

European best practices on government telecommunications surveillance

This report provides an overview of some of the legal powers that various European government agencies have in order to request the assistance of telecommunication companies with conducting real-time interception and the disclosure of data about their customers.

In the majority of cases, the telecommunication companies maintain complete control over data and provide assistance in surveillance activities only when the appropriate court order is presented to them. There are only a small number of examples in the EU where the government agency maintains complete control over surveillance activities, without informing the telecommunication companies.

France

PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

The French Criminal procedure code (“CPP”) provides that, for the investigation of felonies and misdemeanours, if the penalty incurred is at least two years’ imprisonment, the investigating judge (“juge d’instruction”) may authorise the implementation of the interception, recording and transcription of telecommunication correspondence where necessary to conduct the investigation. According to article 100 of the CPP, the judge’s decision must be in writing and issued for maximum period of 4 months (renewable once under the same conditions of form and duration).

Article 706-95 of the CPP provides that, as part of investigations relating to organised crime and delinquency, public prosecutors may request from the judge in charge of liberties and custody (the “juge des libertés et de la détention”) an authorisation to implement the interception, recording or transcription of correspondence by telecommunications in accordance with the provisions of Articles 100 ff. of the CPP as mentioned above. The interception may only be ordered for a maximum period of fifteen days, renewable once under the same conditions of form and duration. The judge’s decision must be in writing, setting out the justification and granted for a maximum period of one month (renewable once under the same conditions of form and duration).

The CPP provides that, further to the judge’s order, the judge or the police officer appointed by the judge or the public prosecutor may issue a judicial order requiring the telecommunications operator to provide assistance in implementing the interception system.

Under Article 100 of the CPP, interceptions are conducted under the authority and supervision of the investigating judge. The same article expressly provides that the decision does not bear the status of a judicial decision and is therefore not subject to appeal before any judge.

DISCLOSURE OF COMMUNICATIONS DATA

French Code of Post and Electronic Communications

The CPCE requires, under article L34-1-III, that electronic communication service providers retain connection data, mainly for the needs of the research, establishment and sanction of criminal offences for a period of up to one year.

Article L32-1-II of the CPCE specifies that electronic communications service providers are required to implement the relevant internal procedures to answer the requests received from public authorities regarding user data. The same applies to access providers.

Germany

PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

In Germany, there appears to be no specific laws that grant government and law enforcement agencies with the legal powers to mandate direct access into a telecommunication service provider's network without the operational control or oversight of the telecommunication service provider.

The German Telecommunication Act ("TKG") requires certain operators of telecommunication systems used to provide telecommunication services to the public to maintain technical and organizational capabilities to execute interception measures provided for by law (Sec. 110 TKG).

Sec. 110 TKG requires operators of telecommunication systems used to provide telecommunication services to the public (as further specified in Sec. 3 TKG) to maintain the technical facilities, and to make the organizational arrangements, to execute telecommunication interception measures expressly provided for by law. This includes the obligation to maintain interception capabilities to execute any interception order without delay (including, in particular, handing over a copy of the requested communication).

Code of Criminal Procedure ("StPO")

The measures pursuant to Sec. 100a Strafprozessordnung ("StPO") require a prior court order following an application by the public prosecutor's office (or, in relation to tax offences, the tax authority); yet, in pressing circumstances, the public prosecutor's office may also issue an order, which must be confirmed by the court within three working days in order not to become ineffective (Sec. 100b(1) StPO).

An order may only be granted in cases where certain facts give rise to the suspicion that a serious criminal offence referred to in Sec. 100a(2) StPO has been committed (or, in cases where there is criminal liability for an attempt, there was an attempt to commit such an offence, or such offence had been prepared by committing a criminal offence), and the offence is one of particular gravity in the individual case as well, and other means of establishing the facts or determining the accused person's whereabouts would be significantly more difficult (Sec. 100a(1) StPO).

All persons providing, or contributing to the provision of, telecommunications services on a commercial basis are required to assist the public prosecutor's office (and certain officials working in the police force or, in relation to tax offences, the tax authority) to implement the necessary measures required for the interception/recording of the communication and to provide all necessary information without delay (Sec. 100b(3) StPO). The measures to be taken are further specified by Sec. 110 TKG and the TKÜV/TR-TKÜV.

Article 10 Act (Artikel 10-Gesetz-G10)- National Security Order

An order under Sec. 3 G10 may be granted where actual facts give rise to the suspicion that a serious criminal offence directed against the free democratic basic order or the existence or safety of the Federal Republic of Germany or its federal states (as listed in Sec. 3(1) G10) will be, is being, or has been committed, or a person is part of a group having the purpose of committing such crimes, and the investigation of the facts by other means would be significantly more difficult.

An order under Sec. 5 (for bundled telecommunications) or Sec. 8 G10 may be granted where the intercepted information is necessary in order to prevent the danger of an armed attack or terrorist attacks on Germany, international drug trafficking, money laundering, or similar crimes with impact on German territory (as listed in Sec. 5(1) G10) or to prevent the danger to the life or physical integrity of a person abroad, if such danger directly affects German interests (Sec. 8 G10).

The telecommunication service provider must allow the Intelligence Service to install the relevant technical capabilities on its premises and must grant access to the relevant employees of the Federal Intelligence Service as well as the G10 Commission (Sec. 110(1) No. 5 TKG and Sec. 27 TKÜV). The measures to be taken are further specified by the TKÜV/TR-TKÜV.

However, these technical capabilities do not constitute "interception capabilities" in the direct sense of the term. Rather, the interception itself still has to be performed by the telecommunication provider which then (electronically) hands over a so-called "interception copy" (Überwachungskopie) of the communication to the equipment of the Federal Intelligence Service. The communication is filtered by this equipment with the help of pre-defined search terms and the irrelevant part of the interception copy has to be deleted before the relevant part is passed on to the Federal Intelligence Service.

DISCLOSURE OF COMMUNICATIONS DATA

The German Telecommunications Act ("TKG") requires any person providing, or contributing to the provision of, telecommunication services on a commercial basis to provide certain subscriber,

line identification and other data upon manual information requests from a range of law enforcement agencies, foreign and domestic intelligence services, and other public authorities, where such requests can be based on a legal statutory authorization (Sec. 113 TKG).

Subscriber Data, Line Identification and Other Data

Sec. 113 TKG requires any person providing, or contributing to the provision of, telecommunication services on a commercial basis to provide certain subscriber, line identification and other data (specified in Sec. 95 and 111 TKG) to certain public authorities listed in Sec. 113(3) TKG (law enforcement agencies, foreign and domestic intelligence services and other public authorities), as far as necessary for the prosecution of criminal or administrative offences, for averting danger to public safety or order, and/or for the discharge of the legal functions of such agencies.

The request must be made in text form (except in pressing circumstances) and be based on an express legal authorization. Respective authorizations (which may stipulate further requirements) are, for example, set out in Sec. 100j StPO, Sec. 7 and 15 ZFdG, Sec. 7, 20b and 22 BKAG, Sec. 22a BPolG, Sec. 8d BVerfSchG, Sec. 4b MADG and Sec. 2b BNDG.

Greece

PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

According to Article 19(1) of the Greek Constitution, the confidentiality of communications should not be released; however, there are conditions under which a judicial authority is not bound by such confidentiality where national security or particularly serious crimes are involved.

Law 2225/1994 was adopted on the basis of Article 19(1) of the Greek Constitution and sets out the procedure that judicial or other public authorities should follow when requesting the withdrawal of confidentiality. An application for the withdrawal of confidentiality (which would allow for the interception of individual customer communications) can only be made for reasons of national security (Article 3) or for the purposes of identifying certain criminal offences (Article 4). Withdrawal of confidentiality is also permitted in order to investigate the crimes listed in Article 253A of the Hellenic Criminal Procedure Code.

The Hellenic Authority for Communications Security and Privacy (“ADAE”) has issued guidelines on the measures that telecommunications service providers should have in place in order to ensure that confidentiality is protected during the real-time interception of communications (Decisions 52/2009 and 53/2009).

For the withdrawal of confidentiality, an order is issued by the competent judicial authority on the basis of Article 5 of Law 2225/1994. The order includes information on the public authority, public prosecutor or investigator requesting the withdrawal, the purpose of the withdrawal, the means of communication which form the object of the withdrawal and, in the case of criminal offences

being investigated, the name of the person against whom the withdrawal is directed as well as his or her residential address.

Article 5(4) of Law 2225/1994 provides that an excerpt of the order, containing its operative part, is delivered to the Chairman, Board of Directors, General Manager or representative of the company concerned. According to Article 6(1) of Presidential Decree 47/2005, when a competent authority seeks the execution of an order, a service provider is obliged to activate the equipment and software, under its control, which is required for the withdrawal of confidentiality within three hours from notification of the order, regardless of when the order was actually served and, in cases of urgency, which have to be specifically mentioned, as early as possible. Article 7(2) of Presidential Decree 47/2005 specifies that the execution of an order for the withdrawal of confidentiality is performed by the competent authority in cooperation with the service provider.

In the event of war, mobilisation due to external threats or an immediate threat to national security as well as an armed coup to overturn democracy, under Article 48 of the Greek Constitution, the Greek Parliament has the power, following the government's recommendation, to implement special measures. It is possible that such measures could include direct access to a service provider's network to enable interception, although this is not expressly mentioned.

DISCLOSURE OF COMMUNICATIONS DATA

Article 4 of Presidential Decree 47/2005 lists the specific communications data that a service provider may be required to disclose and this includes the content of customer communications and metadata, depending on the type of communication involved.

Article 5(4) of Law 2225/1994 provides that an excerpt of the order, containing its operative part, is delivered to the Chairman, Board of Directors, General Manager; or representative of the company concerned.

According to Article 7(2) of Presidential Decree 47/2005, the execution of an order for the withdrawal of confidentiality is performed by the competent authority in cooperation with the service provider.

OVERSIGHT OF THE USE OF POWERS

Following the execution of an order, one or more reports are prepared by the service provider that was involved in the withdrawal of confidentiality and these are submitted to the judicial authority that issued the order as well as to ADAE and the applicant authority (see Article 5(5) of Law 2225/1994).

Spain

Spanish law does not appear to grant government agencies the legal powers to mandate direct access into a communication service provider's networks without the operational or control or oversight of the communication service provider.

Service providers and operators of public electronic communication networks may be required to intercept communications in the following scenarios:

PROVISION OF REAL-TIME LAWFUL INTERCEPTION ASSISTANCE

Following the judicial police's initiative, a judge may issue an interception order following the legal requirements established in Article 579 of the Criminal Procedure Act, approved by Royal Decree of 14 September 1882 (the "Criminal Procedure Act"), in cases where evidence suggests that by making use of these means a relevant issue or circumstance of the case may be discovered or ascertained.

In addition, pursuant to the Organic Law 2/2002, dated May 6, 2002, on the Prior Judicial Control applicable to the National Intelligence Centre, the National Intelligence Centre ("CNI") may ask the operator to intercept communications in cases where the Secretary of State or Director of the CNI has obtained an authorization from the relevant judge of the Spanish Supreme Court, in accordance with the aforementioned requirements of such Organic law.

Articles 83 to 101 of the Regulation on the conditions for the provision of electronic communication services, the universal service and the protection of users, approved by Royal Decree 424/2005, of 15 April 2005 (the "Universal Service Regulation"), determines the procedure and the measures to be adopted by service providers and operators of public electronic communication networks for intercepting communications in cases where they are obliged to do so by law. The Universal Service Regulation establishes, among other things, the general requirements of the procedure, access requirements, the information to be delivered to the authorised agent (judicial police or CNI agent), and other operational requirements (previous information, locations, authorised personnel, confidentiality, real time access, interfaces, etc.).

In addition, Order ITC/110/2009, of 28 January 2009 on the general framework applicable to the specifications to be followed for the legal interception of communications ("General Framework Order"), establishes the relevant technical requirements and interfaces to be implemented by service providers and operators of public electronic communication networks in order to be communicated by the relevant agent about the need to carry out the interception of a communication.

Article 33 of the General Telecommunications Act 32/2003, of 3 November 2003, sets out the operator's duty to intercept communications when required to do so by the relevant authorities through the appropriate interfaces, duly ready for this purpose. Together with such Act, the

Universal Service Regulation and the General Framework Order, all provide for a detailed description of the obligations to which operators are subject in terms of measures, procedures, interfaces and technical requirements to be put in place in order to comply with their interception duties.

DISCLOSURE OF COMMUNICATIONS DATA

The Data Retention Act regulates: (1) the operator's obligation to retain traffic and localisation data, and other necessary data to identify the user ("traffic data") generated or processed in connection with the provision of electronic communication services or public communication networks; and (2) the duty to transfer such traffic data to the relevant agents whenever they are required to do so, through the relevant court order or judicial authorisation. In addition to the judicial police and CNI agents, the Data Retention Act explicitly includes the staff members of the Office of Customs Surveillance as authorised agents in this regard.

In accordance with Article 4 of the Data Retention Act, operators have the obligation to disclose the retained data to the authorised agents, following the instructions contained in a court order issued by the relevant judge, and pursuant to the provisions of the Criminal Procedure Act.

The Data Retention Act, among other things, regulates the particular traffic data to be retained, the particular obligation to store traffic data, the period of time such traffic data must be stored or retained by the operator, the procedure and security measures involved in the transfer of such traffic data to the relevant agents, and the sanctions to be imposed on operators which do not comply with such obligations.

The content of communications is explicitly excluded from the scope of the aforementioned Act.

European Telecommunications Standards Institute (ETSI)¹

Wherever legally permitted to do so, telecommunication companies, such as one of Europe's largest companies – Vodafone, follow the lawful interception technical standards set down by the **European Telecommunications Standards Institute (ETSI), which define the separation required between the agency or authority monitoring centre and the operator's network.** The ETSI standards are globally applicable across fixed line, mobile, broadcast and internet technologies, and include a formal handover interface to ensure that agencies and authorities do not have direct or uncontrolled access to the operators' networks as a whole. Government agencies and authorities should allow operators to conform to ETSI technical standards when mandating the implementation of lawful interception functionality within operators' networks.²

¹ <http://www.etsi.org/technologies-clusters/technologies/security/lawful-interception>

² http://www.vodafone.com/content/dam/sustainability/2014/pdf/operating-responsibly/vodafone_law_enforcement.pdf