BILAG 3

MINISTERUL JUSTIȚIEI

Bucharest 25 September 2015
Our ref. 75864/2015
Your ref. 2015-42343/861082

Royal Danish Embassy
Bucharest

The Ministry of Justice of Romania presents its regards to the Royal Danish Embassy and, referring to the note verbale from 16 September 2015, has the honour to transmit, attached, an excerpt from the Romanian code of criminal proceedings, concerning the legal provisions applicable when issuing a search warrant and authorizing phone tapping.

The Ministry of Justice of Romania avails itself of this occasion to renew to the Royal Danish Embassy the assurance of its highest consideration.

CHAPTER IV

Surveillance or investigation special methods

ART. 138

General provisions

(1) The following are surveillance or investigation special methods:

a) wiretapping of communications or of any type of remote communication;

b) accessing a computer system;

c) video, audio or photo surveillance;

d) tracking or tracing with the use of technical devices;

e) obtaining data regarding the financial transactions of individuals;

f) withholding, delivery or search of mail deliveries;

g) use of undercover investigators and informants;

h) authorized participation in specific activities;

i) controlled delivery;

j) obtaining data generated or processed by providers of public electronic communication networks or by providers of electronic communication services intended for the public, other than the content of communications, stored by these under the special law on storing data generated or processed by providers of public electronic communication networks and by providers of electronic communication services intended for the public.

(2) Wiretapping of communications or of any type of messages designates the wiretapping, accessing, monitoring, collection or recording of communications via phone, computer system or any other communication device.

(3) Accessing a computer system designates the penetration of a computer system or of other data storage device either directly or from a distance, through specialized programs or through a network, for the purpose of identifying evidence.

(4) A computer system is any device or combination of devices interconnected between them or in a functional relationship, one or more of which provide the automatic data processing by means of a computer program.

(5) Computer data is any representation of facts, information or concepts in a form appropriated for processing in a computer system, including a program able to determine the performance of a function by a computer system.

(6) Video, audio or photo surveillance is the taking of pictures of persons, the observation or recording of their conversations, gestures or other activities.

(7) Tracking or tracing with the use of technical devices is the use of devices that establish the location of the person or the object to which such devices are attached.

(8) Search of mail deliveries designates the inspection, through physical or technical methods, of letters or other mail deliveries or objects transmitted through any other means.

(9) Obtaining of data regarding the financial transactions of individuals designates operations that provide knowledge of the contents of financial transactions and other operations performed or to be performed through a credit institution or through other financial entity, as well as the obtaining from a credit institution or other financial entities of documents or information held by it referring to the transactions or operations of a person.

(10) Use of undercover investigators and informants designates the use of a person with an identity other than their real one, for the purpose of obtaining data and information regarding the commission of an offense.

(11) Authorized participation in specific activities means the commission of acts similar to the objective component of a corruption offense, the performance of transactions, operations or any other kind of arrangements related to an asset or to a person who is presumed missing, a victim of trafficking in human beings or of kidnapping, the performance of operations involving drugs, as well as the providing of services, based on an authorization from the judicial bodies of competent jurisdiction for the purpose of obtaining evidence.

(12) Controlled delivery designates a surveillance and investigation technique allowing for the entry, transit or exit from the territory of the country of goods in respect of which there is a suspicion related to the illicit nature of their possession or obtaining, under the surveillance of or based on an authorization from the competent authorities, for the purpose of investigating an offense or of identifying the persons involved in its commission.

(13) Electronic surveillance is the use of any of the methods listed under par. (1) items a) - c).

ART. 139

Electronic surveillance

(1) Electronic surveillance is ordered by the Judge for Rights and Liberties when the following requirements are cumulatively met:

a) there is a reasonable suspicion in relation to the preparation or commission of one of the offenses listed under par. (2);

b) such measure is proportional to the restriction of fundamental rights and freedoms, considering the particularities of the case, the importance of information or evidence that are to be obtained or the seriousness of the offense;

c) evidence could not be obtained in any other way or its obtaining implies special difficulties that would harm the investigation, or there is a threat for the safety of persons or of valuable goods.

(2) Electronic surveillance may be ordered in case of offenses against national security stipulated by the Criminal Code and by special laws, as well as in case of drug trafficking, weapons trafficking, trafficking in human beings, acts of terrorism, money laundering, counterfeiting of currency or securities, counterfeiting electronic payment instruments, offenses against property, blackmail, rape, deprivation of freedom, tax evasion, corruption offenses and offenses assimilated to corruption, offenses against the European Union's financial interests, offenses committed by means of computer systems or electronic communication devices, or in case of other offenses in respect of which the law sets forth a penalty of no less than 5 years of imprisonment.

(3) The recordings set forth by this chapter, done by the parties or by other persons, represent evidence when they concern their own conversations or communications with third parties. Any other recordings may constitute evidence unless prohibited by law.

(4) The relationship between a counsel and a person assisted or represented by them may be subject to electronic surveillance only when there is information that the counsel perpetrates or prepares the commission of any of the offenses listed under par.(2). If during or after the performance of such measure it results that the activities of electronic surveillance also targeted the relations between the counsel and the suspect or defendant defended by the former, the evidence obtained this way may not be used in a criminal proceeding, and shall be destroyed forthwith by the prosecutor. The judge having ordered such measure shall be informed forthwith by the prosecutor. When deemed necessary, the judge may order the information of the counsel.

ART. 140

Procedure for the issuance of an electronic surveillance warrant

(1) Electronic surveillance may be ordered during the criminal investigation, for a term of maximum 30 days, upon request by the prosecutor, the Judge for Rights and Liberties of the court having the competence of jurisdiction to examine the case in first instance or of the court corresponding to its level under whose territorial jurisdiction the premises of the prosecutors' office to which the prosecutor who filed the application belongs are located.

(2) Such application filed by the prosecutor has to contain: the electronic surveillance measures that are requested for authorization, the name or the identification data of the person against whom such measure is to be ordered, if known, the evidence or data giving rise to a reasonable suspicion related to the commission of an offense in respect of which such measure may be ordered, the facts and the charges, and, in case of a video, audio or photo surveillance measure, whether an approval for criminal investigation bodies to enter private spaces

indicated for activating and deactivating the technical devices to be used for the enforcement of the electronic surveillance measure is also requested, and a justification of the proportional and subsidiary nature of the measure. The prosecutor has to submit the case file to the Judge for Rights and Liberties.

(3) An application requesting approval of electronic surveillance shall be ruled on in chambers, on the same day, without summoning the parties. The prosecutor's attendance is mandatory.

(4) If they decide that the application is justified, the Judge for Rights and Liberties shall order admission of the prosecutor's application, through a court resolution, and shall issue forthwith a electronic surveillance warrant. Writing of a report is mandatory.

(5) The court resolution of the Judge for Rights and Liberties and the warrant have to contain:

a) name of the court;

b) warrant issuance date, time and venue;

c) surname, first name and capacity of the person returning the court resolution and issuing the warrant;

d) description of the concrete approved measure;

e) time period and purpose for which the measure was authorized;

f) name of the person subject to a electronic surveillance measure or their identification data, if known;

g) indication, if necessary given the nature of the approved measure, of the identification elements of each phone device, of the access point to a computer system, and of any known data for the identification of a communication channel or of an account number;

h) in case of a measure of video, audio or photo surveillance in private spaces, mention of approving permission to criminal investigation bodies to enter private spaces in order to activate and deactivate the technical devices to be used for the enforcement of the electronic surveillance measure;

i) signature of the judge and stamp of the court.

(6) In the event that the Judge for Rights and Liberties decides that the requirements set by Art. 139 and The stipulations of par. (1) of this Article are not met, they shall deny the application for approving a electronic surveillance measure, through a court resolution.

(7) A court resolution under which the Judge for Rights and Liberties rules on electronic surveillance measures is not subject to avenues of appeal.

(8) A new application for the approval of the same measure may be filed only if new facts or circumstances, which were not known at the moment when the Judge for Rights and Liberties ruled on the previous application, occurred or were discovered.

(9) Upon justified request by an victim, the prosecutor may request the judge to authorize the wiretapping or recording of communications, as well as of any types of communications performed by them through any communication device, irrespective of the nature of the offense subject to investigation. The stipulations of par. (1) - (8) shall apply accordingly.

ART. 141

Authorization of electronic surveillance measures by the prosecutor

(1) The prosecutor may authorize, for a time period of maximum 48 hours, electronic surveillance measures when:

a) there is an emergency situation, and the obtaining of a electronic surveillance warrant under the terms of Art. 140 would lead to a substantial delay of investigations, to the loss, alteration or destruction of evidence, or would jeopardize the safety of the victim, of witnesses or of their family members; and

b) the requirements set by Art. 139 par. (1) and (2) are met.

(2) A prosecutorial order authorizing electronic surveillance measures has to contain the mentions specified by Art. 140 par. (5).

(3) Within a maximum of 24 hours following expiry of a measure, the prosecutor is under an obligation to notify the Judge for Rights and Liberties of the court having the competence of jurisdiction to examine the case in first instance or of the court corresponding to its level under whose territorial jurisdiction the premises of the prosecutors' office to which the prosecutor who issued the order belongs are located, in order for them to confirm the measure and, at the same time, shall forward a report presenting a summary of the electronic surveillance activities performed and the case file.

(4) If the Judge for Rights and Liberties decides that the requirements set by par. (1) were met, they shall confirm the measure ordered by the prosecutor within 24 hours, through a court resolution, returned in chambers, without summoning the parties.

(5) In respect of computer data identified through accessing a computer system, the prosecutor may order, through a prosecutorial order:

a) making and preservation of a copy of such computer data;

b) prohibition of access to or removal of such computer data from the computer system.

Copies shall be made by means of appropriate technical devices and procedures, of nature to ensure the integrity of information contained by these.

(6) If the Judge for Rights and Liberties decides that the requirements set by par. (1) were not met, they shall nullify the measure taken by the prosecutor and shall order destruction of the evidence thus obtained. The prosecutor shall destroy the evidence obtained this way and shall prepare a report in this sense.

(7) Together with the application for a confirmation of their measure, or separately, the prosecutor may request the Judge for Rights and Liberties to warrant electronic surveillance measures under the terms of Art. 140.
(8) A court resolution through which the Judge for Rights and Liberties rules on the measures ordered by the prosecutor is not subject to avenues of appeal.

ART. 142
Enforcement of electronic surveillance warrants
(1) The prosecutor shall enforce an electronic surveillance measure or may order that this be enforced by criminal investigation bodies or by specialized employees of the law enforcement bodies or of other specialist bodies of the state.
(2) Providers of public electronic communication networks or providers of electronic communication services intended for the public or of communication or financial services are under an obligation to cooperate with the criminal investigation bodies, the authorities listed under par. (1), within the limits of their authority, for the enforcement of electronic surveillance warrants.
(3) Persons who are called to provide technical support for the enforcement of surveillance measures are under an obligation to keep secrecy in respect of the performed operation, under penalties set by the criminal law.
(4) The prosecutor is under an obligation to cease electronic surveillance forthwith before expiry of the warrant term if the reasons justifying such measure no longer exist, by immediately informing the judge having issued the warrant.
(5) Data resulted from electronic surveillance measures may be used also in other criminal case if they contain eloquent and useful data or information regarding the preparation or commission of another crime of those set forth by Art. 139 par. (2).
(6) Data resulted from surveillance measures that do not concern the act subject to investigation or that do not contribute to the identification or locating of persons, if such are not used in other criminal cases as per par. (5), shall be archived at the premises of the prosecutors' office, in special places, by ensuring their confidentiality. Ex officio or upon request by the parties, the vested judge or judicial panel may request the sealed data if there is new evidence from which it results that part of these concern an act subject to investigation. One year after the final settlement of a case, these are destroyed by the prosecutor, who shall prepare a report in this sense.

ART. 142^1
(1) Any authorized person conducting electronic surveillance activities, under this law, has the possibility to ensure the electronic signing of data resulting from

electronic surveillance activities, by using an extended electronic signature based on a qualified certificate issued by an accredited certification services provider.
(2) Any authorized person who transmits data resulting from electronic surveillance activities under this law, has the possibility to sign the transmitted data by using an extended electronic signature based on a qualified certificate issued by an accredited certification services provider, which allows for the unambiguous identification of the authorized person, the latter taking this way responsibility for the integrity of the transmitted data.
(3) Any authorized person who receives data resulting from electronic surveillance activities under this law, has the possibility to check the integrity of the received data and to certify such integrity by signing them by means of an extended electronic signature based on a qualified certificate issued by an accredited certification services provider, which allows for the unambiguous identification of the authorized person.
(4) Each person certifying data under electronic signature is liable for the security and integrity of such data under the law.

ART. 143
Recording of electronic surveillance activities
(1) Prosecutors or criminal investigation bodies shall prepare a report for each electronic surveillance activity, in which they shall record the results of activities conducted in respect of an act subject to investigation or that contribute to the identification or localization of persons, the identification data of the medium containing the results of electronic surveillance activities, the names of persons to whom these refer, if known, or other identification data, as well as, as applicable, the date and time when such electronic surveillance activity started and the date and time when it ended.
(2) A copy of the medium containing the results of electronic surveillance activities shall be attached to the reports, in a sealed envelope. Such medium or a certified copy of it shall be kept at the premises of the prosecutors' office, in special places, in a sealed envelope, and shall be made available to the court upon request. Following seizure of the court, a copy of the medium containing electronic surveillance activities and copies of the reports shall be kept at the court's registry office, in special places, in a sealed envelope, at the exclusive disposal of the judge or judicial panel vested with the case disposition.
(2^1) Any authorized person making copies of a computer data storage medium containing results of electronic surveillance activities has the possibility to check the integrity of the data included in the original medium and, after making a copy, to sign the data included in it, by means of an extended electronic signature based on a qualified certificate issued by an accredited certification services provider, which

allows for the unequivocal identification of the authorized person, the latter taking this way responsibility for the integrity of data.
(3) Phone conversations, communications or discussions in a language other than Romanian shall be transcribed in Romanian, by means of an interpreter, who is under an obligation to keep their confidentiality.
(4) Wiretapped and recorded phone conversations, communications or discussions concerning an act subject to investigation or which contribute to the identification or localization of persons, shall be transcribed by the prosecutor or the criminal investigation bodies in a report that shall mention the warrant issued for their conducting, the phone numbers, the identification data of computer systems or of access points, names of the persons who made such communications, if known, and the date and time of each conversation or communication. Such report shall be certified by the prosecutor for authenticity purposes.
(5) After termination of a surveillance measure, the prosecutor shall inform the Judge for Rights and Liberties on the performed activities.

ART. 144
Extension of an electronic surveillance warrant
(1) An electronic surveillance warrant may be extended, for well-grounded reasons, by the Judge for Rights and Liberties of the court of competent jurisdiction, upon reasoned request by the prosecutor, in situations where the requirements set by Art. 139 are met; however, each such extension may not exceed 30 days.
(2) The Judge for Rights and Liberties shall rule in chambers, without summoning the parties, through a court resolution that is not subject to avenues of appeal. Preparation of a session minutes shall be mandatory.
(3) The total duration of an electronic surveillance measure, related to the same person and the same act, may not exceed, in the same case, 6 months, except for the measure of video, audio or photo surveillance in private spaces, which may not exceed 120 days.

ART. 145
Information of persons subject to surveillance
(1) Following termination of an electronic surveillance measure, the prosecutor shall inform each subject of the warrant for electronic surveillance enforced against them, in writing, within maximum 10 days.
(2) Following such information, a person subject to surveillance has the right to learn, upon request, of the content of the minutes recording the electronic surveillance activities performed. Also, the prosecutor has to ensure, upon request, the listening to discussions, communications or conversations, or the watching of images resulted from each electronic surveillance activity.

(3) The term for filing a request in this sense is of 20 days as of the date of communication of the written information set under par. (1).
(4) The prosecutor may postpone such information or the presentation of media on which electronic surveillance activities are stored or the minutes transcribing them, in a justified way, if this could result in:

a) disruption or jeopardizing of the proper conducting of the criminal investigation in the case;

b) jeopardizing of the safety of the victim, witnesses or members of their families;

c) difficulties in the electronic surveillance of other persons involved in the case.

(5) The postponement set under par. (4) may be ordered until completion of the criminal investigation or until the case closure, at the latest.

ART. 146

Preservation of materials resulted from electronic surveillance

(1) If a decision to close a case was returned in a case, against which a complaint was not filed within the legal term set by Art. 340 or such complaint was denied, the prosecutor shall inform the Judge for Rights and Liberties of this forthwith.
(2) The Judge for Rights and Liberties shall order preservation of the material medium or of the certified copy of it, by archiving it at the premises of the court, in special places, in a sealed envelope, in order to ensure confidentiality.
(3) If in a case the court returned a conviction sentence, a waiver of penalty or penalty reprieve, an acquittal or a termination of criminal proceedings, which remained final, the material medium or its copy shall be preserved by being archived together with the case file at the premises of the court, in special places, by ensuring confidentiality.

ART. 152

Obtaining data generated or processed by providers of public electronic communications networks or providers of electronic communication services intended for the public, other than the content of communications, and stored by these.

(1) Criminal investigation bodies, based on a prior authorization from the Judge for Rights and Liberties, may request a provider of public electronic communication networks or a provider of electronic communication services intended for the public to transmit the data stored by it, based on the special law on storage of data generated or processed by providers of public electronic communication networks and providers of electronic communication services intended for the public, other than the content of communications, in the event that there is a reasonable suspicion related to the commission of an offense and there are grounds to believe that the

requested data represent evidence for the categories of offenses set forth by the law on the storage of data generated or processed by providers of public electronic communication networks and by providers of electronic communication services intended for the public.

(2) The Judge for Rights and Liberties shall rule within 48 hours on requests transmitted by criminal investigation bodies regarding the transmission of data, through a reasoned court resolution, in chambers.

(3) Providers of public electronic communication networks and providers of electronic communication services intended for the public that cooperate with criminal investigation bodies are under an obligation to keep secrecy of the conducted operations.