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 3 December 2019)

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 the provision of information on postal and telecommunications services.

[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** 147
1 SR **780.1**
2 SR **312.0**
3 SR **322.1**

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

h. postal service providers (PSPs);

i. telecommunications service providers (TSPs);

j. the providers of services based on telecommunications services and that enable one-way or multi-way communication (providers of derived communication services);

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 Submissions to the PTSS

1 The ordering authority shall use one of the following transmission channels to submit surveillance orders and orders for their extension or termination to the PTSS and to notify it of the access rights to be established:

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

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

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

2 The PTSS may replace the means of transmission of submissions in accordance with paragraph 1 letter a with online-access to the Service's processing system.

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 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. 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[4] in conjunction with Article 23 of the Intelligence Service Ordinance of 16 August 2017[5].

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.

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.

4 SR **121**
5 SR **121.1**

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 Data Protection Commissioner or the PTSS Data Protection Commissioner.

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[6] on the Processing System for the Surveillance of Post and Telecommunications (PSO-PTSS).

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.

6 SR **780.12**

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 Services outside the normal working hours

1 Outside normal working hours and on public holidays, the PTSS shall provide the following on-call services:

a. the forwarding of requests for information specified in Articles 35–43;

b. issuing assignments for the activation of real-time surveillance in accordance with Articles 54–59;

c. issuing assignments for the conduct of retrospective urgent surveillance activities in accordance with Articles 60–63, 65 and 66;

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

e. the rectification of faults.

2 The TSPs, with the exception of those with reduced surveillance duties in accordance with Article 51, and providers of derived communication services with more extensive surveillance duties in accordance with Article 52 must be able to support the PTSS so that it may provide the services in accordance with paragraph 1 at any time. The PTSS must be able to contact them at any time.

3 The ordering of special surveillance activities and requests for special information (Art. 25) shall not be accepted or processed outside normal working hours.

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.

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. the type of information, surveillance, missing person search or wanted person search;

d. the duration of surveillance, if applicable;

e. the fees;

f. the compensation.

Art. 13 **S**tatistics 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. 269bis para. 2 and 269ter para. 4 CrimPC and Art. 70bis para. 2 and 70ter 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.

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 services 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[7].

[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.

Art. 18 Obligations for the supply of information

[1] TSPs and providers of derived communication services with more extensive duties to provide information in accordance with Article 22 must be able to provide the information specified in Articles 35–37 and 40–48 as well as in Article 27 in conjunction with Articles 35, 40, 42 and 43 that relates to services that they provide. They may enlist the support of third parties to do so.

[2] They shall provide the information specified in Articles 35–37 and 40–42 and in Article 27 in conjunction with Articles 35, 40 and 42 in an automated process via the query interface of the PTSS processing system. They may also provide the information specified in Articles 43–48 and in Article 27 in conjunction with Article 43 manually.

[3] TSPs with reduced surveillance duties in accordance with Article 51 may also provide information of all types outside of the processing system in writing.

[4] TSPs, with the exception of those with reduced surveillance duties in accordance with Article 51, and the providers of derived communication services with more extensive surveillance duties in accordance with Article 52 must be able to provide the information specified in Articles 38 and 39 that relates to services that they provide via the query interface of the PTSS processing system. They may enlist the support of third parties to do so.

[5] Providers of derived communication services without more extensive duties to provide information and conduct surveillance and operators of internal telecommu-

7 SR **780.12**

nications networks are not required to provide information of the types specified in Articles 35–48 and in Article 27 in conjunction with Articles 35, 40, 42 and 43. They shall supply the information available to them via the processing system or by a different method in written form.

6 If the number the data records found exceeds the maximum value specified in the request, the provider shall only disclose their number.

Art. 19 Identification of the participants

1 TSPs, providers of derived communication services with more extensive duties to provide information in accordance with Article 22, providers of derived communication services 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, TSPs must ensure that all end users are identified by suitable means.

Art. 20 Recording personal details in the case of mobile services

1 In the case of mobile services, TSPs and retailers in accordance with Article 2 letter f SPTA must, on supplying the means of access or on the initial activation of the service, verify the identity of the subscriber by means of a passport, an identity card or a foreign national identity card in accordance with Article 71 and 71*a* of the Ordinance of 24 October 2007[8] on Admission, Period of Stay and Employment. They must retain an easily legible copy of the identity document.

2 In the case of the natural persons, the following details must be recorded:

a. surnames and forenames;

b. date of birth;

c. type of identity document, identity document number and the issuing country or issuing organisation;

d. address;

e. if known, occupation;

f. nationality.

3 In the case of legal entities, the following details must be recorded:

a. name, registered office and contact details for the legal entity;

b. business identification number (UID) in accordance with the Federal Act of 18 June 2010[9] on the Business Identification Number;

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

8 SR **142.201**
9 SR **431.03**

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

a. the time at which the means of access was supplied;

b. the point of supply (name and complete address);

c. the name of the person supplying the means of access.

Art. 21 Retention periods

1 TSPs and providers of derived communication services with more extensive duties to provide information and conduct surveillance (Art. 22 and 52) must retain and be able to supply the information about the telecommunications services and the information recorded for the purpose of identification for the duration of the customer relationship and for 6 months after its termination. TSPs must retain and be able to supply identification data in accordance with Article 19 paragraph 2 for as long as the right to access the public WLAN access point applies and for 6 months after its expiry.

2 TSPs, with the exception of those with reduced surveillance duties in accordance with Article 51, and providers of derived communication services with more extensive surveillance duties in accordance with Article 52 must retain and be able to supply the following data for the purpose of identification for 6 months:

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

b. the secondary telecommunications data relating to the assignment and translation of IP addresses and port numbers, in order to be able to provide the information specified in Articles 37, 38 and 39.

3 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 Providers of derived communication services with more extensive duties to provide information

1 The PTSS shall declare a provider of derived communication services 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[10], the provider and the

10 SR **220**

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 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 providers of derived communication services 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 Types of information in general

1 The providers concerned shall provide the following types of information on telecommunications services or derived communications services:

a. information on subscribers (Art. 35, 40, 42 and 43 together with Art. 27 in conjunction with Art. 35, 40, 42 and 43);

b. information on services (Art. 36–39 and 41);

c. other information:

1. information on the method of payment (Art. 44),
2. requests for copies of identity documents (Art. 45),
3. requests for copies of invoices (Art. 46),
4. requests for copies of contracts (Art. 47),
5. information on technical data relating to telecommunications systems and network elements (Art. 48).

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

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 Types of surveillance

1 The providers concerned must conduct the following types of real-time surveillance for telecommunications services and derived communications services:

a. real-time surveillance of secondary telecommunications data in the case of network access services (Art. 54);

b. real-time surveillance of content and secondary telecommunications data in the case of network access services (Art. 55);

c. real-time surveillance of secondary telecommunications data in the case of applications (Art. 56 and 58);

d. real-time surveillance of content and secondary telecommunications data in the case of applications (Art. 57 and 59).

2 The providers concerned must conduct the following types of retroactive surveillance activities for telecommunications services and derived communications services:

a. retroactive surveillance in the case of network access services (Art. 60);

b. retroactive surveillance in the case of applications (Art. 61 and 62);

c. locating the last active position of the mobile terminal device (Art. 63);

d. an antenna search (Art. 66) and the corresponding preparations (Art. 64 or 65).

3 The providers concerned must conduct the following types of missing person searches (Art. 67):

a. locating the last active position of the mobile terminal device (Art. 67 let. a);

b. real-time surveillance of content and secondary telecommunications data in the case of network access services and telephony and multimedia services (Art. 67 let. b);

c. real-time surveillance of secondary telecommunications data in the case of network access services and telephony and multimedia services (Art. 67 let. c);

d. retroactive surveillance in the case of network access services and telephony and multimedia services (Art. 67 let. d).

4 The providers concerned must conduct the following types of searches (Art. 68):

a. locating the last active position of the mobile terminal device (Art. 68 let. a);

b. real-time surveillance of content and secondary telecommunications data in the case of network access services or applications (Art. 68 let. b);

c. real-time surveillance of secondary telecommunications data in the case of network access services or applications (Art. 68 let. c);

d. retroactive surveillance in the case of network access services or applications (Art. 68 let. d).

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 surveillance

[1] The PTSS may conduct test surveillance; 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 purposes;

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 targets and the required telecommunications services or derived communications services at its request free of charge and permanently.

[4] The prosecution authorities and the FIS may also conduct circuit trials 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 providers of derived communication services 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.

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 information about subscribers to network access services:

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

b. in the case of mobile services, the details of the natural person or legal entity in accordance with Article 20 and, if known, further contact details and the sex of the natural person;

c. in the case of the other network access services, the identification information specified in Article 19 and, if known, the details of the natural or legal entity, further contact details and the sex of the natural person;

d. the following information about each network access service that the subscriber obtains from the provider:
   1. the unique identifier for the provider (e.g. TSP number),
   2. the unique service identifier (e.g. user name, MSISDN, DSL identifier),
   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. if applicable, the SIM number (ICCID) at the time of its supply,
   10. if applicable, the IMSI,
   11. the type of the service (e.g. prepaid, subscription),
   12. if applicable, the alternative subscriber identifier for the network access 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. If letters a–e are used, a second query criterion must be added. If searching for character strings (lets a, c, d

and f), the provider must search only for the specified spelling of the term in accordance with the applicable FDJP regulations:

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. business identification number (UID);
h. subscriber identifier (e.g. customer number);
i. service identifier other than IP addresses (e.g. user name, MSISDN, DSL identifier);
j. IMSI;
k. SIM number (ICCID).

Art. 36 Information Request Type IR_6_NA: Information on network access services

[1] Information Request Type IR_6_NA comprises the following information about network access services. For information specified in letters b, c and e, details of the common period of validity shall be provided:

a. if available, the unique subscriber identifier (e.g. customer number);
b. the unique service identifier (e.g. user name, DSL identifier);
c. if applicable, the IMSI and MSISDN;
d. the list of unique device identifiers in accordance with international standards (e.g. IMEI, MAC address) of the devices used in connection with this service from the provider as well as, if available, their name in text form;
e. if applicable, the SIM numbers (ICCID);
f. if applicable, the PUK and PUK2 codes.

[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, DSL identifier);
b. the IMSI;
c. the unique device identifier in accordance with international standards (e.g. IMEI, MAC address);
d. the installation address of the fixed location access to the network.

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 information about the identified subscriber if this person was assigned a unique IP address at the time in question:

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

b. the unique service identifier (e.g. user name, MSISDN, DSL identifier) of the network access service;

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

[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 information about the identified subscriber if this person was not assigned a unique IP address (NAT) at the time in question:

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

b. the unique service identifier (e.g. user name, MSISDN, DSL identifier) of the network access service.

[2] The request for information shall contain information about the NAT translation procedure for the purpose of identification:

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. the date and time.

Art. 39[11] Information Request Type IR_9_NAT: Information on NAT translation procedures

[1] Information Request Type IR_9_NAT comprises the following information for the purpose of identification in connection with NAT translation procedures if required for identification:

11 The correction of 9 April 2019 relates to the French text only (AS **2019** 1201).

a. the source IP address before or after the NAT translation procedure, as the case may be;

b. the source port number before or after the NAT translation procedure, as the case may be.

2 The request for information shall contain the following information about the NAT translation procedure:

a. the source IP address after or before the NAT translation procedure, as the case may be;

b. the source port number after or before the NAT translation procedure, as the case may be;

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

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

e. the type of the transport protocol;

f. the date and time of the NAT translation procedure.

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 information about subscribers to telephony and multimedia services:

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

b.[12] in the case of mobile services, details of the natural person or legal entity in accordance with Article 20 and, if known, further contact details and the sex of the natural person;

c. in the case of the other telephony and multimedia services, the identification information specified in Article 19 and, if known, details of the natural person or legal entity, further contact details and the sex of the natural person;

d. the following information about each telephony and multimedia service obtained by the subscriber from the provider:

1. the unique identifier designating the provider (e.g. TSP number),
2. the unique 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,

12 The correction of 3 Dec. 2019 relates to the French text only (AS **2019** 4085).

6. the statuses of the service as designated internally by the provider (e.g. active, suspended, blocked),
7. if applicable, the list or range of other addressing elements or identifiers registered in connection with this service (e.g. telephone numbers, IMPU),
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. if applicable, the IMSI,
11. if applicable, the SIM number (ICCID) at the time of supply.

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. If using letters a–d, a second query criterion must be added. If searching for character strings (let. a, c, d and f), the provider must search only for the specified spelling of the term in accordance with the applicable FDJP regulations:

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. business identification number (UID);
h. subscriber identifier (e.g. customer number);
i. addressing elements or identifiers (e.g. telephone number, SIP URI, TEL URI, IMPU);
j. IMSI;
k. SIM number (ICCID).

Art. 41 Information Request Type IR_12_TEL: Information on telephony and multimedia services

1 Information Request Type IR_12_TEL comprises the following information about telephony and multimedia services. . For information specified in letters b, c and e, details of the common period of validity shall be provided:

a. if available, the unique subscriber identifier (e.g. customer number);
b. the addressing elements or identifiers registered for this service (e.g. telephone numbers, SIP URI, IMPI);
c. if applicable, the IMSI;

d. for the purpose of identification, the list of unique device identifiers in accordance with international standards (e.g. IMEI, MAC address) of the devices user in connection with this service from the provider as well as, if available, their designation in text form;

e. if applicable, the SIM numbers (ICCID);

f. if applicable, the PUK and PUK2 codes.

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 addressing element (e.g. telephone number, SIP URI, MSISDN, TEL URI);

b. the IMSI;

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

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

e. the service identifier (e.g. IMPI).

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 information about subscribers to email services:

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

b. the identification information specified in Article 19 and, if known, the details of the natural person or legal entity, additional contact details and the sex of the natural person;

c. the following information about each email service that the subscriber obtains from the provider:

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 elements (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);

d. if applicable, the additional addressing elements recorded by the provider in connection with this service (e.g. email address, MSISDN).

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. If using letters a–d, a second query criterion must be added. If searching for character strings (let. a, c, d and

f), the provider must search only for the specified spelling of the term in accordance with the applicable FDJP regulations:

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. business identification number (UID);

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

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

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 information about subscribers to other telecommunications or derived communications services (e.g. messaging services, communications services in social networks, cloud and proxy services):

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

b. the identification information specified in Article 19 and, if known, details of the natural person or legal entity, additional contact details and the sex of the natural person;

c. the following information about each additional telecommunications service or derived communications service that the subscriber obtains from the provider:

   1. the unique identifier that designates 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 elements or identifiers registered in connection with this 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. If using letters a–d, a second query criterion must be added. If searching for character strings (let. a, c, d and f), the provider must search only for the specified spelling of the term in accordance with the applicable FDJP regulations:

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. business identification number (UID);

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

i. addressing element or identifier (e.g. user name).

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 information about the method of payment used by subscribers to telecommunications and derived communications services:

a. the unique identifier that designates the provider;

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

c. 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. 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 information specified in with 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:[13]

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

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

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

13 The correction of 6 March 2018 relates to the French text only (AS **2018** 989).

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

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

Art. 45 Information Request Type IR_18_ID: Copy of official ID

[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.

[2] The request for information shall specify the period and subscriber or service identifier, SIM number (ICCID) or IMSI 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.

[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 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, the SIM number (ICCID) or IMSI or, if applicable, the device identifier to which it relates.

Art. 48 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, in particular the location data for mobile radio cells and public WLAN access points.

[2] The location data comprise:

a. the identifiers of network elements (e.g. CGI, ECGI, SAI, RAI, TAI, BSSID) and the geographical coordinates or other details of the location in accordance with international standards;

b. if applicable, the postal address of the location;

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

d. if applicable, other available location features.

[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 location of the network element;

b. the identifier of the network element (e.g. CGI, ECGI, BSSID).

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 information:

a. the contact details of the ordering authority;

b. the contact details 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 details.

Art. 50 Surveillance duties

[1] Each TSP and each provider of derived communication services with more extensive surveillance duties in accordance with Article 52 must be able to conduct the surveillance activities in accordance with 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. The foregoing does not apply to TSPs with reduced surveillance duties in accordance with Article 51.

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 identifier under surveillance (target ID).

5 It shall support the PTSS, if necessary, in order to ensure that the transmitted surveillance data actually corresponds to the telecommunications traffic specified in the surveillance assignment.

6 If additional identifiers are associated with the identifier under surveillance (target ID) (e.g. IMPI with IMPU, email address with alias address), the provider shall ensure that these identifiers are also monitored as part of the type of surveillance.

Art. 51 TSP 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:

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 Providers of derived communication services with more extensive surveillance duties

[1] The PTSS shall in a ruling declare a provider of derived communication services 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 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 shall allow the PTSS access to buildings, devices, lines, systems, networks and services to the extent required for surveillance.

[2] They shall make existing means of network access to public telecommunications networks available free of charge. In consultation 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 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 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 identifier and the IMSI in the case of mobile communications;

d. the IP addresses or address ranges assigned to the network access service under surveillance and the date and time of each assignment;

e. the available addressing elements of the network access service under surveillance, in the case of mobile communications, for example, the MSISDN or the IMSI;

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

g. the type, date and time of the start and if applicable the end of technical modifications of access to the network (e.g. location update, change in mobile communications technology) and, if known, its causes;

h. the target's available current location data or the cell used by the target or of the WLAN access point used by the target in accordance with paragraph 3.

3 The location data comprise:

a. the identifiers or a combination of identifiers (e.g. CGI, ECGI, SAI, RAI, TAI, BSSID) and the geographical coordinates, and, if applicable, the main direction of emission of the cell or of the WLAN access point, and, if available, the type of mobile communications technology used;

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, and, if available, the type of mobile communications technology used; or

c. if available, other details in accordance with international standards of the location of the target or of the cell or of the WLAN access point, and, if available, the type of mobile communications technology used.

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 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 surveillance 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 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), the IMSI in the case of mobile communications 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 or change to converging services, changes in mobile communications technology, location updates), if applicable:

   1. their type, the date and the time of their start and if applicable their end,
   2. the addressing elements (e.g. MSISDN, 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, 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,
   9. and in the case of mobile location services, the available current location data for the target or the cell used by the target or for the WLAN access point used by the target in accordance with paragraph 2.

2 The location data comprise:

a. the identifiers or a combination of identifiers (e.g. CGI, ECGI, SAI, RAI, TAI, BSSID) and the geographical coordinates of the cell or the WLAN access point and, if available, the type of mobile communications technology used;

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 as well as the type of mobile communications technology used; or

c. if available, other details in accordance with international standards relevant to the location of the target or the cell or of the WLAN access point, and the type of mobile communications technology used.

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.

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 Surveillance Type HD_28_NA: Retroactive surveillance of secondary telecommunications data in the case of network access services

Surveillance Type HD_28_NA includes the retroactive surveillance of secondary telecommunications data of a network access service. The following secondary telecommunications data of the past 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;
c. the identifier that was used for authenticating the user at the access point under surveillance, for example the user name;
d. the IP addresses or address ranges assigned to the target and their type;
e. if available, the unique device identifier of the terminal device used by the target in accordance with international standards (e.g. MAC address, IMEI in the case of mobile communications);
f. if available, the volumes of data that were uploaded and downloaded during the session;
g. in the case of access to the network via mobile communications: the GPRS or EPS information (in particular IMSI or MSISDN) and the following location data at the beginning and the end of the session as well as during the session if available; if known, additional location information from maritime navigation or aviation must be transmitted:
    1. the cell and region identifiers as well as the geographical coordinates, the postal addresses and if applicable the main directions of emission the cells used by the target, 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;

h. in the case of access to the network via a public WLAN: the BSSID, and, if available, the SSID and the location data in the form of geographical coordinates and the postal address of the WLAN access point used by the target; the user name, the type of authentication, the available additional information on user authentication (telephone number, MAC address, IMSI, user identifier and password used for authentication) and the IP address of the WLAN access point. If available, additional location information from maritime navigation or aviation must be transmitted;

i. in the case of fixed network access: the addressing elements of the access to the network 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, MMS and voice mail. The following secondary telecommunications data of the past telecommunications traffic in communications and communication attempts using the services under surveillance must be transmitted:

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

b. the addressing elements (e.g. MSISDN, E.164-number, SIP URI, IMPU) of all subscribers in communication and their roles;

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

d. in the case of mobile communications (multimedia services if available): the IMEI of the terminal device used by the target and the IMSI of the target;

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. in the case of mobile communications: the location data for the cell used by the target at the beginning and at the end of the communication or of the communication attempt. If known, additional location information from maritime navigation or aviation must be transmitted:

1. the cell and region 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;

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); and

i. in the case of multimedia services: information on the target's network access:
1. the access type,
2. the access class,
3. 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 the case of access to the network via mobile communications: the location data for the cell used by the target in accordance with letter g, or
– in the case of access to the network via WLAN: the available location data of the WLAN access point used by the target (geographical coordinates, postal address), or
– in the case of fixed network access: the available postal address of the access used by the target.

Art. 62 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 of the server and the client, and, if applicable, the delivery sta-

tus 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 Surveillance Type HD_31_PAGING: Identifying most recent activity on the mobile terminal device of the person under surveillance

Surveillance Type HD_31_PAGING comprises the identification of the most recent activity detected by the mobile telephony provider (network access services, telephony and multimedia services) on the mobile terminal device of the person under surveillance and providing the MSISDN, IMSI, IMEI (if available), the type of mobile communications technology, the frequency band, the unique identifier of the mobile network, the date and time of most recent activity detected, as well as one of the following details required to determine the location:

a. information about the cell used: the identifier or a combination of identifiers (e.g. CGI, ECGI, SAI, RAI, TAI), the postal address, the main direction of emission or, in the case of complex cells, the main directions of emission and the type of cell, the geographical coordinates;

b. the postal address and details of the position of the terminal device during its most recent activity as determined by the network, for example in the form of geographical coordinates and the related uncertainty value or in the form of a polygon together with details of the geographical coordinates of each polygon point; or

c. the postal address and other standardised details determined by the network of the position of the terminal device during its most recent activity or of the location of the cell used.

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 The TSPs shall supply the PTSS with a list of cell identifiers (e.g. CGI, ECGI) or the BSSID for the mobile radio cells or public WLAN access points identified.

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 location concerned and shall send the PTSS a list with the following related details:

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 element 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 base 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 identifiers (e.g. CGI, ECGI) or BSSID completed in accordance with paragraph 2.

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.[14]

[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

Art. 67 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 most recent activity detected by the mobile telephony provider (network access services and telephony and mul-

[14] The correction of 3 July 2018 relates to the Italian text only (AS **2018** 2551).

timedia services) of the mobile terminal device belonging to the missing person or a third party and provision of the MSISDN, the IMSI, the IMEI (if available), the type of mobile communications technology, the frequency band, the unique identifier of the mobile network, the date and the time of the most recent activity detected as well as any one of the following details required to determine the location:

1. information about the cell used: the identifier or a combination of identifiers (e.g. CGI, ECGI, SAI, RAI, TAI), the postal address, the main direction of emission or, in the case of complex cells, the main directions of emission and the type of cell, the geographical coordinates,
2. the postal address and the details of the position of the terminal device determined by the network during its most recent activity, for example in the form of geographical coordinates and the related uncertainty value or in the form of a polygon together with details of the geographical coordinates of each polygon point, or
3. the postal address and other standardised details determined by the network of the position of the terminal device during its most recent activity or of the location of the cell used;

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

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

d. Type EP_38_HD (retroactive surveillance of secondary telecommunications data): the combination of types of surveillance in accordance with Article 60 (network access services) and in accordance with Article 61 (telephony and multimedia services).

Art. 68 Wanted person search

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. one 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;

b. one 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;

c. one of the types of retroactive surveillance in accordance with Articles 60–63;

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

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 identifier under surveillance (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 the conduct of 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[15] on the Surveillance of Post and Telecommunications is repealed.

Art. 73 Amendment of other enactments

The ordinances below are amended as follows:

1. and **2.** …[16]

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] Circuit trials 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 providers of derived communication services 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' details 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 providers of derived communication services 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 58, 59 and 62. Before then, they must supply the data on email services in the same way as before.

15 [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]

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

7 Until the new processing system procured under the telecommunications surveillance[17] 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 providers of derived communication services 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 providers of derived communication services 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. 75 Commencement

This Ordinance comes into force on 1 March 2018.

17 BBl **2015** 3033

Annex
(Art. 2)

Terms and abbreviations

1. *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;
2. *Subscribers:* persons who have entered into a contract with a provider of telecommunications or derived communications services on using its services or who have registered for its services or received a means of access to its services;
3. *Multimedia services:* communications services which in addition to speech integrate other types of media and functions, such as video, file transfer, images, audio, parts of content, presence information (examples: video telephony, unified communication, RCS, multimedia telephony device);
4. *Identifier:* addressing element, identification number or other unique indicator of a specific subscriber, a specific service or a specific device;
5. *MSISDN (Mobile Subscriber Integrated Services Digital Network Number):* unique telephone number on which subscribers to a mobile network can be called;
6. *DSL identifier (Digital Subscriber Line Identifier):* identifier of a *digital subscriber line,* i.e. of a broadband access to the network by means of which data can be sent and received via copper wires;
7. *IP prefix:* part of the IPv6 address that identifies network concerned;
8. *IP address range:* a number of successive IP addresses;
9. *Net mask:* in internet protocol Version 4 (IPv4), describes how many bits at the start of the IP address displayed identify the network concerned;
10. *Prefix length:* in internet protocol Version 6 (IPv6), describes how many bits at the start of the IP address displayed identify the network concerned;
11. *SIM (Subscriber Identity Module):* smart card or chip permanently built into to the terminal device on which the IMSI 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)*;
12. *ICCID (Integrated Circuit Card Identifier):* series-number of a built-in chip (e.g. eSIM) or of a smart card (e.g. SIM card) that uniquely identifies the chip;
13. *IMSI (International Mobile Subscriber Identity):* number that allows the unique international identification of mobile communication subscribers;
14. *IMEI (International Mobile Equipment Identity):* number that allows the unique international identification of mobile communication terminals;

15. *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;
16. *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;
17. *PUK2-Code (Personal Unblocking Key 2):* same as the PUK code, but assigned to the PIN2 code;
18. *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);
19. *Source IP address:* IP address that is assigned to the communication end point (normally the client) that establishes the connection;
20. *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;
21. *Source port number:* port number that is assigned to the communication end point (normally the client) that establishes the connection;
22. *Destination IP address:* IP address that is assigned to the communication end point (normally the server) with which the connection is established;
23. *Destination port number:* port number that is assigned to the communication end point (normally the server) with which the connection is established;
24. *SIP (Session Initiation Protocol):* communication protocol that is used for signalling and maintaining multimedia communication sessions;
25. *SIP URI (SIP Uniform Resource Identifier):* URI scheme for addressing the SIP. The SIP URI are addressing elements in the format *user@domain.tld*;
26. *IMPU (IP Multimedia Public Identity):* in addition to the IMPI, a subscriber to the IMS has one or more IMPUs that are used to communicate with other subscribers. One IMPI may be assigned several IMPUs. Conversely an IMPU may also be shared with other subscribers;
27. *TEL URI (Telephone Uniform Resource Identifier):* URI scheme for telephone numbers. The TEL URI are addressing elements in the format *tel:number*, e.g. *tel:+41-868-868-868*;
28. *IMPI (IP Multimedia Private Identity):* globally unique identifier, assigned by providers to their subscribers, which is used inter alia for registration and AAA events. Every subscriber to IP Multimedia Subsystems (IMS) has an IMPI. The IMS is telecommunications system based on the internet protocol that integrates mobile voice services and internet functions;
29. *Alias address:* additional email address that the subscriber can set up, change and delete at will. The email provider determines the 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;

30. *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;
31. *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);
32. *Cloud-services:* derived communications services such as storage services and applications that are available online and hosted in data centres around the world depending on the need for resources;
33. *Proxy services:* communication interface in a network. It works as an intermediary that accepts requests on one side in order to establish a connection via its own address with the other side. Proxy services are therefore relevant for the purposes of identification;
34. *Public WLAN access point:* public wireless access point to a public telecommunications network that can be found both in public and in private spaces;
35. *CGI (Cell Global Identity):* unmodified cell identifier in second and third generation mobile networks (2G and 3G) (see 3GPP TS 23.003, Clause 4.3.1);
36. *ECGI (E-UTRAN Cell Global Identity):* unmodified cell identifier in fourth generation mobile networks (4G) (see 3GPP TS 23.003, Clause 19.6);
37. *SAI (Service Area Identity):* unmodified identifier for a service area that is used in mobile networks for mobility management (see 3GPP TS 23.003, Clause 12.5);
38. *RAI (Routing Area Identity):* unmodified identifier for a routing that is used in mobile networks for mobility Management related to packet-switched data transmission (see 3GPP TS 23.003, Clause 4.2);
39. *TAI (Tracking Area Identity):* unmodified identifier for a tracking area that is used for mobility management in fourth generation mobile networks (see 3GPP TS 23.003, Clause 19.4.2.3);
40. *BSSID (Basic Service Set Identifier):* unique identifier (MAC address) of the WLAN access point;
41. *Target ID:* identifier under surveillance, i.e. the identifier of the target of the surveillance;

42. *AAA (authentication, authorisation and accounting) information:* information on which subscribers are allowed to use which services and 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;
43. *SMS (Short Message Service):* messaging service for transmitting short text messages;
44. *Voice mail:* storage devices used in telecommunication networks that offer answering services (e.g. receiving, forwarding and storing voice messages). There are also 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 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; the RCS services are provided to subscribers by their mobile telephony provider;
46. *E.164 number:* telephone number in accordance with international numbering plan E.164 of the ITU-T;
47. *DTMF (Dual-Tone Multi-Frequency):* a signalling procedure, i.e. during a telephone conversation, signals can be sent by pressing the telephone keypad, for example to interact with answering machines or automatic voice response systems;
48. *MMS (Multimedia Messaging Service):* messaging service for transmitting messages in different types of media (multimedia) in mobile networks.