Publication 00x/2018 J of the Finnish Communications Regulatory Authority APPENDIX

Background study: Data protection, information security and verifying reliability of contracting parties

Viestintävirasto

Contents

1 Introduction

Sections 6, 7 and 8 of publication 00X/2018 J xx of the Finnish Communications Regulatory Authority (FICORA) include brief summaries of issues pertaining to data protection, information security and verifying the reliability of contracting parties. These issues should be considered when signing agreements.

This background study discusses the said issues in more detail. Both observations regarding acting on someone else's behalf and observations regarding a single ticket sales interface discussed in FICORA's publication 004/2017 J *Lippu project report on contractual practices for travel chains defined in the Act on Transport Services (code of practice for travel chains)* are covered in this background study.

Legal studies by Dittmar & Indrenius from 2017 and 2018 on the processing of personal data and the appendix LIPPU-API: *Security Considerations. ADDITION 2018: informative list of standards, specifications or frameworks* have to do with the subject matter of this background study.

In this context, 'mobility service network' refers to contractual relationships and cooperation between providers of mobility services in accordance with the Act on Transport Services that enable the provision of uninterrupted travel chains for passengers and the acting on someone else's behalf.

1 Processing of personal data (data protection)

1.1 Regulations and oversight

Part III, chapter 4, section 4 of the Act on Transport Services includes general regulations on privacy protection and data protection when opening interfaces.

There are regulations on the protection of personal data in the European Union's General Data Protection Regulation (EU) 2016/679. Legislation on the protection of personal data applies whenever personal data is being processed.

The competent authority in the oversight of the Data Protection Regulation is the Data Protection Ombudsman. Consequently, the Finnish Transport and Communications Agency Traficom cannot determine which actions comply with the requirements of the Data Protection Regulation.

Legal expert reports on the opening of a single ticket sales interface and on acting on someone else's behalf have been acquired to support the parties involved. The report on acting on someone else's behalf also provides practical instructions on the design of systems (including issues such as the minimisation of the number of attributes used, logs, the determination of retention periods and careful consideration of mass delivery).

In this section of the code of practice background study regarding the processing of personal data, the term '**report**' refers to a legal analysis by Dittmar & Indrenius on the processing of

personal data in the travel chain and when acting on someone else's behalf.

This section of the background study concerning the processing of personal data has been prepared from the viewpoint of the application of the General Data Protection Regulation using the concepts and processing principles defined therein.

1.2 Concept of personal data and personal data in mobility service network

1.2.1 Definition of personal data

According to Article 4(1) of the GDPR, 'personal data' refers to any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be authenticated, 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.

The definition of personal data is very broad. When travel chain services are offered to passengers, personal data is usually processed. Such data includes contact details and credit card data processed when a passenger places an order. Personal data also includes the information required to authenticate a travel authorisation.

As a result, the GDPR largely applies to the mobility service network.

1.2.2 Pseudonymisation and anonymisation

It should be noted that even if data is pseudonymised, it is still regarded as personal data. Even if a single party to the travel chain cannot authenticate the identity of a passenger, authentication of a person by combining different pieces of information is considered sufficient. Therefore, a travel identifier that does not include a passenger's name or any other distinctive personal data, but that a party can connect to a single passenger, is regarded as personal data.

In exceptional cases, one of the parties to the mobility service network may not process any personal data in the travel chain. If data is anonymous or if it cannot be connected to a natural person, either directly or indirectly, such data remains outside the scope of the GDPR.

Data is anonymous if personal data is irrevocably converted into a format in which the data subject cannot be identified by any party, either directly or indirectly. In its statement (5/2014) regarding data anonymisation, WP 29 consisting of representatives of data protection authorities from EU member states determined that data is anonymised by processing personal data in a manner that irrevocably prevents the identification of the data subject; also see Government Proposal 145/2017, Section 2.1.1.9, Henkilötietojen anonymisointi ("Anonymisation of personal data").

1.3 Positions of controller and processor

Different roles are involved in the processing of personal data.

- A controller defines the purposes and methods of processing personal data, independently or together with others.
- A processor processes personal data on behalf of the controller. In this case, processing is commissioned or subject to subcontracting or a partnership.
- There can also be parallel controllers, in which case each controller has an independent right to process personal data.

The controller independently determines the purposes of data processing and uses data for its own purposes in accordance with its own data processing procedures. The processor does not process data for its own purposes. Instead, the processor processes the data in accordance with instructions issued by the controller and an agreement signed with the controller, and only on behalf of the controller. Furthermore, the processor does not have any independent right to use the data.

The controller must notify data subjects of any processing of personal data. This information must be provided in a clear and understandable format. The GDPR defines the information to be provided in more detail. This information includes the controller's contact details, information about the purpose and principles of data processing, and information about the rights of the data subjects. However, the parties can also agree upon their mutual responsibilities so that a contracting party is obligated to give information to the data subjects.

When data is transferred from one controller to another, the transferring party is responsible for ensuring that the data is transferred in compliance with legislation.

1.3.1 Roles in travel chains

In the mobility service network, the MaaS operator, being the comprehensive service provider, acts as the controller regarding personal data collected from passengers.

The MaaS operator, being the intermediary, and transport service providers can act as controllers and/or processors, depending on which data is being processed and what has been agreed upon regarding the tasks and roles of each party. The roles must always be assessed on the basis of the actual processing function and case, however. Deviating from any roles defined in legislation is not possible.

1.3.2 Roles when acting on someone else's behalf

On the basis of a legal analysis, the parties' roles in the processing of personal data seem clear. According to the report, in the case of acting on behalf of a natural person's user account, the parties are, as a rule, independent controllers. In such a case, each party bears the responsibility for the processing of personal data.

The GDPR does not specifically mention parallel controllers, but in practice, responsibilities can be assessed as a relationship between parallel controllers. Issues to be agreed by parallel controllers are discussed below.

An assessment of the roles in the processing of data in the user account of a **natural person**:

- User: data subject.
- Party acting on someone else's behalf (mobility service or integrated mobility service): independent controller.
- Party granting access (mobility service or integrated mobility service): independent controller.
- Party granting access (party responsible for a ticket and payment system on behalf of the mobility service or integrated mobility service): depends on the agreement between the mobility service or integrated mobility service and the party responsible for the ticket and payment system, i.e. whether the party responsible for the ticket and payment system is an independent controller or a processor. When processing personal data, a processor acts in compliance with its agreement with the controller (Article 28 of the GDPR), and decisions on any transfers to another controller are made by the controller, not by the processor.
- Third party managing data pertaining to the determination principles of a discount, compensation or special condition: independent controller.

An assessment of the roles in the processing of data in the user account of a **legal person**:

- From the perspective of the GDPR, the roles are different than in the case of a user account of a natural person.
- Employee, consultant, etc. of the legal person (user company): data subject
- Legal person (user company): controller
- Party acting on someone else's behalf: may be a processor on behalf of the user company, but may also be a controller
- Valid grounds for processing must be assessed on the basis of the role

1.4 Principles of processing personal data and purpose of personal data

Processing personal data is always subject to a legal processing principle. The purpose of the processing of personal data has an impact on the selection and determination of the processing principle.

According to the GDPR, personal data can be processed

(a) with the consent of the data subject;

(b) in order to implement an agreement between the data subject and controller;

(c) for compliance with a legal obligation to which the controller is subject;

(d) to protect the vital interests of the data subject or of another natural person;

(e) 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 controller; or

(f) for the purposes of the legitimate interests pursued by the controller or by a third party.

The purpose of the processing of personal data has an impact on the selection and determination of the processing principle. Purposes must be planned and determined before any data is collected. In the mobility service network, data is mainly collected to provide services and manage customer accounts. The controller must inform data subjects of the purposes before processing any data. It should also be noted that, primarily, data can only be used for the predetermined purposes.

1.4.1 Grounds for processing in the travel chain

In the mobility service network, personal data will mainly be processed on the basis of item b (implementation of an agreement) or f (protection of legal interests). In addition, a public party regarded as an authority taking part in the implementation of the travel chain (such as a joint municipal authority) can process personal data on the basis of legal interests, insofar as the processing does not concern the exercise of public power or the performance of other public administrative tasks. A controller may have several parallel principles for processing personal data for different purposes.

If the controller wants to process other personal data in addition to the data required to provide services, the data subject's consent (a) may be required. It is essential that the request for consent is clearly formulated so that the data subject understands to what they are giving their consent. The data subject must give their consent voluntarily by means of an active procedure.

1.4.2 Processing principles when acting on someone else's behalf

According to the report, the personal data processing principles can be clearly determined when someone is acting on someone else's behalf. As a general rule, the processing principles may consist of the implementation of an agreement or compliance with the statutory obligations of a party obligated to open up its API. However, consent from the data subject is required for the processing of sensitive personal data.

The existence of valid grounds for processing must be assessed on the basis of the specific controller's position and the purpose of the data. The grounds for processing must be assessed in light of the GDPR, which limits the freedom of contract.

Personal data may be disclosed to a controller that has valid grounds for processing. A right to view the data is also considered disclosure, even if the party viewing the data does not save any data.

Assessment on grounds for processing in compliance with the GDPR:

- Party acting on someone else's behalf: implementation of an agreement with the user.
- Party obligated to open up its API: a statutory obligation; alternatively, preparation of the implementation of an agreement with the data subject.
- Third party: a statutory obligation has been specified in the Act on Transport Services, but it takes the form of a general cooperation obligation. However, the processing may also be based on, at the very least, the legitimate interests of the party obligated to open up its API. The impact of special regulations in relation to the Act on Transport Services has not been assessed in the case of the Social Insurance Institution of Finland (Kela), for example.
- Sensitive data: specific consent from the data subject is required, because the Act on Transport Services does not include any specific regulations to the contrary. From a technical viewpoint, the consent can be given through an electronic signature or two-factor authentication, for example. Requesting the consent once is sufficient, as long as the request is carefully formulated to cover more continuous acting on someone else's behalf.

1.4.3 Personal data required for acting on someone else's behalf

The general requirement of only processing necessary personal data means that each controller must assess which personal data it needs to process. The fact must be kept in mind that on this necessity basis, the personal data may only be used for the purpose of acting on someone else's behalf; the data may not be used for marketing purposes, for example.

To assess necessity, the following issues must be considered:

- Minimisation: the controller may only process data that is necessary to complete the process of acting on someone else's behalf. The controller must assess whether data is necessary and whether the service can be reasonably provided without a specific piece of personal data. Furthermore, when disclosing data, the controller must verify that the recipient actually needs the data. Any mass disclosure of data must be assessed with special care.
- Relevance to the purpose: personal data may only be used for the purpose for which it was provided. Therefore, personal data provided for the purpose of acting on someone else's behalf may not be used for marketing purposes, for example.
- Retention period: the retention period of the data must be specified and the data must be retained only for the period of time that is necessary to secure legitimate interests, such as to ensure the possibility to process complaints. When this period expires, the data must be deleted or anonymised. Proper deletion of personal data when the agreement is terminated must also be ensured.

1.5 Rights of data subjects

Data subjects, or the users of services, have several rights related to the processing of personal data. Initially, each controller is responsible for the fulfilment of rights regarding the data they have collected.

Parties to the mobility service network must take the fulfilment of the data subjects' rights into account in their activities and in mutual agreements.

- In order to ensure that data is processed in a transparent manner, the controller must give information to data subjects before processing any data.
- If a data subject wants to obtain more information about the processing of their personal data, the controller must respond to the data subject's requests without undue delay. There are regulations on deadlines in the GDPR.
- Data subjects have the right to check what personal data the controller processes, to have data erased or rectified, or to restrict the processing of data.
- In certain cases, data subjects also have the right to object to the processing of data.
- If data is processed in order to execute an agreement or based on the data subject's consent, the data subject has the right to transfer their data from one system to another (to another controller). Furthermore, data subjects always have the right to revoke any consent given to process data.

1.6 Data protection stages and agreements when acting on someone else's behalf

1.6.1 The following data protection stages can be identified:

- The parties assess their roles in the processing of personal data
- Each controller assesses and documents the necessary data and its purpose when acting on someone else's behalf
- Each controller assesses and documents its grounds for processing data
- Each controller assesses and documents the information security of its personal data processing
- If personal data will be processed by a party (usually a subcontractor) that must be considered a processor, the controller must ensure that there is an agreement on the processing of data as specified in Article 28 of the GDPR
- An agreement between parallel controllers, i.e. the party acting on someone else's behalf that has right of access and the party obligated to open up its API, covers all the necessary issues
- In case of a personal data breach at the production stage, each controller is obligated to investigate the case and inform the contractual partner and the data subject

1.6.2 Agreement between parallel controllers

Parallel controllers should consider the following in their agreement:

- Personal data to be processed.
- A list of which personal data and for which purposes the contractual parties may view and save when acting on someone else's behalf.
- Due to the data protection obligations, the party obligated to open up its API has the obligation to ensure that data will only be disclosed to parties who have the right to process the data; the grounds for processing of the personal data and the purpose in the case of parties viewing/receiving personal data must be considered with special care. The party disclosing information can use the agreement to prove that they have ensured that personal data is only disclosed to parties which have the right to process the data.
- Securing the integrity and confidentiality of another controller's data, such as agreeing on the use of logs (if any).
- Verifying protection of the user's/data subject's rights.
- Communication between the controllers in case a data subject wishes to rectify or erase their data.
- Necessary communication in case of a personal data breach.
- Informing users.
- Retention periods of data (if required).

2 Information security

2.1 Regulations and oversight

Part III, chapter 4, section 4 of the Act on Transport Services includes general regulations on information security when opening interfaces.

Article 32 of the General Data Protection Regulation includes regulations on the information security of personal data processing.

Oversight of the Act on Transport Services is the responsibility of the Finnish Transport and Communications Agency Traficom (prior to 2019, the Finnish Transport Safety Agency Trafi).

The Data Protection Ombudsman oversees information security requirements in personal data processing.

2.2 Verifying proper level of information security (information security requirements)

To ensure the information security of the interface and the service, good information security practices must be followed.

Maintenance of information security refers to the technical and organisational activities that a party implements in order to ensure integrity and availability of networks and data systems, as well as confidentiality of information.

Verification of information security requires continuous management of information security as a whole and implementing the necessary information

security actions to verify the security of data communication and data systems, operational security and physical security.

These actions must be based on recent technical development and the costs of the actions, and the actions must be proportional to the current threats and risks.

2.2.1 Confidentiality, integrity and availability

Maintenance of information security refers to the technical and organisational activities that a party implements in order to ensure integrity and availability of networks and data systems, as well as confidentiality of information.

- *Confidentiality* means that only people entitled to use the data are able to access it. In practice, this requires determining the data and the persons entitled to use the data to a sufficient detail.
    - The *Bell–LaPadula Model* (BLP) can be used, for example.
- *Integrity* means that nobody must be able to modify the data or the system, or unlawfully destroy the data during its lifecycle, and that all such modifications must be detected.
- *Availability* means that the data or the system must be available whenever it is needed. Availability also means that the capacity must be sufficient for the needs.
    - The code of practice does not include any more detailed specification of availability issues. The parties must agree on these issues, taking into account statutory requirements on fairness, reasonableness and non-discrimination.

2.2.2 Security of data communication, security of data systems, operational security and physical security

Good information security practices cover the management of general information security, as well as the security of data communication, the security of data systems, operational security and physical security.

All the issues listed below should be taken into account, where applicable, when determining the adequate information security actions.

1) Security of data communication

a) Structural network security

b) Segmenting of the communication network

c) Filtering rules according to the principle of least privilege

d) Management of the entire lifecycle of filtering and control systems

e) Control connections

2) Data system security

a) Management of access rights

b) Authentication of system users

c) Hardening of systems

d) Malware protection

e) Tracing security events

f) Security incident observation capability and recovery

g) Internationally or nationally recommended encryption solutions

3) Operational security

a) Change management

b) Processing environment for confidential materials

c) Remote access and remote management

d) Management of software vulnerabilities

e) Backup copying

4) Physical security

a) Physical protection and access control in facilities of the operator

b) Physical protection and access control of service providers used

Identifying contractual parties

The security of data communication and data systems includes the contracting parties being able to agree upon the reliable changing and management of certificates used to authenticate the parties or their credentials. The authorities do not offer any centralised management of certificates for the mobility service network. The contracting parties must apply good information security practices to the management. Furthermore, it is recommended that certificates be granted for a maximum period of three years at a time.

2.2.3 Procedures in proportion to risks

The starting point of the information security practices required from both parties is the use of threat modelling and risk evaluations. These are based, for example, on the volume of personal data and payment instrument data

to be protected and financial risks, as well as financial losses or reputation risks if the service is not available due to a denial of service attack.

A contracting party may require that the other contracting party plans its technical and organisation procedures to maintain information security in correct proportion to the severity and likelihood of threats, the costs arising from the actions and the available technical abilities to prevent threats.

When assessing the severity of a threat, at least the following must be considered:

- Nature of the data being protected (requirements for the processing of personal data or the management of certificate keys, for example)
- Criticality of the function being protected for the integrity of the system
- Magnitude of any personal data breaches or financial damage in case the threat is realised

When assessing the probability of a threat, at least the following must be considered:

- Latest information on information security threats targeted to online services
- and their platform infrastructure

It is recommended that the threat analysis be based on a frame of reference in accordance with a general standard.

2.2.4 Standards and recommendations

The regulations on the opening of interfaces in the Act on Transport Services do not include any references to standards. Therefore, standards are not mandatory and there is no specific standard that would set the statutory level of information security.

Standards describe general good information security practices, however. The parties can use standards in their own operations and agreements, as well as when determining the preliminary criteria for the opening of an interface to act on someone else's behalf.

The first version of the code of practice on the opening of a single ticket sales interface includes as an appendix a recommendation prepared during the Lippu project on secure implementation of the interface (publication 004/207 J APPENDIX 2, *LIPPU-API: Security Considerations).* The recommendation is based on general good practices and sources, as well as a threat analysis.

The recommendation also applies to the opening of an interface to act on someone else's behalf. The acting on someone else's behalf expands the information security requirements because personal data is processed, for example, which is why the information security recommendation has been supplemented with informative references to useful standards. (APPENDIX

LIPPU-API: Security Considerations. ADDITION 2018: informative list of standards, specifications or frameworks)

2.3 Reliability of authentication

2.3.1 Regulations

Part III, chapter 4, section 2 a of the Act on Transport Services includes general regulations on verifying identity when acting on someone else's behalf.

According to the Act, *verifying the identity in a particularly reliable way must be possible when a relationship with a party acting on someone else's behalf is established or substantially changed. It must also be possible to verify the identity in conjunction with a transaction on someone else's behalf.*

2.3.2 Need for authentication in travel chains and when acting on someone else's behalf

The contracting parties must assess whether passengers need to be authenticated so that their identity is verified and tied to the travel chain at some point during the travel chain. The contracting parties in acting on someone else's behalf must assess, on the basis of the need to protect the personal data processed and the need to maintain the reliability of the user account, whether identification and linking of user accounts will suffice or whether there is a need to authenticate the user. The contracting parties must agree which procedures they will use to identify the users, to verify their identity and to link the authorisations given by the users to the user accounts.

The leading principle is that no personal data should be unnecessarily processed. This also applies to the identification of passengers.

Passengers can be electronically identified or identified on site when they use services/enter a mode of transport if this is necessary for the provision of the services (and grounds for the processing of personal data exist as specified in the GDPR).

The parties can use the report on the processing of personal data to assess to which extent the passengers will be able to complete the travel chain fully anonymously when viewed from the viewpoint of the processing of personal data. It is likely that completely anonymous acquisition and use of the travel chain will only be possible if a passenger pays in cash.

Generally speaking, the need to identify a person in connection with a transport service can arise in the following cases:

- If a discount is offered on the basis of identity
- In the case of personal ticket products/season tickets
- Some modes of transport set requirements for the authentication of passengers (the verification of identity)

The minimum product in accordance with the obligation to open up a sales interface as set out in the Act on Transport Services **does not include any of the aforementioned reasons to identify passengers**. However, passengers may be identified expressly or indirectly for practical reasons or needs related to the acquisition of use of a travel chain.

- This authentication is not necessarily related to the passenger as such. It may be related to, for instance, an electronic payment method with which the passenger or another person pays for the trip.
- The authentication may also be related to the identifier that is used when the travel authorisation is verified onboard the vehicle. The identifier is not necessarily tied to a specific person but to the holder of the identifier.
- If identity is tied to the travel chain, it is also significant when a person is tied to the travel chain. Identity can be verified from a personal ID card during travel, for example.
- In the case of complaints or compensation, it must be possible to reliably link a passenger demanding compensation to the travel chain for which they demand compensation.

In the case of acting on someone else's behalf, the need for authentication may arise for the following reasons:

- The party acting on someone else's behalf and the party obligated to open up its API agree that the party acting on someone else's behalf can use a user account maintained by the party obligated to open up its API as an authorised user. Both parties must link the authorisation with the correct user account and the same person.
- The party acting on someone else's behalf uses a user account that is linked to a specific person on behalf of the user. Only those entitled to process the personal data may have access to the personal data.
- The party acting on someone else's behalf purchases a product that is linked to a discount connected to the person or a special condition on behalf of the person. Only those entitled to process the personal data may have access to the personal data and only the person entitled to use the products may use them.

The necessity to identify and verify identity can be assessed at the stages of user account management and acting on someone else's behalf that are listed below.

Stage	**Need to authenticate the identity of the user account holder**	**Need to verify that the acting party is the user account holder**	**Statutory requirement**

Party obligated to open up its API links an authorisation to a user account or the authorisation is modified/cancelled	Depends on the service and the content of the user account	Yes	Special care
Party acting on someone else's behalf links an authorisation to a user account or the authorisation is modified/cancelled	Depends on the service and the content of the user account	Yes	Special care
Communication between the party obligated to open up its API and the party acting on someone else's behalf on the creation, modification or cancellation of an authorisation	Depends on the services and the content of the user accounts	Both parties must be able to connect the data to the same user account	Special care
Acting on someone else's behalf	As above, no additional requirements	Both parties must be able to connect the data to the same user account	Care
External controller discloses personal data to the party obligated to open up its API and/or the party acting on someone else's behalf (the right to view the data is also considered such disclosure)	Depends on the personal data and the regulation of personal data, but in most likelihood sufficient verification that the personal data will be linked to the correct person's user account only and that the data will only be made available to the correct person or a party authorised to represent them (guardian, trustee, employer,	Both parties must be able to connect the data to the same user account	No special regulations in the Act on Transport Services

	etc.) is required		

2.3.3 Reliability of identification in electronic services in general

A variety of methods to identify users can be used in electronic services. The reliability of these methods varies.

Weak authentication

A service may create a username and password pair for the user based on personal data provided by the user. This is a case of weak authentication, because the only known fact will be that the party using the service is a party who has access to the username and password (or who has access to a terminal device in which the username and password have been saved). Personal data can be verified or authenticated from a variety of sources.

Strong authentication

Strong electronic authentication is based on always using two different types of authentication factors when identifying a person: something that the person knows (a PIN code, a password or a username, for example), something that the person has in their possession (identification number device, list of PIN numbers, mobile device) or a characteristic of the person (fingerprint or other biometric factor). Strong authentication also requires reliable linking of the authentication factors with the correct person when creating the means of authentication, i.e. verifying the person's identity using a reliable source and reliably linking the means of authentication to the specific person and only handing over the means of authentication to this person. The authentication method must also be fully secure.

In Finland, all methods that have been announced and accepted to a register maintained by the Finnish Communications Regulatory Authority in compliance with the Act on Strong Electronic Identification and Electronic Signatures (617/2009) are accepted as forms of strong electronic authentication. There are regulations on the authentication to be used in payment services in regulations on payment services.

Strong electronic authentication methods include online banking credentials, mobile certificates and identification certificates by the Population Register Centre in ID cards granted by the police. In addition to banks and mobile operators, strong electronic authentication for online services is offered by identification broker services listed in the register maintained by the Finnish Communications Regulatory Authority.

2.3.4 Identification when acting on someone else's behalf

The reliability of the identification of the user when acting on someone else's behalf can be assessed on three levels:

1) Identification of the user account. The user account is separated from other user accounts with a unique identifier and it is ensured that the party/person using the service is the correct user account, but identity or the person using the account is not verified.

2) Identification of the party to the user account. It is ensured that the correct user and the same party that issued the authorisation is the party to the service, but the identity or the person using the account is not verified.

3) Identification of the user as a person. In addition to the above, the user's identity is verified by means of strong electronic authentication or another method that has been deemed sufficient.

According to the Act on Transport Services, the verification of identity must be done with care or with special care.

The justification for the Act states that the Act does not require the use of strong electronic identification in the case of acting on someone else's behalf. Other regulations may pose other requirements for authentication, however. The justification offers the regulation of payment services as an example.

In the case of the **own online service** of a mobility service or an integrated mobility service, the provider of the mobility service or integrated mobility service must assess, based on their own starting point, the need to verify their customer's identity and the reliability requirements of the authentication to be used in the service. **In other words, the provider of the mobility service or integrated mobility service must assess from the perspective of their own service and their own obligations how important is it to ensure that the user has announced/will announce their actual/own personal data.** If strong electronic authentication is not used, the procedure can also include a one-time or recurring confirmation by email or text message in addition to the user giving their personal data.

When sufficiently reliable linking of the user accounts of **two parties** is necessary in the case of acting on someone else's behalf, the party obligated to open up its API and the party acting on someone else's behalf must agree on which method and which personal data are sufficient for the acting on someone else's behalf. **In other words, the party obligated to open up its API and the party acting on someone else's behalf must assess together how they can verify, in a sufficiently reliable manner, that they are actually processing the user accounts and personal data of the same person.** Also in this respect, the objective of the Act on Transport Services to provide user-friendly services and the principle of minimising the processing of personal data in the GDPR should also be taken into account in the case of acting on someone else's behalf.

If the contracting parties do not use or one of the contracting parties does not use strong electronic authentication, the contracting parties can agree on which personal data (name, address, email, telephone, date of birth, etc.) will be compared when linking the authorisation to a user account, **i.e. which data the parties will use to ensure that they are processing the data of the same person.**

If the authorisation applies to more than a single time of using the service on someone else's behalf, the contracting parties must agree, in addition to identifying the user account and user, which data (such as user account number or another type of pseudonym) will be used in the technical aspects of the acting on someone else's behalf when the party acting on

someone else's behalf uses the service of the party obligated to open up its API on behalf of a user.

2.4 Summary of the information security and data protection requirements when opening a sales interface

Party obligated to open up its API refers to the mobility service or integrated mobility service or the service provider that provides a ticket and payment system on behalf of the mobility service or integrated mobility service, which is the party that must, by law, offer access to the single ticket sales interface.

Contracting parties refers to the party obligated to open up its API and the mobility service that acquires products through the sales interface.

- The party obligated to open up its API must ensure that the opening can take place without compromising the service's information security or privacy protection.
- A contracting party may require that the other party applies good information security practices in proportion to the risks to data connections related to the sales interface of the ticket and payment system and to its own systems that have an impact on the data connections of the sales interface or the information security of data obtained through it.

2.5 Summary of the information security and data protection requirements when acting on someone else's behalf

The list below includes a general description of the information security and personal data protection requirements when acting on someone else's behalf.

Party acting on someone else's behalf refers to the mobility or integrated mobility service that has been authorised by a user to use the user's account in another mobility or integrated mobility service.

Party obligated to open up its API refers to the mobility service or integrated mobility service or the service provider that provides a ticket and payment system on behalf of the mobility service or integrated mobility service, which is the party that must, by law, offer access to the user account or another form of electronic service.

- The party acting on someone else's behalf can access the user account using the interface or credentials of the user/the party acting on someone else's behalf that the party obligated to open up its API provides them as the party maintaining the user account and on which an agreement is made when opening the connection.
- The use of the service on someone else's behalf is initiated by the user.
- The party acting on someone else's behalf and the party obligated to open up its API must both do the following:
  - Use good information security practices proportional to the risks when processing the data in their data systems

- Use good information security practices proportional to the risks when transferring data
- Ensure that the user's personal data is processed in a secure manner
- Ensure that only the personal data needed to complete the acting on someone else's behalf is processed
- Ensure that the contracting parties' business secrets, cryptographic secrets or any other data required to open the user account when acting on someone else's behalf are processed in a secure manner and are used only for the agreed purpose
- Save the data required to authenticate the acting on someone else's behalf and retain it for the period needed to investigate any disturbances or complete any similar actions

- The party acting on someone else's behalf must do the following:
  - Identify itself to the party obligated to open up its API that maintains the user account in the manner agreed when opening the connection
  - Ensure that the user's credentials and other personal data are only made available to the user and the party obligated to open up its API

2.6 Information security issues to be agreed

This section offers a checklist of issues related to information security that should be agreed upon. Such issues include the following:
- ✓ Information security in the storage of data
- ✓ Information security in the transfer of data
- ✓ Procedure regarding modifications of the system, interface and requirements
- ✓ Handling of incidents and threats related to the interface or system
- ✓ Confidentiality of incident, modification and event information
- ✓ Procedure to ensure information security/reliability of the contracting parties

The contracting parties should demand at least the following from one another:

- Information security in the storage of data
  - Classification of data and access rights
  - Encryption and protection of data in accordance with a mutual agreement
  - Logs for processed data, where applicable
  - Tracing of data processing and transfer of data from the system down to the person who performed the action
- Information security in the transfer of data
  - System zones – sufficient separation of the interface and background systems
  - Identification of the parties

        - Certificates, the interface can only be accessed from pre-defined IP addresses
        - TLS level authentication for the network interface or another similar procedure; whenever possible, both parties to network traffic should be authenticated using certificates (client and server certificates) that are exchanged before the start of operations
        - Exchange and management of certificates
    - Data transfer: protocol requirements, encryption
- Procedure regarding modifications of the system, interface and requirements
    - Informing the other contracting party in good time
- Handling of incidents and threats related to the interface or system
    - Observation ability
        - For example, the ability to monitor logs and detect non-conformances, the ability to detect and produce triggers at least regarding deviations in typical transaction quantities or corresponding estimated threshold values
    - Communication between the contracting parties and a procedure regarding information security non-conformances
        - Appointing a contact person for incidents. Both parties should appoint a contact person whom the other contracting party can contact in the case of an information security problem.
        - Communication channels and communication times. The level of information security in the communication channels should be high in proportion to the information being transmitted.
        - The contracting parties should agree on communicating information security threats and incidents to allow other mobility service network operators to anticipate such situations and take the necessary preparatory or corrective actions. For example, the threshold for communicating information security threats, such as software vulnerabilities, ongoing phishing campaigns or DoS attacks, should be fairly low to allow other contracting parties or mobility service network operators to anticipate the situation.
        - Cooperation in the investigation of incidents
        - Closing the interface or a part thereof as a temporary security measure, if necessary
    - Communication between the contracting parties and a procedure for anticipated or unanticipated maintenance interruptions or malfunctions in the interface/related services.

- Communication is necessary at least when the incident will affect the services of the contracting parties.

- Confidentiality of incident, modification and event information
    - The contracting parties do not have the right to disclose any confidential information they have obtained on the basis of an agreement to any third parties.
    - The contracting parties can agree upon communicating any incidents to third parties or the public on behalf of each other.

Mutual secrecy of the contracting parties must not adversely affect consumers' right to obtain information about to whom they should turn to in order to invoke their legal rights.

- Procedure to ensure information security/reliability of the contracting parties
    - In the case of acting on someone else's behalf, the procedure and the proving of reliability are determined in assessment criteria and conditions prepared by the party obligated to open up its API; see Section 3.3. below.
    - Recommended procedures for the opening of a single ticket sales interface are discussed below in Section 3.2.
    - In both cases and when opening interfaces in general, the following good practices can be used:
    - Evidence that information security in the application used to carry out the service and in the application platform has been verified by means that are sufficient in proportion to the risks. This can include the following:
        - An application penetration test report or a similar document that indicates that the contracting party has tested the information security of its application or commissioned such a test
        - Approvals or information security certifications of the service provider (e.g. cloud service provider) of the application's server platform
        - The aforementioned should always be easily available so that compliance with the obligations can be verified as easily as possible.

3 Verifying information security of contracting parties

3.1 Regulations and oversight

Part III, chapter 2, section 4 of the Act on Transport Services includes regulations on the information security and data protection requirements when opening an interface and on the access conditions.

Section 2 a in the same chapter includes regulations on the right of the party obligated to open up its API to *assess in the connection with acting on someone else's behalf the reliability of the mobility service or integrated mobility service provider using predetermined assessment criteria and conditions*.

The Finnish Transport and Communications Agency Traficom bears the responsibility for the oversight of compliance with the Act on Transport Services, and thus also compliance with the assessment criteria and the conditions.

3.2 Single ticket sales interface

A contracting party can require from the other party that they agree upon a procedure with which they can verify that sufficient level of information security is maintained.

A recommended and reasonable procedure is to define thorough requirements in the agreement and perform a technical test on all interfaces open towards the internet.

Possible procedures include:

- Information security requirements are defined and their fulfilment is documented in a written agreement.
- A technical test is performed for all network interfaces of the parties' systems open towards the internet by an independent evaluator, or by the concerned party itself if it can show evidence of the tester's professional expertise. Any interfaces opened through subcontractors must be taken into account in the test. The other contracting party must be notified of the testing results.
    - See APPENDIX *LIPPU-API: Security Considerations* for information on selecting suitable self-testing tools and methods.
- An independent audit of the information security of the contracting party's entire system must be conducted (including network interface testing). If the threat level is high, a standard (e.g. ISO 27001) certification of information security is required.
- The contracting parties have the right to audit the information security of the other party's system.

A recommended and reasonable procedure is to at least define thorough requirements in the agreement and perform a technical test for interfaces open towards the internet.

Demanding an independent audit or certification of the entire system simply for the sake of opening up the sales interface is not considered reasonable. If a contracting party performs an audit, the protection of trade and professional secrets and personal data must be considered. Procedures heavier than these can be used if they are otherwise used by the parties for business purposes.

3.3 Duties of the contracting parties at the different stages of opening a connection for acting on someone else's behalf

1) Before opening the connection

Party obligated to open up its API

- Identifies the personal data and other data content, as well as the information security features related to the provided user account or another method of electronic service and its own certificates and other information security evidence
- Prepares a description of the interface or another method of access to the provided user account or another method of electronic service
- Prepares the assessment criteria and conditions for the party acting on someone else's behalf, i.e. the user of the interface or another method of access

Party acting on someone else's behalf

- Prepares a description of its information security and its processing of personal data

2) When access is requested

Party obligated to open up its API

- Publishes or delivers the description of the interface or another method of access and the predetermined assessment criteria and conditions to the party requesting access
- Reviews the information security and personal data processing report of the party requesting access
- If necessary, conducts negotiations with the party requesting access on the information security evidence of the party requesting access or reconciliation of the systems
- Agrees upon procedures to be applied in case of modifications or incidents

Party acting on someone else's behalf

- Submits a report on its information security and the processing of personal data to the party obligated to open up its API
- If necessary, conducts negotiations with the party obligated to open up its API on the information security evidence or reconciliation of the systems

- Agrees upon procedures to be applied in case of modifications or incidents

3) At the production stage

Party obligated to open up its API and party acting on someone else's behalf

- Inform each other of any incidents
- Inform each other of any modifications
- Investigate incidents together as necessary
- If necessary, discontinue the use of the interface or another method of access as specified in the agreement

3.4 Predetermined criteria and conditions of the party obligated to open up its API

The party obligated to open up its API must prepare assessment criteria and conditions for the party acting on someone else's behalf.

The party obligated to open up its API should publish the assessment criteria and conditions on its website, for example. If the party obligated to open up its API does not publish the information, it must deliver the information without delay after the party acting on someone else's behalf has requested opening of the access.

By law, the assessment criteria and conditions must be fair, reasonable and non-discriminatory, and they may not include any conditions that limit use.

In light of the statutory fairness, reasonableness and non-discrimination requirement, the party obligated to open up its API must consider in the criteria its own corresponding evidence on reliability. These cannot be used as the minimum requirements, however. The requirements on the authentication of users by the party requesting access must also be fairly proportioned to the authentication ability and practices of the party obligated to open up its API and the necessity to verify the identity of users.

The assessment criteria and conditions must include at least the following:

1) A description of the reasonable information security practice requirements for the contractual party in different system sectors

   - Justification for the requirements and any references to standards divided on the basis of the classification used in this background study, for example (see Section 2.2.2).

   - A description of the methods the party requesting access can use to meet or prove the reliability of the authentication of the user account or the user account holder. Particular attention must be paid to whether verification of identity is necessary or whether mere identification of the user account suffices.

2) A description of the methods that the party requesting access can use to prove that they meet the reasonable information security requirements

as laid down in point 1 and the statutory requirements on the processing of personal data

- A description of licences, approvals, audits or certificates granted by an authority or a third party authorised by an authority on the basis of which the party acting on someone else's behalf prove its reliability.
- A description of any other procedures with which the party acting on someone else's behalf can prove that its operations comply with a generally approved standard or generally approved conditions of the industry and that the party acting on someone else's behalf can use to prove its reliability. A description to which extent proving compliance with the General Data Protection Regulation suffices should be included.
- A description of how the party acting on someone else's behalf can prove compliance with the requirements if it cannot provide the evidence specified in points 2 and 3.

3) A description of the methods the party requesting access can use to prove compliance with the other reliability requirements that can be related to the following, for example:
   - Submission of the notification laid down in the Act on Transport Services if the party acting on someone else's behalf is a brokering and dispatch service (part III, chapter 5, section 1)
   - Registrations or public sources of information regarding legal capacity or eligibility for business
   - Any obstacles caused by international sanctions
4) Any other conditions necessary for the interface or access related to supporting services, terms of use, software, licences or other required services
5) A description of what kind of authorisation procedures the party obligated to open up its API supports in the case of acting on someone else's behalf
   - For example, whether the party obligated to open up its API will obtain the authorisation from the user itself or whether the party obligated to open up its API will accept a notification by the party acting on someone else's behalf on the party acting on someone else's behalf having obtained the authorisation.

FICORA
www.viestintävirasto.fi