction of the development model. We have also implemented development-related architecture work processes and architecture controls as part of the development model.

The work to change the classification of data required under the new act was launched in summer 2019 and we were able to incorporate the changes into our case and document management systems from the start of 2020. Drafting of the changes required under the new act will continue with the preparation of an information management model, a document publicity description and other changes to the case management system.

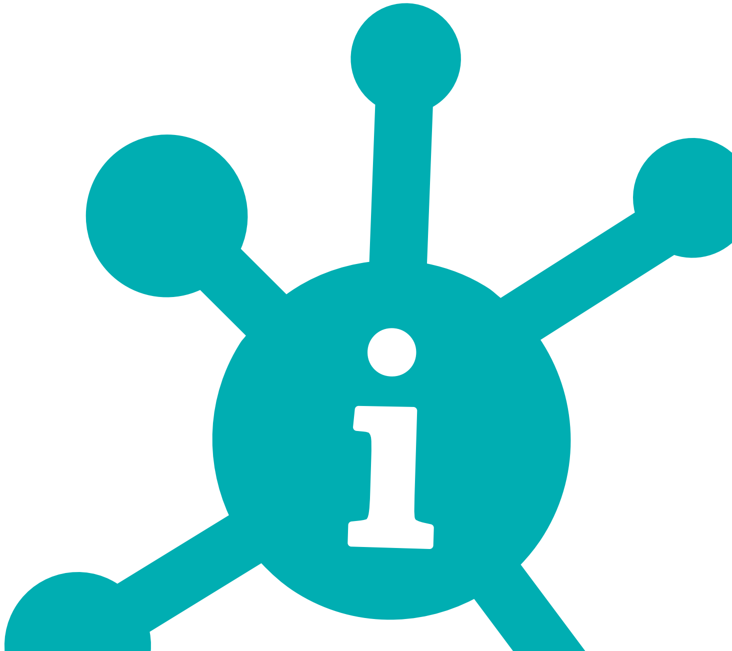
4.2 Developing data architecture

Data architecture is assuming an increasingly important role as data masses are growing and society is becoming more and more digitalised. Because of its scope, data architecture is one of the most challenging sectors of the enterprise architecture. Launching the description of the agency's data capital was the key data architecture development priority in Traficom during 2019. The description is carried out by compiling a data catalogue based on data groups.

The data groups described in the data catalogue form a hierarchical, four-level structure. The data is first broken into primary data groups under which data subgroups are placed. The levels of data groups are used when data capital is categorised and structured for different purposes. With the help of the categorisation factors associated with the data groups, analyses for a broad range of different purposes can be produced. The metadata incorporated into the data groups describes whether the data group contains personal data or whether the information contained in the data group is public or confidential. Furthermore, each data group contains the details of the information management plan task groups comprising the data and the registers to which the data belongs.

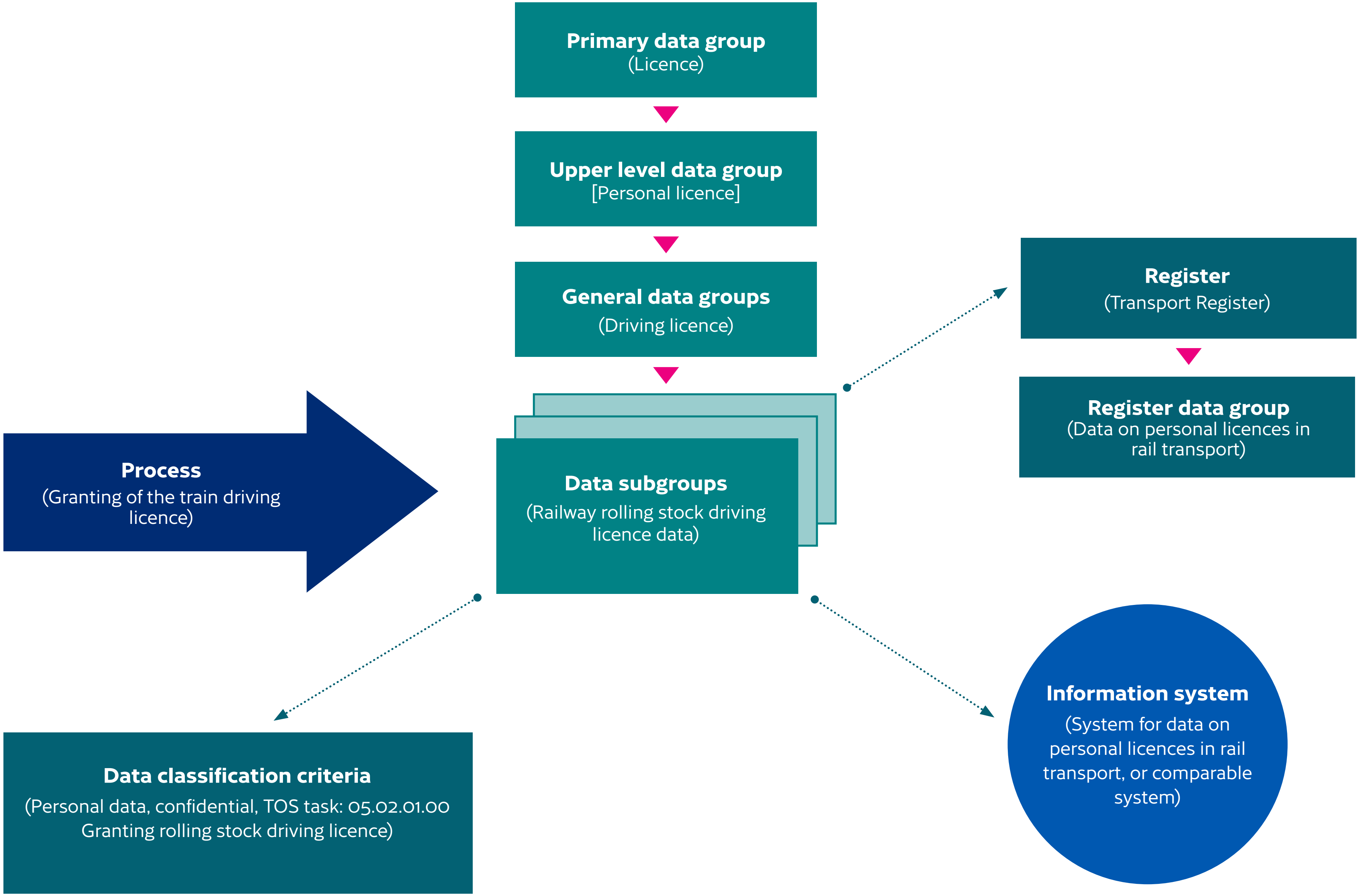
Data categorisation and descriptions can be used in business operations and development tasks when the data in question is described. This also produces an overview of which types of data the development task involves, whether the task involves personal data and whether the data is confidential. The aim of the data architecture work is also to ensure the realisation of business needs and specifications in information systems development and to support the application architecture.

We started the compilation of the data catalogue with the description of the Transport Register and the work is expected to be completed during 2020.



Definition of Traficom’s data groups

[Granting of the train driving licence is used here as an example.]



Primary data group
(Licence)

Upper level data group
[Personal licence]

General data groups
(Driving licence)

Data subgroups
(Railway rolling stock driving licence data)

Process
(Granting of the train driving licence)

Register
(Transport Register)

Register data group
(Data on personal licences in rail transport)

Data classification criteria
(Personal data, confidential, TOS task: 05.02.01.00 Granting rolling stock driving licence)

Information system
(System for data on personal licences in rail transport, or comparable system)

4.3 Case and document management

Information management is guided by good information management practices, under which the authorities must ensure the appropriate availability, protection, integrity and other factors affecting the information throughout its life cycle. In order to ensure good information management and continuity of operations, we decided to start the case and document management in the new agency with separate transport and communications systems. With this move, identifying common principles and operating models for the steering, planning and development of information management was set as the information management objective of our agency. To achieve this, we launched a development task in which the aim was to find and implement, during 2020, a joint centralised case and document management solution meeting all information security requirements.

With the establishment of the new agency, the number of the users of our case and document management systems increased to nearly 1,000 internal and more than 700 external users. We harmonized our operating models and practices by drawing up guidelines and arranging regular user training and support sessions and information briefings on different information management themes. At the beginning of 2019, we also drew up a joint information management plan (TOS), which incorporates the administrative tasks of the new agency and the policy specialist tasks transferred from the predecessor agencies.

About 590,000 cases were processed in the case management systems in 2019. The case management matters are initiated in connection with transport and communications licences, approvals and decisions either through electronic channels or as paper documents via the registry. With the growth of e-services and digitalisation, the number of automatically initiated cases is constantly increasing. Last year, almost 90% of the cases were initiated using automation.

Traficom digitalised about 1.3 million documents in 2019. The digitalisation service is a service supplied by an outsourced service provider in which vehicle registration and inspection documents, application documents related to driving and driver licences are digitalised, and original documents are delivered to the external archive service. During the year, we put the provision of the services out to tender, and they were successfully launched with the new service provider.

Case and document management in figures – 2019

Cases processed in the case management systems **590,000**	**Digital case management documents** **880,000**
Digitalised documents **1.3 million**	**Internal users almost** **1,000**
External users more than **700**	**New working facilities** **200**

5. Development model

As part of the agency reform, a development model tailored to the needs of Traficom was introduced and a number of adjustments have been made to the model during the year. The current version was launched at the start of 2020. In the future, we will develop the operating model using the methods of continuous improvement.

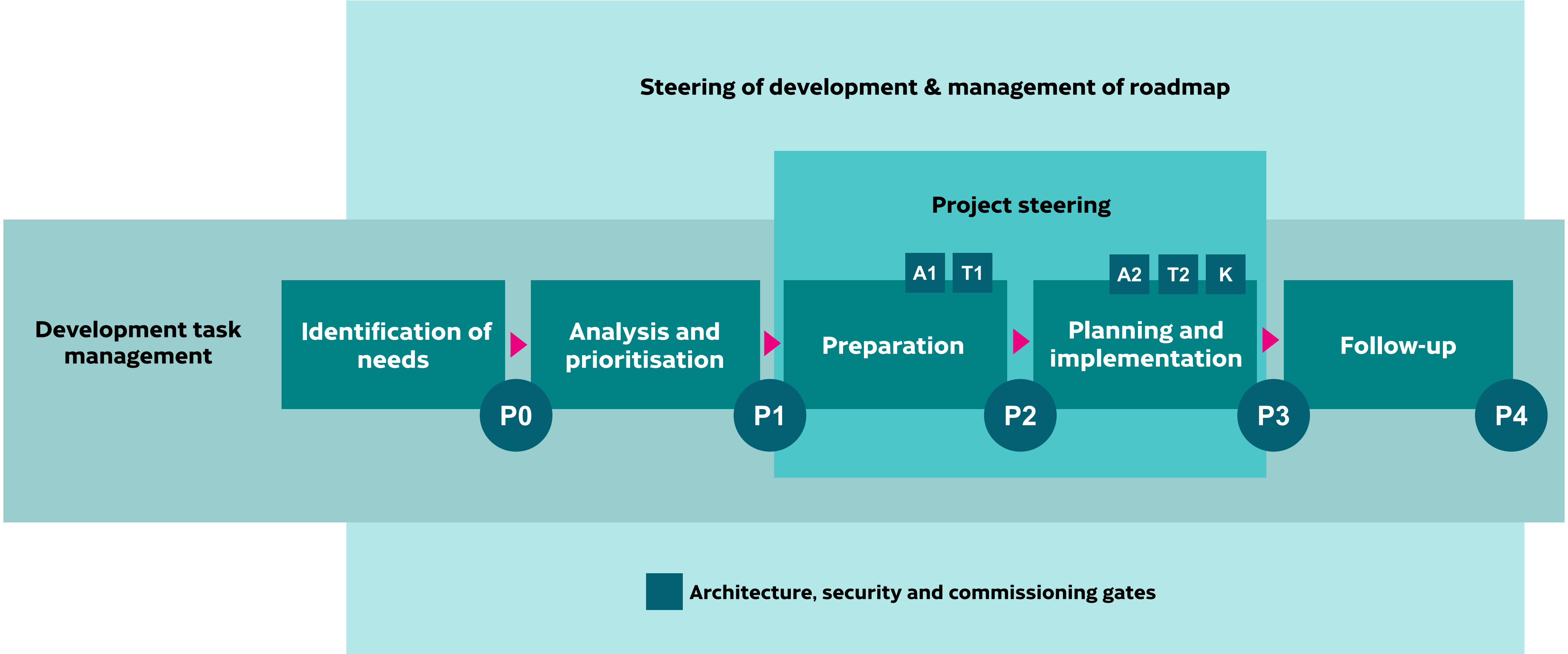
Focus in the construction of the development model has been on the role of data protection, information security and risk management in development work. Transparency of development is one of the key operating principles of the model - except for such tasks as technical systems maintenance and small-scale development, all development is processed through the model. Transparency allows the prioritisation of agency-level development tasks and the focusing of joint resources on major development tasks.

In the operating model, development task interfaces can be used in the agency's shared services, policy functions and other development tasks. The development task passes through architecture and security gates during the preparatory process, planning stage and implementation. The gate procedure ensures that the development task is in compliance with all requirements. The purpose of the commissioning process taking place during the planning and implementation phase is to ensure that the information systems to be used in production, and other development task outputs have passed through the required gates. In addition to gate processing, the development life cycle also involves continuous risk management and assessment of data protection.

The development tasks prioritised by Traficom's executive group team constitute the development roadmap. The roadmap is managed and its development guided in the development steering network, in which all competence areas and the sectors of shared services are represented.

Transparent development is the key principle behind the development model.

Development model



Steering of development & management of roadmap

Project steering

Development task management

Identification of needs

Analysis and prioritisation

Preparation

Planning and implementation

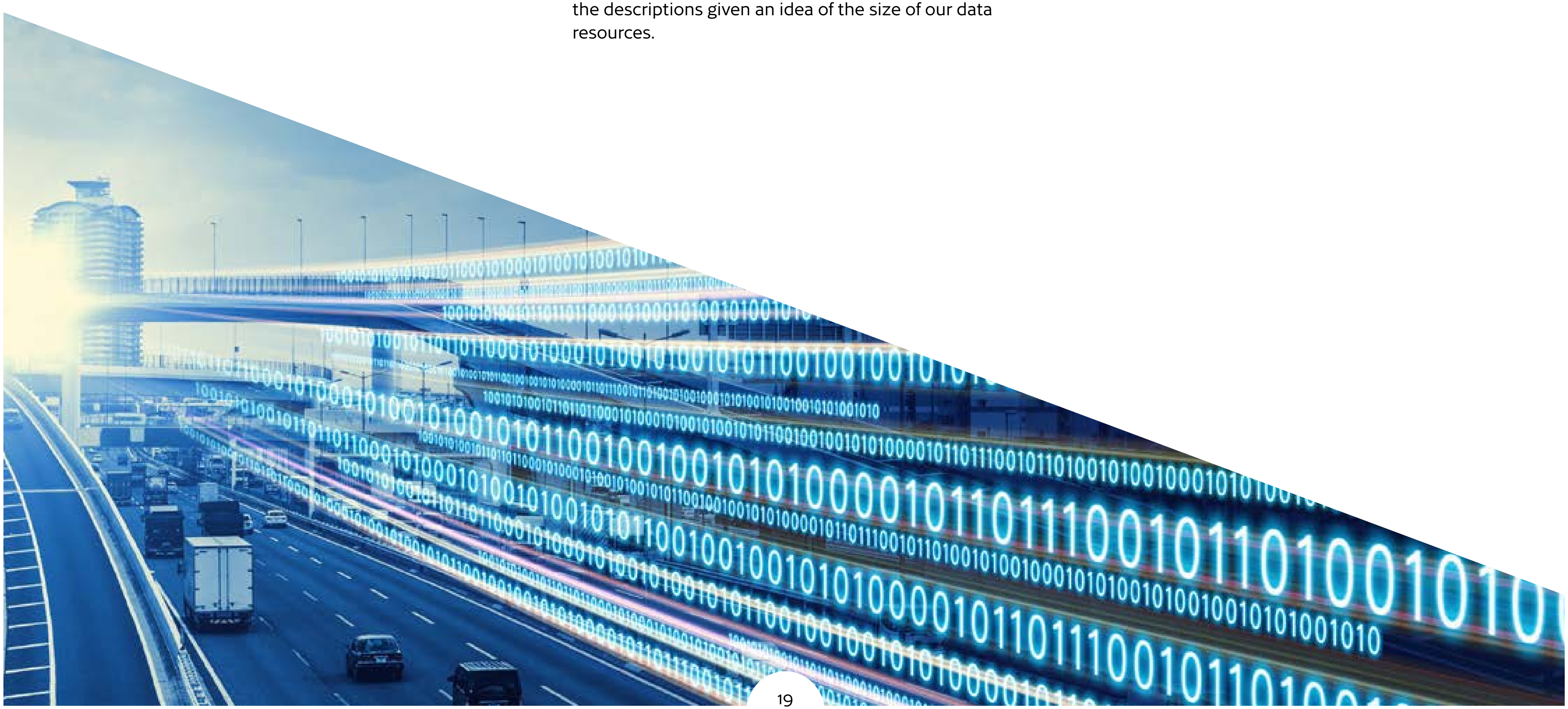
Follow-up

■ Architecture, security and commissioning gates

6. Data flows and information service figures

The Finnish Transport and Communications Agency is a service-oriented licensing, registration and supervisory authority in transport and communications. Performing these tasks requires comprehensive data capital, which comprises extensive communications, transport and mobility data resources.

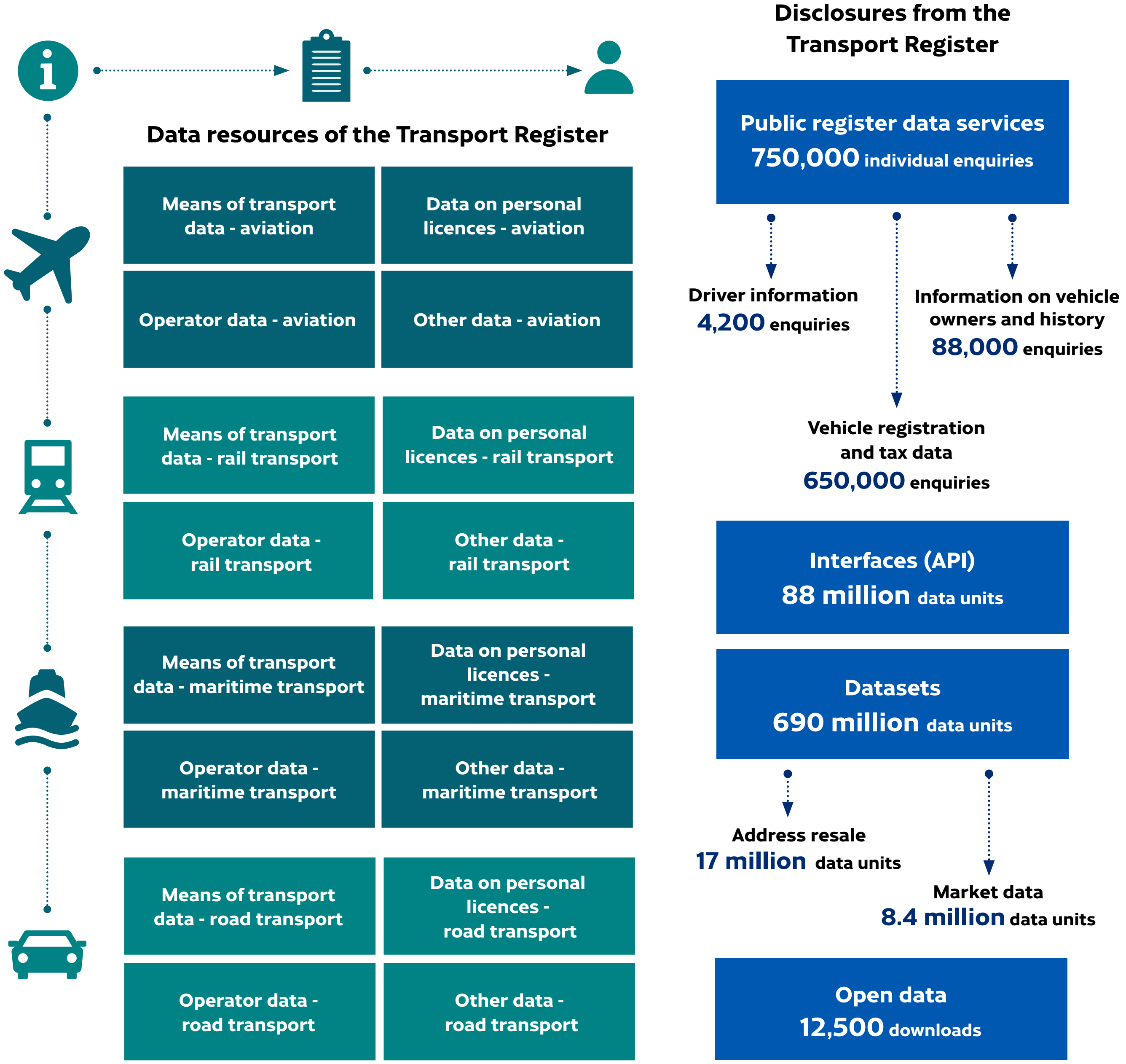
The data flows of the agency's key registers and data resources are described in more detail below. The parties from which data is obtained on a regular basis, storage of the data, and the parties to which data is regularly disclosed are detailed in the descriptions of the agency's data flows. The key figures contained in the descriptions given an idea of the size of our data resources.



Transport Register – Data sources and data resources

Data for the Transport Register is supplied by the following bodies:

- Licence applicants and/or holders
- Those engaged in activities subject to notification
- Owners, holders and/or users of means of transport
- Manufacturers and/or importers of means of transport or the motors for them, or representatives of such organisations
- Education institutions, training organisations and those receiving proficiency tests
- Doctors, psychologists, and communities and/or institutions engaged in nursing or healthcare activities
- Manufacturers and/or processors of licences and cards
- Those engaged in railway transport between Finland and Russia
- Those carrying out registration tasks
- Operators carrying out surveys and inspections
- Those granting individual approvals
- Traficom’s contracting partners
- Motor Insurers’ Centre
- Insurance companies
- Ship operators and shipping companies
- Other authorities



Data resources of the Transport Register

Means of transport data - aviation	Data on personal licences - aviation
Operator data - aviation	Other data - aviation
Means of transport data - rail transport	Data on personal licences - rail transport
Operator data - rail transport	Other data - rail transport
Means of transport data - maritime transport	Data on personal licences - maritime transport
Operator data - maritime transport	Other data - maritime transport
Means of transport data - road transport	Data on personal licences - road transport
Operator data - road transport	Other data - road transport

Disclosures from the Transport Register

Public register data services
750,000 individual enquiries

Driver information
4,200 enquiries

Information on vehicle owners and history
88,000 enquiries

Vehicle registration and tax data
650,000 enquiries

Interfaces (API)
88 million data units

Datasets
690 million data units

Address resale
17 million data units

Market data
8.4 million data units

Open data
12,500 downloads

Data stored in the Transport Register and data storage periods

Personal data

- Personal identity code
- Gender
- Date of birth (if no personal identity code)
- Nationality
- Municipality of residence
- Name
- Signature sample
- Address or other contact information
- Date of birth, municipality of birth and country of birth
- Information on whether the person is alive or deceased
- Photograph
- Business ID
- Mother tongue and communication language
- Statutory fees
- Taxes and their payment
- Functions of persons working as seafarers on Finnish vessels
- Seizures
- Card data from road transport recording equipment
- Enforcement of judgements
- Sequestrations
- Insurance policies
- Parking permits for people with disabilities
- Issuing or cancellation of licences
- Debt restructuring
- Mortgages
- Driving bans and other similar sanctions
- Sentences received for offences committed
- Offences committed on which sanctions have been imposed as an outcome of monitoring tasks

Details of the organisation

- Auxiliary company name
- Communication language
- Domicile
- Name
- Address or other contact information
- Details of the other person responsible for the organisation’s operations
- Identification and contact information of the persons responsible for the organisation’s operations
- Managing director
- General partner
- Company ownership
- Business ID
- Lien data
- Bankruptcy data
- Statutory payment data
- Tax data and details of tax payments
- Data on persons working as seafarers on Finnish vessels
- Seizure data
- Card data from road transport recording equipment
- Data on enforcement of judgements
- Data on sequestrations
- Insurance data
- Debt structuring data
- Data on restructuring of enterprises

Stored for 10 years

Personal data:

- Personal data relating to means of transport is removed 10 years after the means of transport has been scrapped.
- Details of a person are removed 10 years after the person's death.
- Operating ban on a data subject or other administrative measure taken by the Finnish Transport and Communications Agency or the police is removed after 10 years.

Stored for 5 years

Personal data:

- Data found to be erroneous and marked as such

Data that is removed as soon as it is no longer needed

- Data on criminal offences
- Information on the data subject’s health

Data stored in the Transport Register and data storage periods

Means of transport data

- Appropriation data
- Management data
- Holder data
- History
- Approval data
- Inspection data
- Commercial data
- Bodies responsible for maintenance
- Maintenance data
- User data
- Data on prohibitions of use
- Data on restrictions of use
- Data on purpose of use
- Data on commissioning
- Data on decommissioning
- Classification data
- Other registration data
- Other data on technical inspections
- Ownership data
- Construction data
- Registration number and other identification and numbering data
- Technical data
- Data on domicile and operating area
- Data on official inspections
- Data on temporary use

Storage period

Data on means of transport is stored permanently.

Data on personal licences

- Data on issued and cancelled licences
- Licence conditions
- Licence dispensations
- Licence changes
- Licence applications denied
- Licence issuer and home country
- Application and processing of licence, qualification, approval or competency
- Training and experience
- Required language skills
- Health condition and details of examinations made by a doctor or psychologist
- Issuing, cancellation, disappearance and destruction of cards and certificates relating to licences, qualifications, approvals, and competencies
- Any other data to be recorded in the Transport Authority's registers in accordance with EU legislation and international agreements.

Stored for 10 years

- After the expiry of the licence or when the personal data is no longer needed for the purpose it was recorded for
- Railway qualification data after the expiry of the licence

Stored for 70 years

- Seafarers' seagoing service, training and competency information from the data registration

Data on organisations' licences

- Data used for assessing good reputation and reliability
- Data on processing of notifications
- Data on operations subject to notification
- Licence content
- Licence conditions
- Licence number
- Data on licence application and processing
- Changes to licence
- Data on the requirements for issuing a licence and for creating the register entry on operations subject to notification
- Licence period of validity
- Issuing or cancellation of licence
- Data on incident reports
- Data on undertakings classed as posing an increased risk

Storage period

From the cancellation or expiry of the licence.

Disclosure of data from the Transport Register

Generally available data:

- Valid operator's licences
- Licence number
- Name of licence holder
- Contact details for licence-related operations
- Contact details relating to operations subject to notification

The data can be disclosed so that it cannot be connected with natural persons or legal persons.

Everyone has the right to get as individual release

- The following data on operator licences, by providing a Business ID, company name or licence number:
  - Name and contact information of the licence holder
  - Licence number
  - Licence period of validity
  - Name of the person responsible for the company's operations
- The following information on a natural person as an
  - Operator on the basis of the first and last name,
  - Personal identity code, or other unique identifier:
  - Operator's name
  - Work contact details
  - Licence number
  - Licence period of validity
- On the basis of a means of transport identifier
  - Details of a means of transport and the name of its owner, holder, user and representative, as well as address and other contact information, and information on vehicle inspections, taxation, mortgages and insurance policy holders
  - Based on the first and family name, personal identification code or another unique identifier, information on the right of a person to operate a means of transport or on the validity and scope of other personal licences.

Data can be disclosed for the following transport-related purposes:

- For providing and developing transport services
- For public opinion surveys and market research, for direct marketing and for other address and information services
- For updating the contact details and means of transport data entered in the customer database
- For other similar purposes approved by the controller.

The disclosed data may only be used for the purpose for which it was disclosed. Data may only be disclosed or otherwise provided to third parties if the disclosure is based on Finnish law, obligations laid down in international agreements that are binding on Finland, European Union legislation, or a specific permission received from Finnish Transport and Communications Agency.

Data can be disclosed for the following development and innovation activities on a case-by-case basis:

- For providing and developing transport systems and services
- For increasing awareness and understanding of transport systems and services
- For improving traffic safety and for promoting the environmental goals of transport.

Confidential data may only be disclosed with the individual's consent or in such a form that the data cannot be connected with individual persons. Data obtained by the Finnish Transport and Communications Agency from criminal records or the register of fines may only be disclosed in such a form that the data cannot be connected with individual persons.

The disclosed data may only be used for the purpose for which it was disclosed. The data must be removed as soon as it is no longer needed for this purpose, and it must not be disclosed to third parties.

Notwithstanding secrecy provisions, the Finnish Transport and Communications Agency may disclose data to another authority or body performing a statutory duty if this authority or body needs the data for performing the duty.

The Finnish Transport and Communications Agency may not, however, disclose any confidential information that it has obtained from criminal records or the register of fines, unless otherwise provided elsewhere by law.

The Finnish Transport and Communications Agency may disclose information kept in the register to authorities of other countries or for official functions if the disclosure is based on the law, European Union legislation or on international agreements binding on Finland. If personal data is transferred outside the European Economic Area, the conditions of Chapter V of the European Union's General Data Protection Regulation must be met.

Other authorities that receive data from the Transport Register may disclose that data to a third party if the above conditions are met.

The Finnish Transport and Communications Agency may also supply a service provider with a photograph and a signature sample if the service provider in question needs them for performing a statutory task.

Restriction of data disclosure from the Transport Register

Natural persons have the right to prohibit the disclosure of their personal data

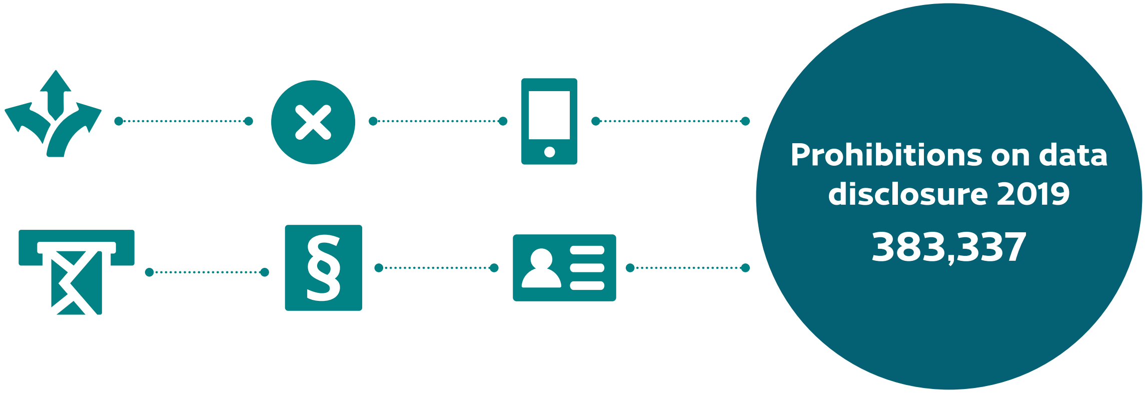
- That is generally available
- For transport-related purposes
- For development and innovation activities
- And to prohibit the disclosure of their contact details as an individual release.

Legal persons have the right to prohibit the disclosure of their data

- For development and innovation activities.

Provisions on the processing of the data of persons subject to an order of non-disclosure for safety reasons are contained in sections 36 and 37 of the Act on the Population Information System and the Certificate Services of the Digital and Population Data Services Agency (661/2009). When the order of non-disclosure is transferred to the Transport Register, the disclosure restriction is extended to cover the name of the natural person. The recipients of the disclosed data must also be notified of the order of non-disclosure and the restrictions on the use and protection of the data.

Notwithstanding the order of non-disclosure, the data can be disclosed to authorities or other bodies if they need the data for performing their statutory duties.



Prohibitions on data disclosure 2019

383,337

Individuals who have prohibited the disclosure of their data in some way	**383,337**
Non-disclosures for direct marketing	**377,793**
Non-disclosures as individual release	**300,556**
Non-disclosures for transport-related purposes	**288,987**
Non-disclosures in open interfaces	**74,865**
Non-disclosures for development and innovation purposes	**67,475**
Order of non-disclosure	**9,827**

In 2019, a total of 383,337 individuals whose data was stored in the Transport Register had prohibited the disclosure of their data in some way.

The table gives the numbers for each type of non-disclosure. One individual may have several types of non-disclosure in force at the same time. Companies and organisations may not restrict the disclosure of their data for activities other than those involving development and innovation. Applications for orders of non-disclosure for safety reasons are submitted to a local register office, which enters the non-disclosure orders into the Population Information System. The system is maintained by local register offices.

The most commonly used type of non-disclosure is the non-disclosure for direct marketing, which prohibits the personal data from being disclosed for for direct marketing. This prevents the individual from receiving marketing messages from vehicle inspection companies, car dealerships or other similar service businesses.

Data on transport services

Providers of transport services

- Aviation
- Rail transport
- Maritime transport
- Road transport

Data resources of the transport service catalogue NAP and the Digitransit open journey planner

The transport services include

- Operating areas and hours of service
- Routes and timetables
- Reservation service information
- Fare information
- Accessibility and other service information

NAP:
A total of about 20 GB of data
has been transferred to the transport service catalogue NAP each month.

The transport service catalogue NAP (National Access Point) can be viewed at www.finap.fi.

Digitransit:
About 20 million route searches each month
About 200 GB of data
has been transferred each each month

Digitransit (www.digitransit.fi) provides information on public transport routes and timetables as open data.

Communications datasets

Data for communications network datasets is supplied by the following parties:

- Telecommunications network companies
- Providers of communications services
- Applicants for radio licences
- Traficom

The data is stored in the following datasets:

- Broadband network availability data
- Data on radio networks subject to licence
- Public frequency allocation table
- TV and radio stations in Finland

The data is used for the following purposes:

- Steering and supervision of the communications market
- MONITORi service
- Steering and supervision of frequency use
- Radio microphone application
- Open data

Data on personal communications licences, qualifications and identifiers issued to persons is supplied by the following parties:

- Examination participants
- Assessors
- Applicants for certificates
- The Finnish Amateur Radio League (SRAL)
- Applicants for radio licences
- Traficom
- Registrars

The data is stored in the following datasets:

- Maritime radio communication certificates
- Amateur radio certificates
- Radio licences granted to private persons
- Amateur radio licences
- Amateur radio call signs
- MMSI numbers
- Details of fi-domain names

The data is used for the following purposes:

- Steering and supervision of frequency use
- Open data
- Register maintenance

Communications datasets

Data on operators and identifiers granted to operators is supplied by the following parties:

- Applicants for phone numbers, codes and identifiers
- Applicants for radio licences
- Applicants for operating licences
- Traficom
- Operators that have submitted a telecommunications notification
- Operators that have submitted a broadcasting notification
- Operators that have submitted a notification of video-on-demand audiovisual services
- Operators that have submitted a pay-television service notification
- Operators that have submitted a notification
- Operators that have submitted a notification on postal operations
- Parties that have registered as a registrar

The data is stored in the following datasets:

- Holders of phone numbers, codes and identifiers related to telecommunications networks
- Radio licence holders
- Holders of operating licences
- Universal service providers obliged to provide phone or broadband access
- Telecommunications operators
- Broadcasters
- Providers of video-on-demand audiovisual services
- Providers of pay-television services
- Qualified providers of electronic trust services
- Providers of strong electronic identification services
- Postal operators
- fi-domain name registrars

The data is used for the following purposes:

- Register maintenance
- Partially open data
- Steering and supervision of frequency use
- Supervision of universal service
- Steering and supervision of domain name operations

Communications datasets

Transport and communications data is supplied by the following parties:

- Telecommunications companies
- Traficom
- Parties and persons submitting incident reports
- Telecommunications operators and other network operators
- Parties submitting notifications of radio interference
- Providers of communications services

The data is stored in the following datasets:

- Reports on information security breaches
- Details of the network monitoring and early warning system
- Information security breaches reported by telecommunications companies
- Faults and disruptions in communications networks
- Radio interference
- Information on developments in the sector

The data is used for the following purposes:

- Supervision of the functioning and safety of communications networks and services
- Partially open data
- Supervision of the functioning and safety of communications networks and services
- Advice
- Supervision of frequency use and investigation of radio interference
- Steering and supervision of the communications market
- Publication of data
- Open data

TRAFICOM
Finnish Transport and Communications Agency

Finnish Transport and
Communications Agency Traficom
PL 320, 00059 TRAFICOM
p. 029 534 5000

traficom.fi