On the basis of the seventh paragraph of Article 228 of the Electronic Communications Act (Official Gazette of the Republic of Slovenia, No 130/22 and 18/23-ZDU-1O) the Minister of Digital Transformation in agreement with the Minister of the Interior, the Minister of Defence and the Director of Slovene Intelligence and Security Agency hereby issues the following

# Rules on equipment and interfaces for legal interception of communications

## Article 1
## (Content)

(1) These Rules determine suitable interfaces and functionality of equipment for legal interception of communications, which the operator provides for the needs of legal control of electronic communications in the Republic of Slovenia.

(2) These Rules have been adopted taking into account the information procedure in the field of standards and technical regulations in accordance with Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17. 9. 2015, p. 1).

## Article 2
## (Meaning of terms)

(1) The terms used in these Rules have the following meanings:

1. A handover interface means an interface on the side of the operator, which allows the transmission of interception results to the competent authority.
2. A public communications network means an electronic communications network used entirely or mainly to provide public communications services that enable the transmission of information between network connection points.
3. A controlled connection point means a connection point subject to legal control of electronic communications.
4. A transcription of an order is a document issued in accordance with Article 228 of the Electronic Communications Act (Official Gazette of the Republic of Slovenia, No 130/22 and 18/23-ZDU-1O hereinafter referred to as: the Act).
5. A communication intercepted in the context of legal interception of communications is a communication which:
    - originates from or ends in a controlled connection point,
    - is routed to a controlled connection point and is temporarily stored in a storage device,
    - is routed from the controlled connection point to storage devices or is requested from there from the controlled connection point, or
    - is routed from the controlled connection point to another connection point in the public communication network or other terminal equipment or passes through the public communication networks of other operators.
6. The competent authority is the authority that implements the measure of legal control of electronic communications in accordance with the law governing criminal proceedings or the law governing the Slovene Intelligence and Security Agency.

7. Data on intercepted communication is signalling and other information that is necessary for the establishment and implementation of a specific public communication service related to intercepted communication.
8. A connection point is a network connection point or another point in a public communications network.
9. The content of the intercepted communication is the information exchanged between two or more users of public communication services, excluding the data on the intercepted communication.
10. Legal control of electronic communications is a measure of control of electronic communications, which includes the legal interception and control and securing of evidence of all forms of communication in the public communication network, carried out by competent authorities in accordance with the law governing criminal proceedings or the law governing Slovene Intelligence and Security Agency.
11. Legal interception of communications is a procedure ordered on the basis of the law governing criminal proceedings or the law governing the Slovene Intelligence and Security Agency, in which content, circumstances and facts related to communications at a specific point in the public communications network are collected.

(2) The rest of the terms used in these Rules have the same meaning as defined in the Act.

**Article 3**
**(Basic Requirements)**

(1) The operator shall install such interfaces and equipment in its electronic communication network that, after receiving the transcript of the order, it can enable the legal interception of communications at a specific controlled connection point in the manner, to the extent and for the duration, as specified in the transcript of the order.

(2) The operator shall ensure in its electronic communications network such a number and arrangement of those nodes in the network where equipment for the legal interception of communications is installed so that access to the interception results is ensured at all times and in an equivalent manner from each controlled connection point that temporarily or permanently uses the operator's public communications network or service.

(3) Legal interception of communications is carried out in such a way that the persons involved in the intercepted communications and other unauthorized persons do not perceive that the legal interception of communications is being carried out. The use of devices and equipment for the implementation of legal interception of communications may not change the operating characteristics or quality of intercepted communications or other public communications services.

(4) The equipment and interfaces for the legal interception of communications shall enable the legal interception of communications at a specific controlled connection point end immediately after the expiration of the permitted duration of the legal control of electronic communications at this connection point, or when the operator receives a notification that the legal control of electronic communications of this connection point has been terminated.

(5) The operator provides such equipment and such an interface that all competent authorities can simultaneously carry out legal control of electronic communications.

**Article 4**
**(Equipment and interception results)**

(1) The operator shall use such equipment to provide the competent authority with the following information about the intercepted communication in addition to the content of the intercepted communication:

1. the number or other designation of the controlled connection point or the identifier of the user;
2. the number or other designation of the connection point:
   - with which the controlled connection point attempts to establish a connection, even if the establishment of the connection failed, or
   - which wants to establish a connection with a controlled connection point, even if the connection was not successfully established or if the intercepted communication from the controlled connection point was redirected elsewhere or if it was directed to a storage device (data storage device);
3. in the event of rerouting, also the numbers or other designations of all connection points to which intercepted communications were rerouted;
4. information on the type of public communications service used at the controlled connection point, or its characteristics;
5. technical reasons for the eventual termination of the connection between the controlled connection point and any other connection point or that no connection with the controlled connection point has been established;
6. the most detailed available information on the location of the controlled connection point, if it is a controlled connection point in mobile public communication networks;
7. the date and time of the attempt to intercept a communication if the connection was not established, and the date and time of the start and end of the intercepted communication if the connection was successful.

(2) The data referred to in the preceding paragraph shall also be provided by the operator:
- when the controlled connection point is included in a connection established between multiple connection points;
- when connections to multiple connection points have been established from the controlled termination point.

(3) If due to technical reasons the operator does not provide all interception results in its public communication network it shall immediately notify the competent authority.

(4) The correlation between the content of the intercepted communication and the associated intercepted communication data must be unique.

**Article 5**
**(Handover interface)**

(1) Regardless of the number of nodes referred to in the second paragraph of Article 3 of these Rules, the operator shall, as a rule, provide one handover interface.

(2) The operator shall be deemed to have complied with the provisions of the sixth paragraph of Article 228 of the Act if it provides the handover interface together with another operator or operators or if it connects its network to another operator's handover interface. In this case, the operator shall ensure that all the data necessary to generate the interception results is accessible to the handover interface.

(3) The handover interface must be implemented in such a way that:

- it provides the competent authority with the results of the interception throughout the duration of the legal control of electronic communications at a specific controlled connection point,
- the quality of communications on the handover interface is not lower than the quality of the corresponding intercepted communications,
- generally available and serviceable transmission routes and transmission protocols can be used for transmission and delivery of interception results,
- the standards SIST ES 201 671, SIST-TS ETSI/TS 102 232 in SIST-TS ETSI/TS 103 280 are taken into account for public communication networks or public communication services.

(4) If the operator encodes, compresses or encrypts communications in its public communication network, it shall ensure that the results of the interception on the handover interface are unencoded, uncompressed or unencrypted.

**Article 6**
**(Cessation of use)**

The Rules on Equipment and Interfaces for the Legal Interception of Communications (Official Gazette of the Republic of Slovenia, No 89/13 and 189/21 - ZDU-1M) shall cease to apply on the day these Rules enter into force.

**Article 7**
**(Entry into force)**

These Rules enter into force on the fifteenth day after their publication in the Official Gazette of the Republic of Slovenia.

No.

Ljubljana, date

EVA 2023-3150-0009

**Dr. Emilija Stojmenova Duh**
Minister of Digital Transformation

I consent!

**Boštjan Poklukar**
Minister of the Interior

**Marjan Šarec**
Minister of Defence

**Joško Kadivnik**
Director

Slovene Intelligence and Security Agency