Issued:	Entry into force:	Validity:
25 October 2022	27 October 2022	until further notice

Legal basis:
Act on Electronic Communications Services (917/2014), sections 145, 243, 247, 303 and 304

Modification details:
Replaces Finnish Communications Regulatory Authority (FICORA) Recommendation 308/2004 S on recording information on identification data processing

Finnish Transport and Communications Agency (Traficom) instruction on recording information on traffic data processing

Content

1 Background and purpose of the instruction

This instruction applies to the recording and storing of event information related to the processing of traffic data (hereinafter referred to as a processing log). Section 145, subsection 1 of the Act on Electronic Communications Services (917/2014, as amended by Act 1003/2018) stipulates the following:

> A communications provider shall record detailed event information on processing of traffic data in data systems containing traffic data essential to confidentiality and protection of privacy, if this is technically feasible without unreasonable cost. This event information must show the time and duration of the processing and the person performing the processing. The event information shall be stored for two years from the date on which it was recorded.

According to subsection 2 of said section, the Finnish Transport and Communications Agency (Traficom) may issue further regulations on the technical implementation of the recording and storing referred to in subsection 1. Instead of a regulation, Traficom issues this instruction. This instruction replaces Finnish Communications Regulatory Authority (FICORA) Recommendation 308/2004 published in 2004. This instruction takes into account the legislative changes and technical development that have since taken place.

Section 145 of the Act on Electronic Communications Services largely corresponds to the provision previously in force. Before the Act on Electronic Communications Services entered into force, the recording of a processing log was stipulated in section 15 of the Act on the Protection of Privacy in Electronic Communications (516/2004). This, however, only applied to telecommunications operators. As a result of section 145 of the Act on Electronic Communications Services entering into force, the obligation to record a processing log was expanded from telecommunications operators to cover all communications providers. At the same time, an exception was provided. The government proposal for the Act on the Protection of Privacy in Electronic Communications (HE 125/2003 vp) states that a recording obligation is necessary in order to investigate any misuse in cases where people employed by a telecommunications operator are suspected of having processed identification data (now traffic data) related to confidential communications for a purpose other than those provided for in the legislation. At the same time, the recorded information on processing can be used as needed to prove that no suspected misuse has taken place, which has a positive impact on the legal protection of the people performing the processing. Traficom may also request to inspect a processing log or other log data in cases related to the monitoring of compliance with provisions concerning the processing of traffic data (section 315 and section 316, subsection 2 of the Act on Electronic Communications Services).

This instruction does not apply to the issue of which original traffic data should be recorded in a log. This instruction also does not provide general instructions on the recording of log data, but deals with the specific characteristics of the obligation set in section 145 of the Act on Electronic Communications Services. Other obligations related to the recording of log data may be entailed e.g. by the EU's General Data Protection Regulation (EU) 2016/679 and the Act on Information Management in Public Administration (906/2019).[1]

[1] For more information, see e.g. the National Cyber Security Centre Finland at the Finnish Transport and Communications Agency Traficom instructions Collecting and using log data; the Office of the Data Protection Ombudsman press release The obligation to document personal data breaches also includes log data; and the Information Management Board's collection of recommendations on the application of certain information security regulations (in Finnish).

2 Application of the event information recording obligation

1. A communications provider shall **identify and define the traffic data management processes and data systems**, the data contained in which has an immediate and essential significance to the confidentiality of communications. A communications provider must implement the recording of a processing log on the processing of traffic data for these data systems.

The detailed rationale for section 145 of the Act on Electronic Communications Services specifies what the provision means by data systems containing essential traffic data (HE 221/2013 vp, p. 154–155):

> Communications providers shall define the traffic data management processes and systems, the data contained in which has an immediate and essential significance to the confidentiality of communications, and implement the recording of information on the processing of traffic data (log data) for them.
>
> These [data systems containing essential traffic data] include systems where traffic data is stored not only for a short period of time, where traffic data is processed by natural persons and where traffic data processing events can be performed on the communications event or events of a specific communicating party. Such systems include e.g. ticket repositories, invoicing systems and various systems used to analyse historical data on communications events.

The logging obligation pursuant to section 145 of the Act on Electronic Communications Services arises when the processing of traffic data is carried out *by natural persons* and the processing events *are performed on the communications of a specific (identifiable) communicating party*. In the case of corporate or association subscribers, the processing of traffic data subject to the recording obligation takes place in connection with managing email systems in particular. The logging obligation only applies to electronic data systems.

The logging obligation pursuant to section 145 of the Act on Electronic Communications Services **does not apply to**

- systems other than those containing "essential traffic data"; such other system may be a switch or router or other system where traffic data is stored only for a very short period of time and where traffic data is processed manually only in exceptional cases, e.g. for troubleshooting purposes
- systems where the processing of traffic data only takes place automatically (e.g. transfer of traffic data between different systems)
- other than electronic datasets (e.g. the processing of paper printouts)
- the processing of anonymous and/or summarised datasets, such as the further processing of a statistical analysis generated by automatic data processing under section 142 of the Act on Electronic Communications Services.

Section 145 of the Act on Electronic Communications Services does not lay down a logging obligation for **providers of a value-added service**[2]. However, in the same manner as a communications provider, a provider of a value-added service must maintain the information security of their services (section 247, subsection 2 of the Act on Electronic Communications Services), which may also entail recording appropriate log

[2] According to section 3, subsection 10 of the Act on Electronic Communications Services, a value-added service means a service based on the processing of traffic data or location data for a purpose other than conveyance of a communication.

data. **Traficom recommends** that providers of a value-added service implement logging corresponding to section 145 of the Act on Electronic Communications Services when traffic data essential to the confidentiality of communications is processed by natural persons in their operations.

2. A communications provider shall **determine the log data to be recorded**.

According to section 145 of the Act on Electronic Communications Services, "detailed event information" on the processing of traffic data shall be recorded, showing at least "the time and duration of the processing and the person performing the processing." The information to be recorded is usually contained in a so-called access log or other audit log.

In addition to information listed separately in the Act, information must naturally also be recorded of *what traffic data has been processed and where this data was stored*. Processing means the same as in the GDPR, including e.g. any retrieval, use and alteration of traffic data.

- It depends on the case whether it is appropriate to record in the processing log the traffic data that has been processed or whether it can be otherwise ensured that the log can be used to determine what traffic data has been processed. According to section 137, subsection 1 of the Act on Electronic Communications Services, similarly to the data minimisation principle of the GDPR, the processing of traffic data is only allowed to the extent necessary for the purpose of such processing, and it may not limit the confidentiality of messages or the protection of privacy any more than is necessary. This means that the traffic data recorded in the processing log should be minimised. Recording the criteria used for retrieving the traffic data in the processing log may be sufficient, if it can be used later to reliably determine what data has been processed.

- Depending on the case, the recording of event information other than those specifically mentioned in the Act may also be necessary (e.g. what was the processing event in question, was it successful, and what was the status of the processed data before and after the event).

Of the person performing the processing, being a natural person, identifiers and information on the authorisation and the source (device, source address) of the function shall be recorded.

The time of the processing refers to recording the timestamp of the event. The correctness of the time must be ensured. The UTC format is recommended.

Specific situations related to recording *the duration of the processing* are discussed in section 3.3 below.

Section 145 of the Act on Electronic Communications Services does not specifically require the recording of the *purpose of use* for the processing of traffic data. However, recording this information is recommended if doubt on the basis for processing may arise.

3. A communications provider may **deviate from the logging obligation** if the recording of event information is not technically feasible without unreasonable cost. The application of this exception requires not only that at the time of assessment, a specific data system does not technically support the recording of event information, but also that *developing or replacing the system with one that supports processing logging would cause the communications provider unreasonable cost*.

The unreasonable nature of costs may be assessed in relation to how essential the processing in question is for the confidentiality of traffic data and the protection of privacy, considering the scope of processing, processed data types and what other measures are being used to ensure the confidentiality of traffic data and the protection of privacy. When assessing the unreasonable nature of costs, among other factors, the share of the costs caused by the processing log out of the overall costs of operations may be taken into account, especially with regard to small-scale operations. The assessment of the unreasonable nature of costs may also take into account e.g. the size of the company, scope of operations and the turnover of the telecommunications operations of a telecommunications operator or, in case of other companies, of the business operations to which the transmission of communications is connected.

Instead of excepting the implementation of the logging obligation in its entirety, the exception may also be applied to the recording of individual event information types. The duration of the processing can be left unrecorded, for example, if the recording is technically infeasible. However, if the recording of other event information is technically feasible without unreasonable cost, they must be recorded in full.

Chapter 3 provides examples of situations where the implementation of the logging obligation fully or for some data types is not necessarily technically feasible at all or not without unreasonable cost.

Should a communications provider deviate from the logging obligation, the grounds for the deviation and the description of technical limitations should be documented in order to provide necessary justification to the supervisory authority as necessary.

4. A communications provider shall **store the processing log data for a minimum of two years from the date on which it was recorded**.

Section 145 of the Act on Electronic Communications Services only stipulates on the minimum duration. A communications provider may determine a longer period on a case-by-case basis, as long as it complies with other applicable law, such as personal data legislation. If the processing log contains traffic data, the processing of the traffic data must comply with section 137 of the Act on Electronic Communications Services.

Especially for authorities acting as communications providers, the retention period for the processing log data could justifiably be set at a minimum of five years due to the statute of limitations in criminal law.[3]

A communications provider must naturally **ensure that the logging is implemented as defined**.

5. A communications provider must **maintain the information security of the processing log**.

According to section 247 of the Act on Electronic Communications Services, when transmitting messages, communications providers must maintain the information security of their services, communications, traffic data and location data. However, corporate or association subscribers as communications providers are responsible for maintaining information security of communications, traffic data and location data of their users only. The information security measures must be commensurate with the seriousness of threats, level of technical development to defend against the threat and costs incurred by these measures.

[3] The Information Management Board's collection of recommendations on the application of certain information security regulations (in Finnish), p. 77.

- According to section 4 of the Finnish Communications Regulatory Authority (FICORA) Regulation 67 A/2015 on the information security of telecommunications operations, a telecommunications operator is responsible for taking into account, among other factors, dataset and operational security, which also includes the prevention of unauthorised access to the log data related to telecommunications operations (memorandum on the explanations and application of the regulation, p. 14). A telecommunications operator must document its measures. Although the explanatory notes for the regulation only mention as specific examples the customers' billing, subscriber and log data, the logs generated of the processing of said data can also be viewed as being within the scope of the regulation. The need to clarify the regulation is taken into account in the ongoing project to update it.

- A communications provider must draw up sufficiently detailed instructions for its staff on the processing of traffic data for different purposes.

A communications provider must ensure e.g. the following measures:

- The processing log must be recorded in an information secure manner. The integrity of the log data, in particular, must be ensured. The obligations related to protecting log data must be in proportion to the risks of the operations. The scope of the obligations also depends on whether or not the provider is a telecommunications operator.

- The processing log data must be available within a reasonable time. The log data shall also be backed up as possible.

- The processing log data monitoring, analysis and automated alerts of security incidents related to log processing must be defined in the appropriate scope.

6. Furthermore, a communications provider must meet **the obligations set in other legislation when recording a processing log**.

A communications provider must take into account requirements of legislation on the processing of personal data (such as the GDPR and the Data Protection Act (1050/2018)) if the processing log contains personal data. If necessary, a communications provider must take into account any need for a co-operation procedure in accordance with the Act on the Protection of Privacy in Working Life (759/2004). In collecting log data, an authority must also comply with section 17 of the Act on Information Management in Public Administration that may set stricter requirements than section 145 of the Act on Electronic Communications Services.

3 Challenges related to the recording of log data on traffic data processing

3.1 Systems that do not support the recording of information on the processing of traffic data or that no longer receive product support from the manufacturer

Some data systems still used by communications providers do not support the recording of information on the processing of traffic data. Building such a functionality into these systems may not be possible with reasonable cost, even when the manufacturer's product support is nominally available. The manufacturer's product support has already expired for some systems, meaning that new features are no longer available for such systems. Updating such systems with new systems may cause unreasonable cost.

Communications providers also use active devices (routers, exchanges, switches, etc.) that are not intended to record information on the processing of traffic data, nor is such a functionality available for these systems.

Communications providers may also transfer traffic data for further processing into some offline or remote system that does not support the recording of information on the processing of traffic data. Such systems include e.g. applications where traffic data is processed, run locally on workstations.

The exception to the obligation to record log data may be applicable in the above-mentioned situations. However, at least for telecommunications operators, the number of such systems and devices is estimated to be significantly smaller than in 2004 when the logging obligation for telecommunications operators first entered into force. However, the number of providers and systems falling within the scope of the logging obligation has grown due to the widening of the scope of application, in addition to which the use of cloud services may cause new challenges (see 3.5). The technical competence for implementing the logging among providers covered by the scope of the obligation may also vary e.g. due to the size of the provider and available resources.

3.2 System and log data fragmentation and real-time log data

Due to the complex structure of communications networks, information describing the processing of traffic data is recorded in many fragmented systems in connection with the processing of traffic data. This means that the processing of individual traffic data does not necessarily generate real-time event information, but instead this information can be generated later by combining log data contained in several different systems. However, combining log data retroactively is not always possible.

In some situations, traffic data is transferred along a system chain from the original system that created the traffic data through a mediation system into a collection system where the actual processing of traffic data takes place. The upstream systems are typically not intended to process traffic data but only to transfer the data forward into a collection system. In such cases, implementing the obligation to record information on the processing of traffic data may be technically challenging.

In a situation where traffic data is distributed between several systems, it must first be assessed whether the data contained in an individual system constitute *essential* traffic data as referred to in the legislation. Secondly, if there is a need to assess the unreasonable nature of costs caused by processing logging in a chain of separate systems, the scope of logging as a whole, other controls related to the processing of traffic data and the risks related to the fact that full-scale logging cannot be implemented for the mediation system must be taken into account.

3.3 Availability of the duration of the processing in specific situations

In systems where the duration of the processing cannot be accurately determined, the communications provider must aim to arrange recording of log data in a way that allows the estimated duration of the processing to be deduced from event timestamps. Recording information on the duration of the processing of traffic data can become challenging e.g. in cases where a customer service agent or invoicing specialist processes traffic data on a screen, e.g. in a browser. In such cases, the data may stay up on the screen for a much longer period than the actual processing of traffic data lasts. Even in such cases, it is typically possible to record at least the opening of the processing view and any sign-out or session time-out.

It is also possible that traffic data is transferred for further processing to an offline system (e.g. a laptop) where the duration of the processing of traffic data cannot be

recorded using technical means. Traffic data can sometimes be printed on paper for continued processing, in which case the information on the processing of paper material cannot be recorded using IT measures; as stated before, the logging obligation only applies to the processing of traffic data in data systems. In the cases mentioned here, however, other event information on the transfer of traffic data into another system or on their printing must be recorded.

3.4 Administrator accounts and console use

Data systems usually have administrator accounts activated and available for system administration purposes. These administrator accounts can vary in type: the account can be a personal one, a shared account known to a small group of people, a device's local root/admin-type non-personal administrator account or a last resort account used for system restoration.

In cases where administrator accounts cannot be made personal and where tracing measures cannot be implemented reasonably with a jump host or other arrangements, the measures carried out with said accounts cannot be allocated to an individual person by using technical means. Administrator accounts also usually offer the option of editing information in the local system describing the processing of traffic data retroactively, thus covering tracks of any unlawful processing. These risks can be reduced by ensuring that non-personal accounts are used only when it is absolutely necessary, and that even in these cases the account credentials are known to as small a group of people as possible, and by using a separate system for collecting the processing log.

Console connections are needed e.g. when a system breaks down and remote control is not possible, or when a system requires configuration changes that apply to the active devices directly. When using console connections, the operating typically takes place with a device's local administrator account directly next to the device, which can make the recording of information describing the processing of traffic data impossible in such cases.

3.5 Use of cloud services and retention period for the processing log

Corporate or association subscribers or other communications providers may use cloud service providers (so-called corporate or association subscriber subcontractors) working on their behalf in implementing their email system, for example. The obligation to record event information applies to communications providers in these cases as well. When using cloud services, it is necessary to establish the extent to which the practical implementation of the processing log is the responsibility of the cloud service provider as the subcontractor of the communications provider or the responsibility of the communications provider who is legally responsible for the storage of the processing log. However, cloud services do not always offer the option of recording log data within the service itself for a period of two years, at least not without an additional charge or separate technical solutions for the storage of log data.

The commercial practice of a cloud service provider does not provide justified grounds for appealing to the exception to the obligation to record a processing log, as the recording of log data in contemporary cloud services cannot be normally considered technically infeasible, nor does the implementation of logging cause unusual costs. A corporate or association subscriber using the service may often have different technical means for recording log data available to them. In addition to acquiring a service for an additional charge, a corporate or association subscriber may have the option of either transferring log data from the service to a separate file or saving the data via an interface for storage in the longer term in their own systems. The statutory retention period must also be taken into account when terminating the use of a cloud service.