*English is not an official language of the Swiss Confederation. This translation is provided for information purposes only and has no legal force.*

# Ordinance on the Surveillance of Post and Telecommunications (SPTO)

of 15 November 2017 (Status as of 1 January 2024)

*The Swiss Federal Council,*

based on the Federal Act of 18 March 2016[1] on the Surveillance of Post and Telecommunications (SPTA),
on Articles 269bis paragraph 2, 269ter paragraph 4 and 445 of the Criminal Procedure Code (CrimPC)[2]
and on Articles 70bis paragraph 2, 70ter paragraph 4 and 218 of the Military Criminal Procedure Code of 23 March 1979[3] (MCPC),

*ordains:*

## Chapter 1 General Provisions

### Section 1 Introduction

**Art. 1** Subject matter and scope of application

[1] This Ordinance regulates the organisational aspects of and procedure for the surveillance of post and telecommunications and for the provision of information on postal and telecommunications services.[4]

[2] It applies to:

a. ordering authorities and the authorities directing proceedings;

b. approval authorities;

c. federal, cantonal and communal police forces;

d. the Federal Intelligence Service (FIS);

e. the State Secretariat for Economic Affairs (SECO);

f. federal and cantonal authorities competent to deal with administrative criminal cases;

AS **2018** 117

1 SR **780.1**
2 SR **312.0**
3 SR **322.1**
4 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

g. the Post and Telecommunications Surveillance Service (PTSS);

h. postal service providers (PSPs);

i. telecommunications service providers (TSPs);

j.[5] providers of derived communication services (PDCSs);

k. operators of internal telecommunications networks;

l. persons who allow third parties to use their access to a public telecommunications network;

m. professional retailers of cards and similar means of gaining access to a public telecommunications network.

**Art. 2** Terms and abbreviations

The terms and abbreviations used in this Ordinance are defined in the Annex.

## Section 2 Surveillance Order

**Art. 3**[6] Submissions to the PTSS

The ordering authority and the approval authority shall transmit surveillance orders and orders for their extension or termination, approvals and the access rights to be established to the PTSS as follows:

a. by means of a secure means of transmission authorised by the FDJP;

b. by letter, if the means of transmission in accordance with letter a is unavailable for technical reasons; or

c. by telephone in urgent cases, provided the surveillance order is submitted in accordance with letter a or b within 24 hours.

**Art. 4** Conduct of surveillance

[1] The PTSS shall determine in specific cases the technical and organisational measures for conducting surveillance, unless these are directly specified in the applicable regulations, in particular for standardised types of information and surveillance.

[2] If, as a result of operational problems, a person or entity required to cooperate is unable to meet its obligations for the surveillance of post or telecommunications, it shall report this to the PTSS without delay and thereafter submit a written statement of the reasons. The PTSS shall inform the person or entity required to cooperate without delay if surveillance cannot be carried out because of operational problems on its side.

[3] Irrespective of where the cause of the error lies, the person or entity required to cooperate must temporarily store at least the undelivered secondary telecommunications

5 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
6 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

data from real-time surveillance and deliver it without delay. If the secondary telecommunications data from real-time surveillance is no longer available or incomplete, the person or entity required to cooperate must deliver without delay the secondary telecommunications data from retroactive surveillance in accordance with the instructions of the PTSS.

**Art. 4*a***[7] Beginning and end of retroactive surveillance

[1] Retroactive surveillance begins no earlier than 6 months before the day on which the order is received by the PTSS, i.e. on the day whose date corresponds to the date of the day on which the order is received. If the date in question does not fall within the month in which monitoring begins, monitoring begins at the earliest on the last day of that month.

[2] It ends no later than the day on which the order is received by the PTSS.

**Art. 5** Protection of official or professional secrecy

If the PTSS establishes that the surveillance relates to a holder of official or professional secrets but that the statutory measures to protect these secrets have not been taken, it shall in the following situations notify the ordering authority and the approval authority without delay and initially shall not allow the former and the persons named in the surveillance order access to the surveillance data:

a. if surveillance has been ordered by a civilian prosecution authority: in the case of persons from the professional groups specified in Articles 170–173 CrimPC unless measures have been taken in accordance with Article 271 CrimPC;

b. if surveillance has been ordered by a military prosecution authority: in the case of persons from the professional groups specified in Article 75 letter b MCPC unless measures in accordance with Article 70*b* MCPC have been taken;

c. if surveillance has been ordered by the FIS: in the case of persons from the professional groups specified in Articles 171–173 CrimPC unless measures have been taken in accordance with Article 58 paragraph 3 of the Intelligence Service Act of 25 September 2015[8] in conjunction with Article 23 of the Intelligence Service Ordinance of 16 August 2017[9].

**Art. 6** Duty of confidentiality

The surveillance or the provision of information shall be carried out so that neither the person concerned nor unauthorised third parties are aware of it.

7 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
8 SR **121**
9 SR **121.1**

**Art. 7** Technical data sorting (filtering)

The PTSS shall at the request of the ordering authority carry out automated filtering if it is technically able to so and the cost and workload involved is not disproportionate.

**Art. 8** Recording telephone calls as evidence

[1] The PTSS shall record as evidence the telephone calls made in connection with its duties.

[2] Any evaluations of the recording shall be carried out by the data protection officer or the PTSS Data Protection Commissioner.[10]

[3] The PTTS shall retain the recorded telephone calls for two years and thereafter destroy the recordings.

**Art. 9** Surveillance file

[1] The PTSS shall open a file in the processing system for each surveillance order.

[2] The file contains all the documents on the case concerned, namely:

a. the surveillance order and its attachments;

b. the surveillance assignment or assignments issued to the relevant person or entity required to cooperate;

c. the confirmation or confirmations of when the assignment was issued to the person or entity required to cooperate;

d. the written acknowledgment from the person or entity required to cooperate that the surveillance assignment or assignments has or have been carried out;

e. the rulings from the approval authority on the approval or non-approval of the surveillance order together with any appeal decisions;

f. any extension orders and rulings from the approval authority;

g. the termination order;

h. the correspondence relating to the measure;

i. the protection measures specially ordered;

j. the accounting records.

[3] The surveillance data shall be stored in accordance with Article 11 SPTA and destroyed in accordance with Article 14 of the Ordinance of 15 November 2017[11] on the Processing System for the Surveillance of Post and Telecommunications (PSO-PTSS).

10 Amended by Annex 2 No II 85 of the Data Protection Ordinance of 31 Aug. 2022, in force since 1 Sept. 2023 (AS **2022** 568).

11 SR **780.12**

## Section 3 Working Hours and On-Call Arrangements

**Art. 10** Normal working hours and public holidays

[1] Normal working hours for the PTSS and the persons or entities required to cooperate are Monday to Friday continuously from 8am to 5pm.

[2] Normal working hours do not apply on public holidays. These are 1 and 2 January, Good Friday, Easter Monday, Ascension Day, Whit Monday, 1 August, 24 December from noon, 25 and 26 December and New Year's Eve (31 December) from noon.

**Art. 11**[12] Services outside normal working hours and on public holidays

[1] Outside normal working hours and on public holidays, the PTSS, the TSPs, with the exception of those with reduced surveillance duties (Art. 51), and the PDCSs with more extensive surveillance duties (Art. 52) must provide an on-call service during which they must be available at all times in order to rectify faults and provide the following services insofar as they are required to do so in accordance with Articles 18 and 50:

a. providing information in accordance with Articles 35–43, 48*a*–48*c* and in accordance with Article 27 in conjunction with the Articles 35, 40, 42 and 43;

b. activating real-time surveillance in accordance with Articles 54–59;

c. conducting urgent retrospective surveillance activities in accordance with Articles 60–63, 65 and 66;

d. conducting missing person searches in accordance with Article 67 and wanted person searches in accordance with Article 68, with the exception of network coverage analysis in preparation for an antenna search in accordance with Article 64;

e. issuing assignments for the mobile phone localisation of suspected terrorists in accordance with Article 68*a*;

[2] The authorities must notify the PTSS on-call service by telephone of services provided under paragraph 1, unless the information is provided automatically via the query interface of the processing systems.

[3] Requests for special information and orders for special surveillance activities (Art. 25) shall not be accepted or processed outside normal working hours or on public holidays.

[4] TSPs with reduced surveillance duties (Art. 51), PDCSs and PDCSs with more extensive duties to provide information (Art. 22) that already have an internal on-call service must provide the PTSS with the current contact details for their on-call service. In particularly urgent cases, the PTSS is permitted to contact them outside normal working hours and on public holidays via this channel.

12 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

## Section 4 Statistics

### Art. 12 Statistics on surveillance measures and information

1 The PTSS shall publish statistics every year about the surveillance activities ordered in the previous calendar year and the information provided. These shall indicate in particular the number:

a. of surveillance measures in real time;

b. of retroactive surveillance measures;

c. of instances in which information was provided;

d. of missing person searches;

e. of wanted person searches;

f.[13] of mobile phone localisations of suspected terrorists.

2 The statistics in accordance with paragraph 1 shall indicate:

a. the type of offence;

b. the canton of the ordering authority, the ordering federal authority or, in the case of missing person searches, also an authority from the Principality of Liechtenstein, and in the case of information, the competent cantonal or federal authority (Art. 1 para. 2 lets c–f);

c.[14] the nature of the information, surveillance, missing person search or wanted person search or mobile phone localisation of suspected terrorists;

d. the duration of surveillance, if applicable;

e. the fees;

f. the compensation.

### Art. 13 Statistics on surveillance measures with special technical devices and special IT programs

1 Public prosecutor's offices and military examining magistrates shall keep annual statistics on the special technical devices and special information technology programs used in the previous calendar year for surveillance activities (Art. 269$^{bis}$ para. 2 and 269$^{ter}$ para. 4 CrimPC and Art. 70$^{bis}$ para. 2 and 70$^{ter}$ para. 4 MCPC respectively). The statistics shall indicate the type of offence.

2 Public prosecutor's offices and the Office of the Military Attorney General at the DDPS shall submit the statistics to the PTSS in the first quarter of the following year. The statistics shall indicate only assignments concluded in the year concerned.

13 Inserted by No I 12 of the O of 4 May 2022 on Police Counterterrorism Measures, in force since 1 June 2022 (AS **2022** 301).

14 Amended by No I 12 of the O of 4 May 2022 on Police Counterterrorism Measures, in force since 1 June 2022 (AS **2022** 301).

3 The PTSS shall publish consolidated statistics every year. These do not contain any details of the canton of the ordering authority or the federal ordering authority.

## Chapter 2 Postal Deliveries

**Art. 14** Obligations of PSPs

1 Each PSP must be able to provide the information specified in Article 20 SPTA and conduct the types of surveillance specified in Article 16 insofar as the information and surveillance activities relate to services that the PSP provides.

2 Each PSP must ensure that it can accept and execute the requests for information and surveillance orders during normal working hours.

**Art. 15** Order to conduct surveillance of postal deliveries

The surveillance order submitted to the PTSS shall contain the following information:

a. contact details for the ordering authority;

b. contact details for the persons authorised to be the recipients of the surveillance data;

c. if known, the surname, first name, date of birth, address and occupation of the person to be placed under surveillance;

d. reference numbers and case names for the surveillance activities;

e. the reason for surveillance, in particular the criminal offence to be investigated by means of surveillance;

f. the name of the PSP;

g. the types of surveillance ordered;

h. if necessary, additional information on a person's postal traffic;

i. the start and duration of surveillance;

j. in the case of persons bound by professional secrecy in accordance with Article 271 CrimPC or Article 70*b* MCPC: a note on this aspect;

k. if need be, the measures to protect persons holding professional secrets and further protection measures that the authorities, the PSP and the PTSS must take.

**Art. 16** Types of surveillance

The following types of surveillance may be ordered:

a. the interception of postal deliveries (real time-surveillance; Surveillance Type PO_1_RT_INTERCEPTION);

b. the provision of the following secondary telecommunications data (real-time surveillance; Surveillance Type PO_2_RT_DELIVERY), insofar as they are available:
   1. the addressee,
   2. the sender,
   3. the type,
   4. the mailing location,
   5. the delivery status,
   6. the recipient's signature;

c. the provision of the following secondary telecommunications data (retroactive surveillance; Surveillance Type PO_3_HD):
   1. for postal deliveries with proof of delivery: the recipient and the sender as well as the type, the mailing location and the delivery status of the postal delivery, if available,
   2. if the PSP has recorded any additional secondary telecommunications data: all available data.

## Chapter 3 Telecommunications

### Section 1 General Provisions on Information and Surveillance Activities

**Art. 17** Requests for information

1 Requests for information from the authorities specified in Article 15 SPTA to TSPs, providers of derived communication, PDCSs[15] and operators of internal telecommunications networks as well as the information returned to the authorities are transmitted in the online request procedure or via the interfaces using the processing system specified in the PSO-PTSS[16].

2 If the online request procedure using the processing system is unavailable for technical reasons, requests for information and the information returned to the authorities may be submitted to the PTSS by post or fax.

3 In urgent cases, the authorities may submit requests for information by telephone to the PTSS, and submit the request for information specified in paragraph 1 or 2 subsequently.

4 The request for information must indicate, in addition to the details required for the type of information concerned, the maximum number of data records to be supplied and, if available, the reference numbers and case names.

15 Term in accordance with No 1 para. 2 of the FA of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685). This amendment is made in the provisions specified in the AS.

16 SR **780.12**

**Art. 18**[17] Obligations of TSPs and PDCSs with more extensive duties to provide information

[1] The following providers of derived communication services shall provide the information via the query interface of the PTSS processing system:

a. TSPs, with the exception of those with reduced surveillance duties 51);

b. PDCSs with more extensive duties to provide information (Art. 22);

c. PDCSs with more extensive surveillance duties (Art. 52).

[2] TSPs, with the exception of those with reduced surveillance duties, shall provide the information in accordance with Articles 35–37, 40, 41 and 48*b* and in accordance with Article 27 in conjunction with the Articles 35 and 40 automatically. They shall provide other standardised information manually or automatically if they so request and by arrangement with the PTSS.

[3] TSPs with reduced surveillance duties are not required to provide information in accordance with Article 48*b*. They shall provide the standardised information as follows:

a. in writing, outside the processing system by means of a secure means of transmission authorised by the FDJP;

b. manually, via the query interface of the processing system; or

c. automatically, if they so request and by arrangement with the PTSS.

[4] PDCSs with more extensive duties in accordance with Article 22 or 52 shall provide the information in accordance with Articles 35–37, 40 and 41 and in accordance with Article 27 in conjunction with Articles 35 and 40 automatically. They are not required to provide information in accordance with Articles 48*a*–48*c*. They shall provide the other standardised information manually or, if they so request and by arrangement with the PTSS, automatically.

**Art. 18*a***[18] Obligations of PDCSs without more extensive duties and operators of internal telecommunications networks to provide information

[1] PDCSs without more extensive duties and operators of internal telecommunications networks are not required to adhere to the types provided for in this Ordinance when providing information.

[2] They shall supply the information available to them in writing outside the processing system via a secure means of transmission authorised by the FDJP.

[3] They may if they so request provide the information manually via the query interface of the PTSS processing system or automatically by arrangement with the PTSS.

17 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
18 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

**Art. 18*b***[19] Involvement of third parties in providing information

The persons or entities required to cooperate may engage third parties to provide information.

**Art. 18*c***[20] Disclosure of the number of data records when providing information

If the number the data records found exceeds the maximum number specified in the request, the person or entity required to cooperate shall only disclose their number.

**Art. 19** Identification of the participants

[1] TSPs, PDCSs with more extensive duties to provide information in accordance with Article 22, PDCSs with more extensive surveillance duties in accordance with Article 52 and retailers in accordance with Article 2 letter f SPTA must ensure that subscribers are identified by suitable means.

[2] In the case of professionally operated public WLAN access points[21], TSPs must ensure that all end users are identified by suitable means.

**Art. 20**[22] Verifying personal details in the case of mobile services

[1] When supplying the means of access to mobile services or on the initial activation of such services, the TSP must verify the proof of identity in accordance with Articles 20*a* and 20*b*.

[2] This obligation applies to the retailer in accordance with Article 2 letter f SPTA and not the TSP, if the means of access is supplied or the services are initially activated directly by the retailer.

[3] The TSP shall verify in an appropriate manner the due registration and identification of the subscriber by the retailer and that the TSP has received the information and the copy of the identity document.

**Art. 20*a***[23] Provision of the proof of identity by natural persons in the case of mobile services

[1] Where the subscriber is a natural person, proof of the identity must be provided by producing any one of the following documents, which must be valid on the day of recording:

a. a Swiss or foreign passport;

b. a Swiss or foreign identity card; or

19 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
20 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
21 Term in accordance with No 1 para. 1 of the FA of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685). This amendment is made in the provisions specified in the AS.
22 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
23 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

c. a foreign national identity card in accordance with the Article 71 and 71*a* of the Ordinance of 24 October 2007[24] on Admission, Period of Stay and Employment.

2 The following data about the subscriber shall be recorded:

a. based on the document:
   1. surname and given name(s),
   2. date of birth,
   3. type of document, number and the issuing country or issuing organisation,
   4. nationalities;

b. address;

c. if known: occupation.

3 In the case of customer relationships that are not based on a subscription contract the following data must also be recorded:

a. the time at which the means of access was supplied or the services were first activated;

b. the name and full address of the point of supply or activation;

c. the surname and given name(s) of the person recording the data.

4 The TSP or if applicable the retailer must make or have made an easily legible electronic copy of the original document. The retailer shall supply the data in accordance with paragraphs 2 and 3 and the copy to the TSP within 3 days of recording the data.

**Art. 20*b***[25] Provision of proof of identity of legal entities in the case of mobile services

1 In the case of legal entities, the following data must be recorded and verified based on suitable proof:

a. the name, registered office and contact data of the legal entity;

b. the unique business identification number (UID) in accordance with the Federal Act of 18 June 2010[26] on the Business Identification Number or the international legal entity identifier (LEI) of the legal entity;

c. if available, the names and forenames of the persons who will use the provider's services.

2 Retailers shall supply the information to the TSP within 3 days of recording the data.

3 Article 20*a* paragraph 3 applies *mutatis mutandis*.

24 SR **142.201**
25 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
26 SR **431.03**

**Art. 20*c***[27] Supply of means of access and activation of services for police authorities and the FIS

[1] The PTSS shall at the request of the federal or cantonal police authorities or of the FIS arrange for a contract to be concluded between a TSP and the authority on the supplying the means of access and activating the services. The contract shall provide that the information in accordance with Article 20*b* is only accessible to a particularly small group of trustworthy persons. The TSP shall decide in consultation with the PTSS on the methods by which further disclosure of the data can be prevented.

[2] The PTSS shall verify the identity of the persons who are entitled to obtain means of access and services on behalf of the authorities, and shall pass on the information required to supply this means of access and to activate these services to the TSP. The TSP shall document the means of access supplied to and the services activated for the authorities internally.

[3] The means of access and services in accordance with this Article may only be used within the scope of the law applicable to the authority concerned.

**Art. 21**[28] Retention periods

[1] The following providers must retain and be able to provide the following data for the duration of and for 6 months following the end of the customer relationship:

a. TSPs and PDCSs with more extensive duties in accordance with Article 22 or 52: the data on the services and the data for the purpose of identification in accordance with Article 19 paragraph 1;

b. TSPs: in addition, data on identifiers assigned on a long-term basis in accordance with Article 48*a*.

[2] TSPs must retain and be able to provide identification data in accordance with Article 19 paragraph 2 for the duration of and for 6 months following the end of authorisation to access the professionally operated public WLAN access.

[3] They must for the purpose of identification retain the data on the unique assignment of IP addresses for the network access point for 6 months and be able to provide the information in accordance with Article 37.

[4] TSPs that offer mobile services must retain and be able to supply the data on the subscribers in accordance with Articles 20*a* and 20*b* and a copy of the proof of identity for the duration of and for 6 months following the end of the customer relationship.

[5] TSPs, with the exception of those with reduced surveillance duties (Art. 51), must retain the following data for the purpose of identification for 6 months:

a. secondary telecommunications data relating to the device identifiers actually used, in order to be able to provide the information specified in Articles 36 paragraph 1 letter b and 41 paragraph 1 letter b number 2;

27 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
28 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

b. secondary telecommunications data relating to the assignment and translation (NAT) of IP addresses and port numbers for the network access, in order to be able to provide the information specified in Articles 38 and 39; and

c. secondary telecommunications data to determine the networks directly adjacent to a communication or an attempt at communication using telephony and multimedia services in order to be able to provide the information in accordance with Article 48*c*.

6 PDCSs with more extensive surveillance duties (Art. 52) must retain the data in accordance with paragraph 5 letters a and b for 6 months for the purpose of identification.

7 The secondary telecommunications data under paragraph 2 must be destroyed as soon as the retention period has expired, unless other legislation requires or permits such data to be retained for longer.

**Art. 22** PDCSs with more extensive duties to provide information

1 The PTSS shall declare a PDCSs to be a provider with more extensive duties to provide information (Art. 22 para. 4 SPTA), if it has met one of the following criteria:

a. 100 requests for information in the past 12 months (effective date: 30 June);

b. annual turnover in Switzerland of CHF 100 million in two successive financial years, provided a large part of its business operations provides derived communication services and 5,000 subscribers use the provider's services.

2 If a provider controls one or more undertakings required to file financial reports as defined in Article 963 paragraph 2 of the Code of Obligations[29], the provider and the controlled undertakings must be regarded as a single unit when calculating the values in accordance with paragraph 1.

3 Providers that exceed or fail to meet the criteria in paragraph 1 letter b must notify the PTSS of this in writing within three months of the end of their financial year and submit related supporting documents.

4 Providers must on request provide the PTSS with the information and supporting documents for assessing the criteria under paragraph 1 letter b. The PTSS may rely on data obtained in implementing the legislation relating to the surveillance of post and telecommunications or by other authorities in implementing federal law.

5 A provider that is declared to have more extensive duties to provide information must ensure that it can store the data required for providing information within 2 months and provide the information within 12 months of the declaration.

**Art. 23** Assistance in providing information and conducting surveillance activities

If third parties are engaged by the provider to assist in providing information or conducting surveillance activities, they shall be subject to the same requirements as the

29 SR **220**

provider. The provider remains responsible for providing information and conducting the surveillance activities ordered to the extent specified; in particular it shall take the measures required to ensure that suitable contact persons for providing information and conducting the surveillance activities ordered are available to the PTSS at all times. Both the provider assigned the task by the PTSS and its assistants serve as contact points for the PTSS.

**Art. 24** Standardisation of types of information and surveillance

1 The Federal Justice and Police Department (FDJP) shall standardise the types of information and surveillance that are defined in this Ordinance.

2 If, based on the international standards and the enquiries made of the persons or entities required to cooperate, it proves impossible or unreasonable to standardise a type of information or surveillance, the FDJP shall dispense with doing so.

**Art. 25** Special information and surveillance activities

In the case of information and surveillance activities that do not correspond to a standardised type of information or surveillance, TSPs and PDCSs shall provide the PTSS with all already available interfaces and connections to the PTSS processing system. The content and the secondary telecommunications data of the telecommunication of the person under surveillance must be supplied as far as possible in accordance with Article 26 paragraph 1 SPTA. The PTSS shall determine the modalities in specific cases.

**Art. 26**[30] Types of information

1 The types of information relate to information about:

a. the subscribers (Art. 35, 40, 42 and 43 together with Art. 27 in conjunction with these articles);

b. services (Art. 36–39 and 41);

c. the method of payment (Art. 44);

d. the proof of identity (Art. 45);

e. the copies of invoices (Art. 46);

f. the copies of contracts (Art. 47);

g. the technical data relating to telecommunications systems and network elements (Art. 48);

h. the identifiers assigned (Art. 48*a* and 48*b*); and

i. determining the adjacent networks (Art. 48*c*).

2 The authorities may only request the information that persons or entities required to cooperate are required to provide in accordance with the procedures defined in this Ordinance.

30 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

**Art. 27** Obtaining information with a flexible name search

[1] Requests for types of information specified in Articles 35, 40, 42 and 43 may be complied with by carrying out a search that tolerates errors and finds phonetic matches (flexible name search). In this case, the suffix "FLEX" shall be added to the abbreviation for the relevant information request type: IR_5_NA_FLEX, IR_11_TEL_FLEX, IR_14_email _FLEX and IR_16_COM_FLEX.

[2] The request for information shall in each case contain the first and at least one additional query criterion for the underlying information request type.

**Art. 28**[31] Types of surveillance

The types of surveillance are as follows:

a. real-time surveillance:
   1. of secondary telecommunications data in the case of network access services (Art. 54),
   2. of content and secondary telecommunications data in the case of network access services (Art. 55),
   3. of secondary telecommunications data in the case of applications (Art. 56 and 58),
   4. by means of position determination by the network (Art. 56*a* and 56*b*),
   5. of content and secondary telecommunications data in the case of applications (Art. 57 and 59);

b. retroactive surveillance:
   1. of network access services (Art. 60),
   2. of applications (Art. 61 and 62),
   3. by determining the location of the most recent activity (Art. 63),
   4. by means of an antenna search (Art. 66) and the related preparations (Art. 64 and 65);

c. the missing person search (Art. 67):
   1. by determining the location of the most recent activity (Art. 67 let. a),
   2. by means of position determination by the network (Art. 67 let. b and c),
   3. by means of real-time surveillance of content and secondary telecommunications data for network access services and telephony and multimedia services (Art. 67 let. d),
   4. by means of real-time surveillance of secondary telecommunications data for network access services and telephony and multimedia services (Art. 67 let. e),
   5. by means of retroactive surveillance of network access services and in the case of telephony and multimedia services (Art. 67 let. f);

d. the wanted person search (Art. 68):

31 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

1. by determining the location of the most recent activity (Art. 68 para. 1 let. a),
2. by means of position determination by the network (Art. 68 para. 1 let. b and c),
3. by means of real-time surveillance of content and secondary telecommunications data for network access services and telephony and multimedia services (Art. 68 para. 1 let. d),
4. by means of real-time surveillance of secondary telecommunications data for network access services and telephony and multimedia services (Art. 68 para. 1 let. e),
5. by means of real-time surveillance of secondary telecommunications data for network access services and telephony and multimedia services (Art. 68 para. 1 let. f),
6. by means of an antenna search and the related preparations (Art. 68 para. 1 let. g);

e. real-time mobile phone localisation of terrorist suspects (Art. 68*a*).

## Section 2 Quality Assurance

### Art. 29 Quality of the data transmitted

[1] The quality of the data transmitted is acceptable if:

a. the data delivery meets the requirements specified by the FDJP;

b. the data is delivered without loss of data and without interruptions; and

c. the transmitted surveillance data or information data correspond to that specified in the surveillance order or request for information.

[2] The persons or entities required to cooperate are responsible for the quality of the transmitted information and surveillance data up to the point of delivery.

[3] If a provider or the PTSS identifies any defects in the quality of the data transmitted, they shall inform each other without delay. The PTSS shall determine the seriousness of the defects and the procedure for their rectification after consulting the provider. The provider and the PTSS shall inform each other regularly and promptly about the status of the rectification of defects.

### Art. 30 Test connections

[1] The PTSS may make test connections; in doing so, it may work with the prosecution authorities and the FIS. The tests serve the following purposes in particular:

a. assuring the quality of the data diverted to the PTSS and the prosecution authorities by the persons or entities required to cooperate;

b. verifying the ability of the persons or entities required to cooperate to provide information and conduct surveillance;

c. testing the PTSS processing system;

d. training;

e. generating reference data.

2 The PTSS may instruct the persons or entities required to cooperate to participate in generating the test data. The PTSS shall draw up a test plan after consulting the persons or entities required to cooperate.

3 The persons or entities required to cooperate shall provide the PTSS with the required test connections and the required telecommunications services or derived communications services at its request free of charge and permanently. They shall assist the PTSS in making the required test connections that they cannot themselves provide.[32]

4 The prosecution authorities and the FIS may also make test connections at their own expense for the purpose of quality assurance and the training. To this end, they shall submit orders to the PTSS and pay fees.

## Section 3
## Ensuring Ability to provide Information and conduct Surveillance

**Art. 31** Verifying ability to provide information and conduct surveillance

1 TSPs and PDCSs with more extensive information (Art. 22) or surveillance duties (Art. 52) shall in accordance with Article 33 paragraph 1 SPTA provide proof of their ability to provide information and conduct surveillance.

2 Proof is provided if:

a. the tests that must be conducted in accordance with PTSS requirements have been successfully completed; and

b. the provider confirms in a questionnaire drawn up by the PTSS it meets the requirements in relation to standardised information and surveillance activities that cannot be proven by testing.

3 The PTSS shall ensure that it conducts the verification process promptly and does not cause any delay in market introduction. To do so, it shall carry out the following tasks:

a. It shall check the results of the tests in accordance with paragraph 2 letter a.

b. It shall evaluate the questionnaire in accordance with paragraph 2 letter b.

c. It shall keep a record of the test procedures.

d. It shall issue the providers with confirmation in accordance with Article 33 paragraph 6 SPTA.

e. It shall retain the records for as long as the confirmation remains valid and for ten years after its expiry.

32 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

4 The PTSS shall state in the confirmation that the provider has proven its ability to provide certain types of information and conduct certain types of surveillance activities.

**Art. 32** Term of validity of the confirmation

1 The confirmation of ability to provide information and conduct surveillance is valid for three years.

2 On expiry of the term of validity, the PTSS may extend the confirmation by a further three years if the person or entity required to cooperate certifies that since confirmation was granted no modifications have been carried out that influence data delivery or the ability to provide information or conduct surveillance.

3 If a provider can no longer provide information or conduct surveillance, it shall notify the PTSS immediately.

**Art. 33** Acceptance procedure

The FDJP shall regulate the procedure for verifying ability to provide information and conduct surveillance.

**Art. 34** Declaration of invalidity of the confirmation of ability to provide information and conduct surveillance

The PTSS shall immediately declare a confirmation of ability to provide information and conduct surveillance that has already been issued to be invalid for the relevant types of information or surveillance if:

a. the provider gives notice that it can no longer provide information or conduct surveillance;

b. the provider is unable on two or more occasions to deliver data, provide information or conduct surveillance;

c. the information on the provider that underlies the confirmation is untrue.

## Section 4
## Types of Information Requests for Network Access Services

**Art. 35** Information Request Type IR_4_NA: Information on subscribers to network access services

1 Information Request Type IR_4_NA comprises the following data about subscribers to network access services:

a. if available, the unique subscriber identifier (e.g. customer number);

b.[33] in the case of mobile services:

1. the data on the natural person or legal entity in accordance with Articles 20–20*b*,
2. if available, additional addresses and contact data and their term of validity, and
3. in the case of natural persons, gender;

c.[34] in the case of the other network access services:

1. the identification data specified in Article 19,
2. if known, the details of the natural or legal entity, additional addresses and contact data and their term of validity, and
3. in the case of natural persons, gender;

d. the following information about each network access service that the subscriber obtains from the provider:[35]

1. the unique identifier for the provider (e.g. TSP number),
2.[36] the main unique service identifier (e.g. user name, MSISDN, GPSI),
3. the period over which the service was used (start, first activation and, if applicable, termination),
4. if applicable, further information about additional options or restrictions on the network access service,
5. if applicable, the installation addresses of the fixed location access to the network and their period of validity in each case,
6. the statuses of the service as designated internally by the provider (e.g. active, suspended, blocked) and their period of validity in each case,
7. if applicable, all static IP addresses, IP prefixes, IP address ranges and net masks or prefix lengths assigned to network access service concerned and their period of validity in each case,
8. in the case of customer relationships that are not based on a subscription contract, the time and the point of supply (name and complete address) for the means of access and the name of the person who made the supply,
9.[37] if applicable, the associated ICCID at the time of its supply,
10.[38] if applicable, the associated IMSI or SUPI,
11.[39] the type of customer relationship (e.g. prepaid, subscription),

33 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
34 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
35 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
36 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
37 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
38 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
39 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

12.[40] if applicable, the list or area for the additional addressing resources and identifiers (e.g. ICCID) registered in connection with or associated with the service (e.g. MSISDN) and their term of validity,

13.[41] the name of the service (e.g. name of the subscriptions or of the tariff).

2 The request for information shall specify the period to which the request relates. It shall contain at least one of the following query criteria.[42]

a. surname(s), first name(s);

b. date of birth;

c. country and postcode or country and place;

d. street and, if possible, house number;

e. identity document number and, optionally, the type of identity document;

f. name and, optionally, the registered office of the legal entity;

g.[43] UID or LEI;

h. subscriber identifier (e.g. customer number);

i.[44] subscriber identifier or service identifier other than IP addresses (e.g. user name, MSISDN, GPSI);

j.[45] IMSI or SUPI;

k.[46] ICCID.

3 In the case of the criteria in accordance with paragraph 2 letters a–d, a second query criterion shall be added. In the case of searches for character strings (para. 2 let. a, c, d and f), the provider shall search for the specified spelling in accordance with the FDJP regulations.[47]

**Art. 36**[48] Information Request Type IR_6_NA: Information on network access services

1 Information Request Type IR_6_NA comprises the following data about network access services:

a. if available, the unique subscriber identifier (e.g. customer number);

b. the following data about the requested services and any additional associated network access services:

1. the unique service identifier (e.g. user name),

40 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
41 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
42 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
43 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
44 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
45 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
46 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
47 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
48 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

2. if applicable, all identifiers associated with the service concerned (e.g. user name, MSISDN, GPSI) and their term of validity,
3. if available, the alternative subscriber identifier, and in particular in the case of professionally operated public WLAN access, an identifier that enables a request for the identification data in accordance with Article 19 paragraph 2 to be made,
4. the unique device identifiers in accordance with international standards (e.g. IMEI, PEI, MAC address) of the devices used in connection with the service for the devices used at the provider in connection with the service concerned in the last 6 months and, if available, the individual names of the devices,
5. if applicable, the ICCID of all SIMs associated with the service concerned and their term of validity, the PUK and PUK2 codes, the IMSI or the SUPI, the MSISDN or the GPSI and the eUICC-ID,
6. in the case of a multi-device offer: information on whether the device is the main device or a secondary device.

2 The request for information shall specify the period to which the request relates. It shall contain at least one of the following query criteria:

a. the service identifier, other than IP addresses (e.g. user name, MSISDN, GPSI or an identifier) that enables a request for the identification data in accordance with Article 19 paragraph 2 to be made;

b. the IMSI or the SUPI;

c. the unique device identifier in accordance with international standards (e.g. IMEI, PEI, MAC address);

d. the installation address of the fixed location access to the network;

e. the ICCID.

**Art. 37** Information Request Type IR_7_IP: Identification of the users in the case of uniquely assigned IP addresses

1 Information Request Type IR_7_IP comprises the following data for the purpose of identification if a unique IP address was not assigned:[49]

a. if available, the unique subscriber identifier (e.g. user name);

b.[50] the unique service identifier (e.g. user name, MSISDN, GPSI) of the network access service or an identifier that enables a request for the identification data in accordance with Article 19 paragraph 2 to be made;

c. the unique identifier that indicates the provider of the network access service (e.g. TSP number).

49 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
50 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

2 The request for information shall contain the following information:

a. the IP address;

b. the date and time.

**Art. 38** Information Request Type IR_8_IP (NAT): Identification of the users in the case of IP addresses that are not uniquely assigned (NAT)

1 Information Request Type IR_8_IP (NAT) comprises the following data for the purpose of identification if a unique IP address was not assigned (NAT ):[51]

a. if available, the unique subscriber identifier (e.g. user name);

b.[52] the unique service identifier (e.g. user name, MSISDN, GPSI) of the network access service or an identifier that enables a request for the identification data in accordance with Article 19 paragraph 2 to be made.

2 The request for information shall contain the information known about the requested NAT context:[53]

a. the public source IP address;

b. if required for identification, the public source port number;

c. if required for identification, the public destination IP address;

d. if required for identification, the destination port number;

e. if required for identification, the type of transport protocol;

f.[54] the relevant date and time, at the beginning, within or at the end of the NAT context.

**Art. 39**[55] Information Request Type IR_9_NAT: Information on NAT contexts

1 Information Request Type IR_9_NAT comprises the following data on a specific NAT context for the purpose of identification in connection with a NAT procedure at provider level:

a. the source IP address before or after the NAT translation;

b. the source port number before or after the NAT translation.

2 The request for information shall contain the data known about the requested NAT context:

a. the source IP address after or before the NAT translation;

b. the source port number after or before the NAT translation;

51 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
52 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
53 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
54 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
55 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

c. if required for identification, the public destination IP address;

d. if required for identification, the destination port number;

e. if required for identification, the type of the transport protocol;

f. the relevant date and time, at the beginning, within or at the end of the NAT context.

## Section 5 Types of Information on Applications

### Art. 40 Information Request Type IR_10_TEL: Information on subscribers to telephony and multimedia services

[1] Information Request Type IR_10_TEL comprises the following data about subscribers to telephony and multimedia services:

a. if available, the unique subscriber identifier (e.g. customer number);

b.[56] in the case of mobile services:

1. data on the natural person or legal entity in accordance with Articles 20, 20*a* and 20*b*,
2. if available, additional addresses and contact data and their term of validity, and
3. in the case of natural persons, gender;

c.[57] in the case of the other telephony and multimedia services:

1. the identification data specified in Article 19,
2. if available, data on the natural person or legal entity, additional addresses and contact details and their term of validity, and
3. in the case of natural persons, gender;

d. the following data about each telephony and multimedia service obtained by the subscriber from the provider:[58]

1. the unique identifier designating the provider (e.g. TSP number),
2.[59] the unique main service identifier (e.g. telephone number, SIP URI),
3. the period over which the service was used (start, first activation and if applicable, termination),
4. the type of the service (e.g. private telecommunications installation, public call station, fixed location or mobile location service),
5. if applicable, the installation addresses of the fixed location network access to the service and their period of validity in each case,

56 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
57 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
58 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
59 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

6.[60] the statuses of the service as designated internally by the provider (e.g. active, suspended, blocked) and their term of validity,

7.[61] if applicable, the list or range of other addressing resources (e.g. telephone numbers, IMPU) or identifiers (e.g. ICCID) registered in connection with this service and their term of validity,

8. in the case of customer relationships that are not based on a subscription contract, the time and the point of supply (name and complete address) of the means of access and the name of the person who made the supply,

9. if applicable, details of predetermined free choice of service provider for connections,

10.[62] if applicable, the associated IMSI or SUPI,

11.[63] if applicable, the associated ICCID at the time of supply,

12.[64] the type of customer relationship (e.g. prepaid, subscription),

13.[65] the name of the service (e.g. name of the subscriptions or of the tariff).

2 The request for information shall specify the period to which the request relates. It shall contain at least one of the following query criteria:[66]

a. surname(s), first name(s);

b. date of birth;

c. country and postcode or country and place;

d. street and, if possible, house number;

e. identity document number and optionally, the type of identity document;

f. name and optional registered office the legal entity;

g.[67] UID or LEI;

h subscriber identifier (e.g. customer number)

i. addressing resources or identifiers (e.g. telephone number, SIP URI, TEL URI, IMPU);

j.[68] IMSI or SUPI;

k.[69] ICCID.

3 In the case of the criteria in paragraph 2 letters a–d, a second query criterion shall be added. In the case of searches for character strings (para. 2 let. a, c, d and f), the provider shall search for the specified spelling in accordance with the FDJP regulations.[70]

60 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
61 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
62 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
63 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
64 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
65 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
66 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
67 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
68 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
69 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
70 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

**Art. 41**[71] Information Request Type IR_12_TEL: Information on telephony and multimedia services

[1] Information Request Type IR_12_TEL comprises the following data about telephony and multimedia services:

a. if available, the unique subscriber identifier (e.g. customer number);

b. the following data about the requested services and any additional associated telephony and multimedia services:

1. if applicable, public addressing resources (e.g. MSISDN, SIP URI, TEL URI) and private addressing resources (e.g. IMPI) associated with the service concerned and their term of validity,

2. the unique device identifiers in accordance with international standards (e.g. PEI) of the devices used in connection with the service concerned from the provider in the last 6 months and, if available, the names of the devices,

3. if applicable, the ICCID of all SIMs associated with the service concerned and their term of validity, the PUK and PUK2 codes, the IMSI or the SUPI, the MSISDN or the GPSI and the eUICC-ID,

4. in the case of a multi-device offer: information on whether the device is the main device or a secondary device.

[2] The request for information shall specify the period to which the request relates. It shall contain at least one of the following query criteria:

a. the public addressing resource (e.g. SIP URI, MSISDN, GPSI);

b. the IMSI or the SUPI;

c. the unique device identifier in accordance with international standards (e.g. IMEI, PEI, MAC address);

d. the installation address of the fixed location access to the network;

e. the private addressing resource (e.g. IMPI);

f. the ICCID.

**Art. 42** Information Request Type IR_13_EMAIL: Information on subscribers to E-Mail-services

[1] Information Request Type IR_13_EMAIL comprises the following data about subscribers to email services:

a. if available, the unique subscriber identifier (e.g. customer number);

b. the identification data specified in Article 19 and, if known, the data on the natural person or legal entity, additional contact data and the gender of the natural person;

71 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

c. the following information about each email service that the subscriber obtains from the provider:[72]
   1. the unique identifier that indicates the provider of the service,
   2. the unique service identifier (e.g. email address, user name),
   3. the period over which the service was used (start, first activation and if applicable, termination),
   4. if applicable, the list of all additional addressing resources (e.g. alias address) that pertain to this service,
   5. if applicable, the list of all addresses, to which messages addressed to the requested address are forwarded (e.g. mailing list),
   6.[73] the name of the service;

d.[74] if applicable, the additional addressing resources or identifiers recorded by the provider in connection with this service (e.g. email address, MSISDN, GPSI, addressing resource provided to restore lost access to the email account).

[2] The request for information shall specify the period to which the request relates. It shall contain at least one of the following query criteria:[75]

a. surname(s), first name(s);

b. date of birth;

c. country and postcode or country and place;

d. street and if possible house number;

e. identity document number and, optionally, the type of identity document;

f. name and, optionally, registered office of the legal entity;

g.[76] UID or LEI;

h. subscriber identifier (e.g. customer number);

i. service identifier (e.g. email address, user name);

j.[77] identifiers associated with the service concerned, such as a recovery addressing resource.

[3] In the case of the criteria in paragraph 2 letters a–d, a second query criterion shall be added. If searching for character strings (let. a, c, d and f), the provider shall search for the specified spelling of the term in accordance with the FDJP regulations.[78]

72 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
73 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
74 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
75 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
76 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
77 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
78 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

**Art. 43** Information Request Type IR_15_COM: Information on subscribers to other telecommunications or derived communications services

[1] Information Request Type IR_15_COM comprises the following data about subscribers to other telecommunications or derived communications services (e.g. messaging services, communications services in social networks:[79]

a. if available, the unique subscriber identifier (e.g. customer number);

b. the identification data specified in Article 19 and, if known, data on the natural person or legal entity, additional contact data and the gender of the natural person;

c. the following data about each additional telecommunications service or derived communications service that the subscriber obtains from the provider:[80]

1. the unique identifier that indicates the provider,
2. the unique service identifier (e.g. user name),
3. the period over which the service was used (start, first activation and if applicable, termination),
4. the statuses of the service as designated internally by the provider (e.g. active, suspended, blocked) and their period of validity in each case,
5. the list of other addressing resources or identifiers registered in connection with this service,
6.[81] the name of the service.

[2] The request for information shall specify the period to which the request relates. It shall contain at least one of the following query criteria:[82]

a. surname(s), first name(s);

b. date of birth;

c. country and postcode or country and place;

d. street and, if possible, house number;

e. identity document number and, optionally, the type of identity document;

f. name and, optionally, the registered office of the legal entity;

g.[83] UID or LEI;

h. subscriber identifier (e.g. customer number);

i.[84] addressing resource or identifier (e.g. user address, pseudonym, unique application-specific identifier);

79 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
80 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
81 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
82 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
83 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
84 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

j.[85] identifier associated with the service concerned, such as a recovery addressing resource.

3 In the case of the criteria in paragraph 2 letters a–d, a second query criterion shall be added. If searching for character strings (let. a, c, d and f), the provider shall search for the specified spelling of the term in accordance with the FDJP regulations.[86]

## Section 6 Further Types of Information

### Art. 44 Information Request Type IR_17_PAY: Information on the method of payment used by subscribers to telecommunications and derived communications services

1 Information Request Type IR_17_PAY comprises the following data about the method of payment used by subscribers to telecommunications and derived communications services:

a. the unique identifier that indicates the provider;

b. the unique subscriber identifier (e.g. customer number);

c.[87] the unique identifier that the provider has assigned to the subscriber for accounting or billing purposes;

d. the unique service identifier (e.g. telephone number, SIP URI, user name);

e. the method of payment (debit, bank transfer or prepaid);

f.[88] the account information that the subscriber has given to the provider, consisting of the name of the bank, account holder and IBAN (or BIC and account number) or national bank number and account number;

g. the billing addresses (house number, street, PO box, postcode, place, country) and their period of validity (start and if applicable, termination).

2 The data specified in paragraph 1 must be supplied if the provider has it.

3 The request for information shall specify the period to which the request relates. It shall contain at least one of the following query criteria:

a. the subscriber identifier (e.g. customer number);

b. the service identifier (e.g. telephone number, SIP URI, user name);

c.[89] the identifier that the provider has assigned to the subscriber for accounting or billing purposes;

d.[90] the subscriber's bank account information: IBAN (or BIC and account number) or national bank number and account number;

85 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
86 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
87 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
88 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
89 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
90 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

e. the billing address (house number, street, PO box, postcode, place, country);

f.[91] the code for topping up the credit or paying for the service.

**Art. 45**[92] Information Request Type IR_18_ID: Proof of identity

[1] Information Request Type IR_18_ID comprises the provision of an electronic copy of the subscriber's identification document recorded in accordance with Article 20*a* paragraph 4.

[2] The request for information shall specify the period and subscriber or service identifier, ICCID, IMSI or SUPI or, if applicable, device identifier to which it relates.

**Art. 46** Information Request Type IR_19_BILL: Copy of invoice

[1] Information Request Type IR_19_BILL comprises the provision of electronic copies of all available billing records pertaining to the subscriber, not including secondary telecommunications data on telecommunications services and derived communications services.[93]

[2] The request for information shall specify the period and unique subscriber or service identifier or unique identifier for accounting or billing to which it relates.

**Art. 47**[94] Information Request Type IR_20_CONTRACT: Copy of contract

[1] Information Request Type IR_20_CONTRACT comprises the provision of electronic copies of all available contract documents pertaining to the subscriber to telecommunications services and derived communications services.

[2] The request for information shall specify the period and subscriber or service identifier, ICCID, IMSI or SUPI or, if applicable, the device identifier to which it relates.

**Art. 48**[95] Information Request Type IR_21_TECH: Technical data

[1] Information Request Type IR_21_TECH comprises the provision of technical data relating to telecommunications systems and network elements at the requested location, in particular the location data for mobile radio cells and professionally operated public WLAN access points.

[2] The location data comprise:

a. the identifiers of network elements (e.g. cell or geographical area identifier) or another suitable designation (e.g. hotspot name)) and the geographical coordinates or other details of the location in accordance with international standards;

b. the available postal address of the location;

91 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
92 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
93 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
94 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
95 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

c. if applicable, the main directions of emission of the antennae of the cells;

d. other available location features; and

e. if applicable, the associated timestamps.

3 The request for information shall specify the period to which the request relates. It shall contain at least one of the following query criteria:

a. the geographical coordinates of the requested location of the network element;

b. the identifier of the network element (e.g. cell or geographical area identifier) or another suitable designation (e.g. hotspot name).

**Art. 48*a***[96] Information Request Type IR_51_ASSOC_PERM: Information on identifiers assigned on a long-term basis

1 Information Request Type IR_51_ASSOC_PERM comprises the provision of all identifiers (IMPU and IMPI) that are or were assigned to the requested identifier (IMPU or IMPI) at the relevant point in time for the provision of a specific telephone and multimedia service, and the term of validity of this assignment.

2 The request for information shall specify the relevant point in time, the requested identifier and its type (IMPU or IMPI).

**Art. 48*b***[97] Information Request Type IR_52_ASSOC_TEMP: Immediate information on identifiers assigned on a short-term basis

1 Information Request Type IR_52_ASSOC_TEMP comprises the provision of the permanent identifiers (e.g. SUPI) that are assigned to the requested temporary identifiers (e.g. SUCI, 5G-GUTI) at the time that the provision of a specific telecommunications service is requested.

2 The request for information shall specify the requested temporary identifiers and the associated mobile area.

**Art. 48*c***[98] Information Request Type IR_53_TEL_ADJ_NET: Determination of the adjacent networks in the case of telephony and multimedia services

1 Information Request Type IR_53_TEL_ADJ_NET comprises, if applicable, the determination and provision of the name of the networks directly adjacent to a communication or an attempt at communication in the case of telephony and multimedia services (e.g. Inter-Operator-Identifier, IP-address).

2 The request for information shall specify the communication or attempt at communication to which the request relates. It shall contain the following query criteria:

a. the time of the communication or attempt at communication;

96 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
97 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
98 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

b. the addressing resources to which the communication or attempt at communication was addressed; and

c. if available, the addressing resources for the origin of the communication or the attempt at communication.

## Section 7
## General Provisions on the Surveillance of Telecommunications

**Art. 49** Order to conduct surveillance of telecommunications

[1] The surveillance order submitted to the PTSS shall contain the following data:

a. the contact data of the ordering authority;

b. the contact data of the authorised persons envisaged as recipients of the surveillance data;

c. if known, the surname, first name, date of birth, address and occupation of the person to be placed under surveillance;

d. the reference numbers and case names for the surveillance activities;

e. the reason for surveillance, in particular the offence to be investigated by means of surveillance;

f. the names of the persons or entities required to cooperate;

g. the types of surveillance ordered or the type of special surveillance;

h. the identifiers subject to surveillance (target ID);

i. if necessary, an application for general authorisation for the surveillance of several connections without authorisation in specific cases (Art. 272 para. 2 and 3 CrimPC or Art. 70*c* para. 2 and 3 MCPC);

j. the starting date and the duration of the surveillance;

k. in the case of persons bound by professional secrecy in accordance with Article 271 CrimPC or Article 70*b* MCPC: a note to this effect;

l. if need be, measures to protect persons holding professional secrets and further protection measures that the authorities and the PTSS must take.

[2] If conducting the surveillance so requires, the FDJP may provide that the surveillance order submitted to the PTSS must include further technical data.

**Art. 50** Surveillance duties

[1] Each TSP, with the exception of those with reduced surveillance duties (Art. 51), and each PDCS with more extensive surveillance duties (Art. 52) must be able to conduct the surveillance activities in Sections 8–12 of this Chapter (Art. 54–69) that relate to services that they provide, or they must be able to arrange for third parties to conduct the surveillance. PDCSs with more extensive surveillance duties are not required

to conduct the types of surveillance in Articles 56*a*, 56*b*, 67 letters b and c and 68 paragraph 1 letters b and c.[99]

2 The provider shall ensure its ability to conduct surveillance of telecommunications from the commercial launch of a service provided to customers.

3 It shall ensure that it can accept surveillance assignments outside normal working hours in accordance with Article 10 and can conduct them or arrange for third party to do so in accordance with the FDJP requirements.

4 It shall guarantee that within the period specified in the surveillance assignment surveillance will be conducted of all telecommunications traffic carried on the infrastructures under its control provided the traffic is part of the services under surveillance and can be assigned to the target ID[100].

5 It shall support the PTSS, at its request, in order to ensure that the transmitted surveillance data actually corresponds to the telecommunications traffic specified in the surveillance assignment.[101]

6 If additional identifiers are associated with the target ID (e.g. IMPI with IMPU, email address with alias address, extra-SIM, multi-device), the provider shall ensure that these identifiers are also monitored as part of the type of surveillance.[102]

7 In the case of real-time surveillance of mobile services, relevant network elements such as HLR, HSS and UDM shall also be monitored, in particular to record information about the network providing the service, a change in the assigned service and device identifiers, location-related events, a change in the network element providing the service, and identification and authentication events involving the target ID and shall be transmitted to the IRI in standardised form.[103]

8 In the case of real-time surveillance in the IMS, determination of location data for the target ID from the network side shall if necessary be initiated.[104]

9 If a new terminal device (multi-device) or a new SIM (extra SIM) is added to a service when real-time surveillance or periodic position determination is already active, this device or SIM must also be monitored. No additional fee is payable for this and no additional compensation is paid. If necessary, the provider may request an additional administrative identification number for the surveillance.[105]

### Art. 51 TSPs with reduced surveillance duties

1 At the request of a TSP, the PTSS shall declare it to be a TSP with reduced surveillance duties (Art. 26 para. 6 SPTA) if it:

99 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
100 Term in accordance with No 1 para. 2 of the FA of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685). This amendment is made in the provisions specified in the AS.
101 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
102 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
103 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
104 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
105 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

a. only offers its telecommunications services in the field of education and research; or

b. meets neither of the following criteria:

1. surveillance assignments for 10 different surveillance targets in the past 12 months (effective date: 30 June),

2. annual turnover in Switzerland from telecommunications services and derived communications services of CHF 100 million in two successive financial years.

2 Article 22 paragraph 2 applies to the calculation of the values specified in paragraph 1 letter b.

3 TSPs with reduced surveillance duties are required to give written notice to the PTSS with supporting documents if they:

a. no longer offer their services exclusively in the field of education and research; or

b. achieve the value specified in paragraph 1 letter b number 2 for a second successive financial year; notice must be given within three months of the end of the financial year.

4 The PTSS may rely on data obtained in implementing the legislation relating to the surveillance of post and telecommunications or by other authorities in implementing federal law.

5 A provider that is declared to have more extensive duties to provide information must ensure that it can store the data required for providing information and provide the information within 2 months and 12 months of the declaration respectively.

**Art. 52** PDCSs with more extensive surveillance duties

1 The PTSS shall in a ruling declare a PDCSs to have more extensive surveillance duties (Art. 27 para. 3 SPTA) if it has met one of the following criteria:

a. surveillance assignments for 10 different surveillance targets in the past 12 months (effective date: 30 June);

b. annual turnover in Switzerland of CHF 100 million in two successive financial years, provided a large part of its business operations is providing derived communication services, and 5000 subscribers use the provider's services.

2 Article 22 paragraphs 2–5 apply *mutatis mutandis*.

**Art. 53**[106] Access to the installations

1 The persons or entities required to cooperate that must allow the PTSS or the third parties that it instructs access to its installations and shall allow the PTSS or the third parties access to buildings, devices, lines, systems, networks and services to the extent that this is required for surveillance or for making test connections.

106 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

2 They shall make existing means of network access to public telecommunications networks available free of charge. By agreement with the PTSS or the third parties that it instructs, they shall provide new means of network access at the expense of the PTSS to the extent that this is required for surveillance.

## Section 8
## Types of Real-Time Monitoring of Network Access Services

**Art. 54**[107] Surveillance Type RT_22_NA_IRI: Real-time monitoring of secondary telecommunications data in the case of network access services

1 Surveillance Type RT_22_NA_IRI comprises the real-time surveillance of a network access service in the mobile communications sector.

2 The following secondary telecommunications data of telecommunications traffic sent or received via the network access service under surveillance must be transmitted in real time:

a. when access to the network is established or disconnected: the date, the time, the type of event and the technology and, if applicable, the reason for disconnection;

b. the type of current access to the network;

c. the AAA information used by the network access service under surveillance, in particular the subscriber identifiers and the associated IMSI or SUPI;

d. the IP addresses assigned to the network access service and the associated terminal devices under surveillance and the date and time of each assignment;

e. the available addressing resources and identifiers of the network access service under surveillance, in particular the associated MSISDN or GPSI and the associated IMSI or SUPI;

f. the unique device identifiers in accordance with international standards for the currently associated terminal devices of the network access service under surveillance (e.g. IMEI, PEI, MAC address);

g. the type, date and time of the start and if applicable the end of events that modify the technical properties of the network access service under surveillance or its mobility management, and, if known, their causes;

h. the current location data for the target, the cells used or the non-3GPP access used, determined by the network if possible and indicated accordingly, whereby the location information relating to the target from NAS signalling messages shall also be transmitted and, in the case of EPS and 5GS, the location information shall be supplemented with the respective associated time stamp or the age of the location data, if available;

107 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

i. if possible, information on the previous and current network providing the service;

j. information about any change in the assigned service and device identifiers, location-related events and if applicable their reason, about any change in the network element providing the service and identification and authentication events involving the target;

k. in the case of 5G-technology: additional information about assigning a new temporary identifier for the target.

[3] The location data comprise the associated timestamps and, if available, the type of network access point technology used and:

a. the identifiers (e.g. cell or geographical area identifier) and the geographical coordinates of the cells and if applicable the directions of emission of the cells and in the case of a combined cell, additional location data in accordance with the applicable FDJP regulations;

b. the position of the target determined by the network, for example in the form of geographical coordinates and the related uncertainty value, or in the form of polygons with details of the geographical coordinates of each polygon point;

c. other data on the location of the target or of the cells in accordance with international standards;

d. in the case of a non-3GPP access:

1. the identifiers or another suitable designation (e.g. hotspot name) for the non-3GPP access, the public source IP address for the secured connection of the target to the gateway and, in the case of NAT, the source port number and the protocol, or

2. the identifier for the network access point and, if available, its postal address.

**Art. 55** Surveillance Type RT_23_NA_CC_IRI: Real-time monitoring of content and secondary telecommunications data in the case of network access services

Surveillance Type RT_23_NA_CC_IRI involves the real-time surveillance of a network access service. The content of the telecommunication sent or received via the network access service under surveillance, and the related secondary telecommunications data in accordance with Article 54 paragraphs 2 and 3 must be transmitted in real time.

## Section 9 Types of Real-Time Monitoring of Applications

### Art. 56[108] Surveillance Type RT_24_TEL_IRI: Real-time monitoring of secondary telecommunications data for telephony and multimedia services

[1] Surveillance Type RT_24_TEL_IRI comprises the real-time monitoring of a telephony and multimedia service and, if applicable, the real-time monitoring of converging services, in particular SMS, voice mail and RCS.

[2] The following secondary telecommunications data of the telecommunication that is sent, processed or received via the services under surveillance must be transmitted in real time:

a. the date and the time of logging-in and logging-out processes and their result;

b. the AAA information used by the services under surveillance and the information on registration and subscription events and the corresponding responses, in particular the subscriber identifier (e.g. SIP URI, IMPI) and the IMSI in the case of mobile services or the SUPI and if applicable, the customer's and server's IP addresses and port numbers as well as details of the protocol used;

c. the signalling information, in particular on the serving system, on subscriber status and on service quality;

d. if applicable, the presence information;

e. in the case of communications, communication attempts and technical modifications (e.g. inclusion of additional services, inclusion of converging services or change to converging services, changes in network access technology, location updates), if applicable:

1. their type, the date and the time of their start and if applicable their end,
2. the addressing resources (e.g. MSISDN, GPSI, E.164-number, SIP URI, IMPU) of all subscribers in communication and their role,
3. the actual known destination address and the available intermediate addresses where the communication or the communication attempt is diverted or forwarded,
4. the unique device identifiers in accordance with international standards for the terminal devices of the services under surveillance (e.g. IMEI, PEI, MAC address),
5. the other available identifiers,
6. the reasons for the termination of communication or its non-materialisation or for the technical modification,
7. the signalling information on additional services (e.g. conference calls, call forwarding, DTMF),
8. the status of the communication or of the communication attempt,

[108] Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

9. in the case of mobile services: in addition the current location data in accordance with Article 54 paragraphs 2 letter h and 3 determined by the network if possible and indicated accordingly;

f. in the case of mobile services: additional information about the previous and current network providing the service, any change in the assigned service and device identifiers, location-related events and if applicable their reason, any change in the network element providing the service, and identification and authentication events involving the target.

**Art. 56*a***[109] Surveillance Type RT_54_POS_ONCE: Immediate non-recurrent position determination by the network

[1] Surveillance Type RT_54_POS_ONCE comprises in each case the immediate non-recurrent position determination by the network of all mobile terminal devices associated with the target ID.

[2] Position determination shall be carried out by the network using an immediate positioning function in accordance with the FDJP regulations.

[3] The following data shall be transmitted immediately:

a. the MSISDN or GPSI, IMEI or PEI and IMSI or SUPI observed, at least one of these data, and any of the others if available;

b. network identifier for the location service client and the timestamp of the position determined;

c. in the case of successful position determination: the timestamp of the position and the following position data:
   1. if available, the positioning method,
   2. if available, data on the accuracy of the position,
   3. the position in the form of:
      – geographical coordinates and if applicable the associated uncertainty values
      – polygons, with details of the geographical coordinates of each polygon point or
      – other data in accordance with international standards, and
   4. if available, the altitude data for the position, the service quality, the movement status and the speed and direction of movement of the terminal device;

d. in the case of unsuccessful position determination: the reason for failure (error code) and the location data specified in Article 63 for the most recent detectable activity, at no additional cost.

[109] Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

**Art. 56*b***[110] Surveillance Type RT_55_POS_PERIOD: Recurrent position determination by the network

[1] Surveillance Type RT_55_POS_PERIOD comprises in each case the recurrent position determination by the network of all mobile terminal devices associated with the target ID.

[2] Position determination shall be carried out by the network using a regular positioning function in accordance with the FDJP regulations.

[3] The following data shall be transmitted immediately:

a. the MSISDN or GPSI, IMEI or PEI and IMSI or SUPI observed, at least one of these data, and any of the others if available;

b. network identifier for the location service client and the timestamp of the position determined;

c. in the case of successful position determination, the timestamp of the position and the following position data:
   1. the positioning method,
   2. data on the accuracy of the position,
   3. the position in the form of:
      – geographical coordinates and if applicable the associated uncertainty values
      – polygons, with details of the geographical coordinates of each polygon point or
      – other information in accordance with international standards, and
   4. if available, the altitude data for the position, the service quality, the movement status and the speed and direction of movement of the terminal device;

d. in the case of unsuccessful position determination: the reason for failure (error code).

**Art. 57** Surveillance Type RT_25_TEL_CC_IRI: Real-time surveillance of content and secondary telecommunications data in the case of telephony and multimedia services

Surveillance Type RT_25_TEL_CC_IRI comprises the real-time surveillance of a telephony and multimedia service and, if applicable, converging services, in particular SMS, voice mail and RCS. The content of the telecommunications traffic sent, processed or received via the services under surveillance, as well as the related secondary telecommunications data in accordance with Article 56 must be transmitted in real time.

110 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

**Art. 58** Surveillance Type RT_26_EMAIL_IRI: Real-time monitoring of secondary telecommunications data on email services

Surveillance Type RT_26_EMAIL_IRI comprises the real-time surveillance of an email service. The following secondary telecommunications data on the telecommunications traffic sent, processed or received via the service under surveillance must be transmitted in real time:

a. the date and the time of logging-in and logging-out processes and their status;

b. the AAA information used by the service under surveillance, in particular the subscriber identifier and, if applicable, the alias address;

c. the customer's and server's IP addresses and port numbers as well as details of the protocol used;

d. the date, time, volume of data, email addresses of the sender and the recipient of the message and the IP addresses and port numbers of the sending and receiving email servers for the following events:

1. sending or forwarding of a message,
2. receipt of a message,
3. processing of a message in the mailbox,
4. downloading of a message from the mailbox,
5. uploading of a message to the mailbox.

**Art. 59** Surveillance Type RT_27_EMAIL_CC_IRI: Real-time monitoring of content and secondary telecommunications data on email services

Surveillance Type RT_27_EMAIL_CC_IRI comprises the real-time surveillance of an email -service. The content of the telecommunications traffic sent, processed or received via the service under surveillance, as well as the related secondary telecommunications data in accordance with Article 58 must be transmitted in real time.

## Section 10 Types of Retroactive Surveillance

**Art. 60**[111] Surveillance Type HD_28_NA: Retroactive surveillance of secondary telecommunications data in the case of network access services

Surveillance Type HD_28_NA comprises the retroactive surveillance of secondary telecommunications data of a network access service. The following secondary telecommunications data of the telecommunication that has been sent or has been received via the network access service under surveillance must be transmitted:

a. the date and the time of the start and if applicable the end or the duration or the session;

b. the type and status of the network access;

111 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

c. the identifier that was used for authenticating the user at the access point under surveillance, for example the user name;

d. the IP address assigned to the target and their type or in the case of non-3GPP access the public source IP address for the secured connection of the target to the gateway and the associated source port number;

e. the unique device identifier of the terminal device used by the target in accordance with international standards (e.g. MAC address, IMEI or PEI in the case of mobile services);

f. the volumes of data that were uploaded and downloaded during the session;

g. in the case of mobile services: the GPRS, EPS or 5GS information (in particular IMSI, SUPI, MSISDN. GPSI) and the location data at the beginning, end of and during the session in accordance with the applicable FDJP regulations;

h. in the case of access to the network via a professionally operated public WLAN: the identifiers (e.g. BSSID) or other suitable designations (e.g. hotspot name), the location data (geographical coordinates or postal address) and, if available, the type of authentication, an identifier that enables a request for the identification data in accordance with Article 19 paragraph 2 to be made and the IP-address of the access used by the target;

i. if available, in addition to the data in letters g and h, the location information from maritime navigation or aviation;

j. in the case of fixed network access: the addressing resources of the access and. if available, the postal address.

### Art. 61 Surveillance Type HD_29_TEL: Retroactive surveillance of secondary telecommunications data relating to telephony and multimedia services

Surveillance Type HD_29_TEL comprises the retroactive surveillance of secondary telecommunications data of a telephony and multimedia service and, if applicable, converging services, in particular SMS, voice mail and RCS. The following secondary telecommunications data of the past telecommunications traffic in communications and communication attempts using the services under surveillance must be transmitted:[112]

a. their type, the date and time of the start and, if applicable, the end or their duration;

b.[113] the addressing resources (e.g. MSISDN, GPSI, E.164 number, SIP URI, IMPU) of all persons communicating with each other and their roles;

c. the reason for the end of the communication or the communication attempt;

d.[114] in the case of mobile services: IMEI or PEI of the terminal device used by the target and the IMSI or SUPI of the target;

112 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
113 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
114 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

e. if applicable, the type of carrier service;

f. in the case of SMS and MMS: the information on the event, the type (only in the case of SMS) and the status;

g.[115] in the case of mobile services: the location data determined by the network if possible and indicated accordingly for the cell or the non-3GPP access used by the target at the beginning and at the end of the communication or the communication attempt and, if available, during the communication, in accordance with the applicable FDJP regulations;

1. the cell and geographical area identifiers, the geographical coordinates and if applicable the main directions of emission and the postal address, or
2. the positions of the target determined by the network (e.g. in the form of geographical coordinates and the related uncertainty value or in the form of polygons with details of the geographical coordinates of each polygon point) as well as the related postal addresses, or
3. other details in accordance with international standards of the target's locations or the cells that he or she used, as well as the related postal addresses;

g$^{bis}$.[116] if available, in addition to the data in letter g, the location information from maritime navigation or aviation;

h. in the case of multimedia services:

1. the customer's IP address and its type and the port number,
2. the communication correlation identifier,
3. the types of multimedia content,
4. information on the multimedia components (time, name, description, initiator, access-correlation identifier), and
5. if applicable, information on the IMS services (type of IMS service used, role of the network element from which the secondary telecommunications data come);

i.[117] in the case of multimedia services: information on the target's network access:

1. the access type,
2. the access class,
3. an indication of whether the information on access to the network comes from the network, and
4. the location data relating to the network access at the beginning and the end of the multimedia session, and, if available, during the multimedia session in accordance with the applicable FDJP regulations;

115 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
116 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
117 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

j.[118] if applicable, the name of networks directly adjacent to the communication or the attempt at communication.

**Art. 62**[119] Surveillance Type HD_30_EMAIL: Retroactive surveillance of secondary telecommunications data in the case of email services

Surveillance Type HD_30_EMAIL comprises the retroactive surveillance of secondary telecommunications data of an email service. The following secondary telecommunications data of the past telecommunication sent, processed or received via the service under surveillance must be transmitted:

a. the date, the time, the type of event, the subscriber identifiers, if applicable the alias address, the sender and recipient addresses, the protocol used, the IP addresses and port numbers of the server and the client, and, if applicable, the delivery status of the message in the case of the following events: sending, receipt, mailbox log-in, mailbox log-out and in the case of the following events, if available: downloading, uploading, deletion, processing, addition of a message;

b. the IP addresses and names of the sending and receiving email servers.

**Art. 63**[120] Surveillance Type HD_31_PAGING: Determination of the location of the most recent activity

[1] Surveillance Type HD_31_PAGING comprises the determination of the location of the most recent activity detectable by the mobile telephony provider (network access services, telephony and multimedia services) for all mobile terminal devices associated with the target ID of the person under surveillance.

[2] The following data shall be transmitted:

a. the MSISDN or the GPSI;

b. the IMSI or the SUPI;

c. if available, the IMEI or der PEI;

d. the type of network access point technology;

e. if applicable, the frequency band;

f. the unique identifier for the mobile network;

g. the date and time of the most recent detectable activity for network access services and telephony and multimedia services; and

h. the location data in accordance with the applicable FDJP regulations.

118 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
119 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
120 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

**Art. 64** Surveillance Type AS_32_PREP_COV: Network coverage analysis in preparation for an antenna search

[1] Surveillance Type AS_32_PREP_COV comprises the network analysis in preparation for an antenna search in accordance with Article 66. It is carried out by the TSPs and serves to identify the mobile radio cells or public WLAN access points that most probably cover the location described by the ordering authority in the form of geographical coordinates or by means of postal address, if applicable taking account of additional information (e.g. time of day, weather, day of the week, location within or outside of a building).

[2] TSPs shall supply the PTSS with a list of cell or geographical area identifiers for the mobile radio cells and identifiers identified (e.g. BSSID) or other suitable designations (e.g. hotspot name) for the professionally operated public WLAN access points identified.[121]

**Art. 65** Surveillance Type AS_33_PREP_REF: Reference communications or instances of reference network access in preparation for an antenna search

[1] Surveillance Type AS_33_PREP_REF comprises the identification of mobile radio cells or public WLAN access points on the basis of reference communications and instances of reference network access in preparation for an antenna search in accordance with Article 66.

[2] The ordering authority shall itself arrange for reference communications to be made and the reference network to be accessed at the relevant location and shall send the PTSS a list with the following related data:[122]

a. the type of communication or of access to the network;

b. the date and the time of the communication or access to the network;

c. the addressing resource of the telephony and multimedia service used or of the network access service;

d. if applicable, the name of the mobile network used.

[3] The PTSS shall instruct the TSPs, on the basis of the secondary telecommunications data relating to previous telecommunications traffic, to identify the mobile radio cells or public WLAN access points used in each case at the beginning and at the end of the reference communications and instances of reference network access in accordance with paragraph 2 and to provide it with a list of the corresponding cell or geographical area identifiers der mobile cells, the associated identifiers (e.g. BSSID) or suitable designations (e.g. hotspot name) for the WLAN accesses completed in accordance with paragraph 2.[123]

121 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
122 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
123 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

**Art. 66** Surveillance Type AS_34: Antenna search

[1] Surveillance Type AS_34 comprises the retroactive surveillance of all communications, communication attempts and instances of network access that have taken place via a specific mobile radio cell or a specific public WLAN access point over a period of up to two hours.[124]

[2] The TSP shall supply the secondary telecommunications data resulting from paragraph 1 relating to previous telecommunications traffic in accordance with Article 60 and 61.

## Section 11
## Missing Person and Wanted Person Searches and Mobile Phone Localisation of Suspected Terrorists[125]

**Art. 67**[126] Types of surveillance EP: Missing person search

The following types of surveillance may be ordered for a missing person search in accordance with Article 35 SPTA:

a. Type EP_35_PAGING: determining the location of the most recent activity detectable by the mobile telephony provider of all mobile terminal devices associated with the target ID of the missing person or a third party; this type corresponds to Type HD_31_PAGING in accordance with Article 63;

b. Type EP_56_POS_ONCE: the immediate non-recurrent position determination by the network of all mobile terminal devices associated with the target ID of the missing person or a third party; this type corresponds to Type RT_54_POS_ONCE in accordance with Article 56*a*;

c. Type EP_57_POS_PERIOD: the recurrent position determination by the network of all mobile terminal devices associated with the target ID of the missing person or a third party; this type corresponds to Type RT_55_POS_PERIOD in accordance with Article 56*b*;

d. Type EP_36_RT_CC_IRI: real-time surveillance of content and secondary telecommunications data; this type corresponds to the combination of types of surveillance in accordance with Article 55 (network access services) and in accordance with Article 57 (telephony and multimedia services);

e. Type EP_37_RT_IRI: real-time surveillance of secondary telecommunications data; this type corresponds to the combination of types of surveillance in accordance with Article 54 (network access services) and in accordance with Article 56 (telephony and multimedia services);

f. Type EP_38_HD: retroactive surveillance of secondary telecommunications data); this type corresponds to the combination of types of surveillance in

124 The correction of 3 July 2018 relates to the Italian text only (AS **2018** 2551).
125 Amended by No I 12 of the O of 4 May 2022 on Police Counterterrorism Measures, in force since 1 June 2022 (AS **2022** 301).
126 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

accordance with Article 60 (network access services) and in accordance with Article 61 (telephony and multimedia services).

**Art. 68**[127] Wanted person search

[1] The following types of surveillance may be ordered for a search for convicted persons in accordance with Article 36 SPTA; "wanted person search" must be indicated in the surveillance order as the reason for surveillance (Art. 49 para. 1 let. e):

a. the location determination in the case of the most recent activity detectable by the mobile service provider of all mobile terminal devices associated with the target ID of the convicted person or a third party in accordance with Article 63;

b. the immediate non-recurrent position determination by the network of all mobile terminal devices associated with the target ID of the convicted person or a third party in accordance with Article 56*a*;

c. the recurrent position determination by the network of all mobile terminal devices associated with the target ID of the convicted person or a third party in accordance with Article 56*b*;

d. any of the types of real-time surveillance of the content and secondary telecommunications data of network access services or applications in accordance with Articles 55, 57 or 59;

e. any of the types of real-time surveillance of secondary telecommunications data of network access services or applications in accordance with Articles 54, 56 or 58;

f. any of the types of retroactive surveillance in accordance with Articles 60–62;

g. an antenna search in accordance with Article 66 and the corresponding preparations in accordance with Articles 64 and 65.

[2] In the case of the surveillance type in paragraph 1 letter f, the start and end of the surveillance are governed by Article 4*a*.

**Art. 68*a***[128] Surveillance Type ML_50_RT: Mobile phone localisation of suspected terrorists in real time

[1] Surveillance Type ML_50_RT may be ordered for the mobile phone localisation of suspected terrorists in accordance with Article 23*q* paragraph 3 of the Federal Act of 21 March 1997[129] on Measures to Safeguard Internal Security.

[2] It comprises the combination of real-time surveillance of the secondary telecommunications data required for mobile phone localisation in the case of mobile network

127 Amended by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).
128 Inserted by No I 12 of the O of 4 May 2022 on Police Counterterrorism Measures, in force since 1 June 2022 (AS **2022** 301).
129 SR **120**

access services, mobile telephony and multimedia services and, if applicable, convergent mobile services, in particular SMS, Voice Mail and RCS.

3 In the case of mobile network access services, the secondary telecommunications data from telecommunications traffic in accordance with Article 54 paragraph 2 letters a–c, g and h and paragraph 3 must be transmitted.

4 In the case of mobile telephony and multimedia services and convergent mobile services, the secondary telecommunications data from telecommunications traffic in accordance with Article 56 paragraph 1 letters a, b, d and e numbers 1 and 9 and paragraph 2 must be transmitted.

## Section 12 Off-Network Identifiers

### Art. 69

Surveillance in accordance with Articles 56–59, 61 and 62 also includes telecommunication carried out via the services under surveillance that can be assigned to the target ID even if the identifier under surveillance is not administered by the provider given the assignment.

## Chapter 4 Final Provisions

### Art. 70 Organisational, administrative and technical regulations

The FDJP shall issue the organisational, administrative and technical regulations on conducting surveillance of post and telecommunications. In particular, it shall determine the deadlines within which the relevant data must be supplied.

### Art. 71 Implementation

1 The PTSS shall provide electronic forms and interfaces to be used by those concerned. The forms and interfaces shall make it possible in particular for:

a. the ordering authorities:
   1. to submit a surveillance order to the PTSS,
   2. to instruct the PTSS to grant or amend rights of access;
b. the PTSS:
   1. to instruct the persons or entities required to cooperate with conducting a surveillance measure,
   2. to pass on a request for information to the persons or entities required to cooperate and to forward their answers to the requesting authority;
c. the authorised authorities to submit a request for information to the PTSS.

2 The PTSS may at the appropriate time replace the electronic forms with online access to the Service's processing system and introduce an electronic approval process

for orders requiring approval. The electronic forms may continue to be used if online access to the processing system is impossible for technical reasons or if the processing system fails.

**Art. 72** Repeal of another enactment

The Ordinance of 31 October 2001[130] on the Surveillance of Post and Telecommunications is repealed.

**Art. 73** Amendment of other enactments

The ordinances below are amended as follows:

…[131]

**Art. 74** Transitional provisions

[1] Surveillance activities ordered before this Ordinance comes into force shall continue unchanged. These activities shall be extended or terminated in accordance with the previous law applicable to those types of surveillance.

[2] Test connections ongoing in accordance with the previous practice when this Ordinance comes into force shall be terminated.

[3] TSPs that submit an application to the PTSS for categorisation as a TSP with reduced surveillance duties in accordance with Article 51 within three months of this Ordinance coming into force shall be deemed to be such from the date on which this Ordinance comes into force and for the duration of the procedure. The PTSS may revoke this categorisation for the duration of the procedure if approval of the application is unlikely. Article 51 paragraph 5 does not apply to TSPs previously required to report.

[4] Within 3 months of this Ordinance coming into force, TSPs and PDCSs with more extensive duties to provide information in accordance with Article 22 shall modify their systems in order to implement the new requirements on the identification the subscribers (Art. 19) and recording persons' data in the case of mobile services (Art. 20).

[5] Within 6 months of this Ordinance coming into force, TSPs, with the exception of those with reduced surveillance duties in accordance with Article 51, and PDCSs with more extensive surveillance duties in accordance with Article 52 shall modify their systems in order to be able to supply the information specified in Articles 38 and 39.

[6] Within 24 months of this Ordinance coming into force:

a. it must be possible to supply the secondary telecommunications data on communication attempts in the case of retroactive surveillance activities;

b. TSPs must make technical modifications to the systems they have available in order to be able to supply the data on email services specified in Articles

130 [AS **2001** 3111; **2004** 1431, 2021 Art. 7, 3383; **2006** 4705 No II 77; **2007** 4029; **2011** 5955; **2016** 4337 No II; **2017** 4151 Annex 4 No II 11]

131 The amendments may be consulted under AS **2018** 147.

58, 59 and 62. Before then, they must supply the data on email services in the same way as before.

7 Until the new processing system procured under the telecommunications surveillance[132] programme comes into operation:

a. the PTSS may continue to compile statistics (Art. 12) in accordance with the previous law;

b. information provision (Art. 35–48) and surveillance activities (Art. 54–68) shall continue to be carried out with the existing system, the previous formats and the corresponding forms. They shall be transmitted using a secure means of transmission authorised by the PTSS, by post or fax; Article 17 paragraphs 1–2 does not apply;

c. information provision based on a flexible name search in accordance with Article 27 in conjunction with Articles 35, 40, 42 and 43 is not possible; from the date on which the new system comes into operation, it will only be carried out by TSPs and PDCSs with more extensive duties to provide information in accordance with Article 22 that have modified their systems accordingly.

8 Within 12 months of the new processing system coming into operation, TSPs and PDCSs with more extensive duties to provide information in accordance with Article 22 shall modify their systems in order to supply the information specified in Articles 35–37 and 40–42 and in Article 27 in conjunction with Articles 35, 40 and 42 automatically via the query interface of the processing system (Art. 18 para. 2) and in order to be able to carry out the flexible name search in accordance with Article 27 in conjunction with Articles 35, 40, 42 and 43.

**Art. 74*a*[133]** Transitional provision to the Amendment of 4 May 2022 relating to the mobile phone localisation of suspected terrorists

1 The PTSS shall adapt its processing system within 12 months of the replacement of the real-time system components of the processing systems in order to be able to conduct the mobile phone localisation of suspected terrorists in a standardised manner and record the same in the statistics.

2 The TSPs, with the exception of those with reduced surveillance duties (Art. 51), and PDCSs with more extensive surveillance duties (Art. 52) shall adapt their systems within 12 months of the replacement of the real-time system components of the processing systems in order to be able to conduct the mobile phone localisation of suspected terrorists (Art. 68*a*) in a standardised manner.

3 If the mobile phone localisation of suspected terrorists cannot yet be conducted in a standardised manner in accordance with Article 68*a*, providers shall instead conduct the types of surveillance specified in Article 54 and, if required, Articles 56 and 63. The PTSS shall pass on the data in accordance with Articles 54 and 63 to the authorised authorities. The PTSS shall only pass on the data in accordance with Article 56

132 BBl **2015** 3033
133 Inserted by No I 12 of the O of 4 May 2022 on Police Counterterrorism Measures, in force since 1 June 2022 (AS **2022** 301).

to the extent specified in Article 68*a*. If its processing system is unable to guarantee this filtering, it shall not pass on any data. It shall destroy data that it does not pass on. The fees and compensation are determined by the type of surveillance ordered (Art. 54, 56 and 63).

**Art. 74*b***[134] Transitional provision to the Amendment of 15 November 2023

[1] TSPs shall be ready to provide the information in accordance with Articles 48*a* and 48*c* within 24 months of the Amendment of 15 November 2023 coming into force.

[2] The TSPs, with the exception of those with reduced surveillance duties (Art. 51), must be able to provide the information in accordance with Article 48*b* in standardised form from the time at which their first commercial mobile network access point which conceals the permanent identifiers on the radio interface comes into operation.

[3] They must be able to carry out the surveillance procedures in standardised form in accordance with Articles 56*a* and 67 letter b within 24 months of the Amendment of 15 November 2023 coming into force.

[4] They must the implement the additional type of retroactive surveillance in accordance with Article 61 letter j within 24 months and ensure the saving of the data required therefor within 18 months of the Amendment of 15 November 2023 coming into force.

[5] They must be able to carry out the surveillance procedures in standardised form in accordance with Articles 56*b* and 67 letter c within 24 months of the replacement of the real-time system components of the processing systems.

[6] The PTSS shall adapt its processing system within 24 months of the Amendment of 15 November 2023 coming into force, so that:

a. the information in accordance with Articles 48*a* and 48*c* can be provided in standardised form and the surveillance procedures in accordance with Articles 56*a* and 67 letter b can be carried out and be recorded in the statistics in standardised form;

b. the data in accordance with Article 61 letter j can be received.

[7] It shall adapt its processing system so that information in accordance with Article 48*b* can be provided and recorded in the statistics in standardised form from the time at which their first commercial mobile network access point which conceals the permanent identifiers on the radio interface comes into operation.

[8] It shall adapt its processing system within 24 months of the replacement of the real-time system components of the processing systems so that the surveillance procedures in accordance with Articles 56*b* and 67 letter c in can be carried out and recorded in the statistics in standardised form.

**Art. 75** Commencement

This Ordinance comes into force on 1 March 2018.

134 Inserted by No I of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

*Annex*[135]
(Art. 2)

## Terms and abbreviations

1. *Communication service*: service that enables communication using telecommunications technology; it includes telecommunications services and derived communication services;
2. *Subscribers:* persons who have entered into a contract with a TSP or a PDCS in order to use their services or who have registered for their services or have been granted access by a TSP or a PDCS to their services;
3. *WLAN*: wireless local area network;
4. *Identifier:* addressing resource, identification number or any other unique indicator of a specific subscriber, service or device;
5. *IP address (internet protocol address):* address that identifies all devices connected to a network that communicate using the internet protocol; there are Version 4 (IPv4) and the Version 6 (IPv6) IP addresses;
6. *Port number:* address of a port; a port is the logical end point for communications with or within a computer system; a port is linked to an IP address and the communication protocol type;
7. *NAT (network address translation):* procedure for translating network addresses. The address information in IP packages is automatically replaced with other address information by a network element (e.g. router);
8. *Telephony service:* interactive service that allows simultaneous real-time voice communication between persons communicating with each other, with addressing according to a numbering plan; a provider's answerphone systems associated with a telephony service (e.g. voice box, voice mail, visual voice mail) are also regarded as a telephony service;
9. *Multimedia service:* more sophisticated telephony service, with which, in addition to speech, other types of media and functions can be used, such as video, images, audio, file transfer, parts of content, presentation of content, transmission of presence information (e.g. video telephony, unified communication, RCS, conference calls, video conference calls, online meetings);
10. *GPSI (Generic Public Subscription Identifier):* unique public addressing resource within and outside 5G networks (e.g. MSISDN);
11. *MSISDN (Mobile Subscriber Integrated Services Digital Network Number):* unique telephone number on which subscribers to a mobile network can be called;
12. *IP prefix:* part of the IP address that identifies network concerned;
13. *IP address range:* a number of successive IP addresses;

135 Amended by No II of the O of 15 Nov. 2023, in force since 1 Jan. 2024 (AS **2023** 685).

14. *Net mask:* in internet protocol Version 4 (IPv4), describes how many bits at the start of the IP address displayed identify the network concerned;
15. *Prefix length:* in internet protocol Version 6 (IPv6), describes how many bits at the start of the IP address displayed identify the network concerned;
16. *ICCID (Integrated Circuit Card Identifier):* series-number of a smart card (e.g. ICCID of a SIM card) or a profile on a built-in chip (e.g. the EID of an eUICC) that uniquely identifies the chip or the profile worldwide;
17. *IMSI (International Mobile Subscriber Identity):* number that allows the unique international identification of mobile communication subscribers;
18. *SUPI (SUbscription Permanent Identifier):* number that allows the unique international identification of mobile subscribers in 5G networks;
19. *IMEI (International Mobile Equipment Identity):* number that allows the unique international identification of mobile communication terminals;
20. *PEI (Permanent Equipment Identifier):* number that allows the unique international identification of mobile communication terminals in 5G networks;
21. *MAC address (Media Access Control Address):* hardware address that is stored in a network card or a network adapter and that is used as the unique address at the level of OSI layer 2;
22. *SIM (Subscriber Identity Module):* smart card or chip permanently built into to the terminal device on which the IMSI or SUPI and the related key are securely stored; the SIM is used to authenticate the subscribers to a mobile network, and includes the *USIM (Universal Subscriber Identity Module), UICC (Universal Integrated Circuit Card) and eSIM (embedded SIM)*;
23. *PUK code (Personal Unblocking Key):* unchangeable PIN assigned to the SIM used to unblock the SIM if the PIN code has been entered incorrectly on several occasions;
24. *PUK2-Code (Personal Unblocking Key 2):* same as the PUK code, but assigned to the PIN2 code;
25. *eUICC-ID (shortened to EID, embedded Universal Integrated Circuit Card-Identifier)*: unique worldwide identifier for a chip permanently built into a terminal device, which hosts the SIM functions (see ICCID and SIM);
26. *Source IP address:* IP address that is assigned to the communication end point (normally the client) that establishes the connection;
27. *Source port number:* port number that is assigned to the communication end point (normally the client) that establishes the connection;
28. *Destination IP address:* IP address that is assigned to the communication end point (normally the server) with which the connection is established;
29. *Destination port number:* port number that is assigned to the communication end point (normally the server) with which the connection is established;
30. *SIP (Session Initiation Protocol):* communication protocol that is used for signalling and maintaining multimedia communication sessions;

31. *SIP URI (SIP Uniform Resource Identifier):* URI scheme for addressing the SIP. The SIP URI are addressing resources in the format *user@domain.tld*;
32. *IMPU (IP Multimedia Public Identity):* identifier that allows communication with other subscribers; a subscriber to the IMS has one or more IMPUs in addition to the IMPI; one IMPI may be assigned several IMPUs. Conversely an IMPU may also be shared with other subscribers;
33. *TEL URI (Telephone Uniform Resource Identifier):* URI scheme for telephone numbers. The TEL URI are addressing resources in the format *tel:number*, e.g. *tel:+41-868-868-868*;
34. *IMPI (IP Multimedia Private Identity):* internationally unique identifier in the IMS, assigned by providers to their subscribers, which is used inter alia for registration and AAA events.
35. *Email service:* mailbox or interface for reading, writing, editing, sending, receiving or forwarding emails, based on SMTP
36. *Alias address:* additional email address that the subscriber can set up, change and delete at will; the email provider determines its maximum number of alias addresses and their structure; the alias addresses are linked to the email account. An email sent to an alias address is delivered to the same email box as used for the subscriber's related main email address;
37. *Mailing list:* list of email addresses, also known as a distribution list or distribution group. The list has its own email address. The messages that are sent to the mailing list address are forwarded on to the email addresses of its members;
38. *Messaging services:* message transmitting services that are independent of from telephony and multimedia services. They include instant messaging, IMS messaging and messaging applications (apps) and SMS services from third-party providers (i.e. SMS services not provided by the subscriber's TSP). These services may also include additional functions such as multimedia communication, data transmission and presence information (e.g. a subscriber can see the current status and potentially the location of the other subscribers);
39. *Cell identifier:* unmodified identifier for radio cells in mobile networks, such as *CGI* (*Cell Global Identity*), *ECGI* (*E-UTRAN Cell Global Identity*), *NCGI* (*New Radio Cell Global Identity*);
40. *Geographical area identifier*: unmodified identifier for geographical areas in mobile networks, e.g. *SAI (Service Area Identity), RAI (Routing Area Identity), TAI (Tracking Area Identity);*
41. *Hotspot name (SSID)*: name of a hotspot freely chosen by the provider, which is generally easy to read and is displayed to users; a hotspot in terms of this Ordinance is public access to the internet via WLAN (Wi-Fi), as opposed to a stationary or mobile (tethering) private hotspot;
42. *Target ID:* identifier under surveillance, i.e. the identifier of the target of the surveillance;

43. *IRI (Intercept Related Information):* secondary telecommunications data of the target recorded during real-time surveillance. The data are normally also transmitted in real time; they must be distinguished from retained secondary telecommunications data (historical data), which are only selectively recorded, normally with a time delay, for the purpose of retroactive surveillance;
44. *HLR (Home Location Register)*: in second- and third-generation mobile networks; a database kept by a mobile service provider, in which the functional characteristics of its subscribers (e.g. IMSI, MSISDN, configuration, service profiles) and their current service-providing network are recorded;
45. *HSS (Home Subscriber Server)*: in fourth-generation mobile networks; a database with similar functions to the HLR;
46. *UDM (Unified Data Management):* in fifth-generation mobile networks; a database with similar functions to the HLR and HSS;
47. *IMS (IP Multimedia Subsystem):* a telecommunications system based on the internet that integrates mobile voice services and internet functions;
48. *AAA (authentication, authorisation and accounting information):* information on which subscribers are allowed to use which services, and information which is used to bill subscribers for service usage. For the purposes of this Ordinance, passwords are not regarded as AAA information. Authentication is the process by which a subscriber is identified before the access is granted. Authorisation determines which rights of access to resources or services that a subscriber holds and also guarantees access control. The subscriber's use of resources is measured for accounting purposes;
49. *3GPP (3rd Generation Partnership Project):* worldwide cooperation among standardisation bodies on standardisation in mobile communications;
50. *Non-3GPP access:* access to the mobile communications core network that is based on technology that is not standardised by the 3GPP (e.g. WLAN access);
51. *EPS (Evolved Packet System)*: architecture of the LTE mobile communication standard of 3GPP, marketed as "4G";
52. *5GS (5G-System)*: system architecture of the 5G mobile communication standard of the 3GPP;
53. *SMS (Short Message Service):* messaging service for transmitting short text messages;
54. *Voice mail:* storage devices used in telecommunication networks that offer answering services (e.g. receiving, forwarding and storing voice messages). There are extensions for various types of media and services, such as SMS, email, fax or video messages as well as function extensions such as converting from one type of media to another (e.g. text to voice) and the sending of messages;
45. *RCS (Rich Communications Services,* originally: Rich Communication Suite) specification of the international industry organisation for mobile telephony providers GSM Association, GSMA for the IMS based provision of

interoperable (i.e. cross-provider and cross-terminal) multimedia services with extended functional scope. Various types of media (e.g. language, music, photographs, videos) and services (e.g. chat, chat groups, calls, multimedia messages, short messages, instant messages, presence information, transmission of files, address books) can be combined; what is meant here is only the RCS services that are provided to subscribers by their mobile telephony provider;

56. *E.164 number:* telephone number in accordance with international numbering plan E.164 of the ITU-T;
57. *DTMF (Dual-Tone Multi-Frequency):* a signalling procedure, i.e. during a telephone conversation, sound signals can be sent by pressing the telephone keypad, for example to interact with answering machines or automatic voice response systems;
58. *BSSID (Basic Service Set Identifier):* unique identifier (MAC address) of the WLAN access point;
59. *Radio interface:* the interface for radio transmission in the mobile communications network, e.g. 5G New Radio (5G NR), also known as the air interface or 3GPP access.