



OPERATIONAL TOPIC ON INTERCEPTION OF TELECOMMUNICATION

ID 67795

SUMMARY AND COMPILATION OF REPLIES

12.05.2022

Contents

1.	Background.....	3
2.	Questionnaire	5
3.	Summary of replies	6
4.	Overview of full responses to the questionnaire	10
4.1.	Answers from National Desks and the Representative for Denmark.....	10
4.1.1.	Austria (AT)	10
4.1.2.	Belgium (BE)	13
4.1.3.	Bulgaria (BG).....	17
4.1.4.	Croatia (HR)	20
4.1.5.	Cyprus (CY)	22
4.1.6.	Czech Republic (CZ)	24
4.1.7.	Denmark (DK)	30
4.1.8.	Estonia (EE).....	32
4.1.9.	Finland (FI).....	36
4.1.10.	France (FR).....	42
4.1.11.	Germany (DE).....	44
4.1.12.	Greece (EL).....	50
4.1.13.	Hungary (HU)	53
4.1.14.	Ireland (IE)	57
4.1.15.	Italy (IT)	59
4.1.16.	Latvia (LV)	62
4.1.17.	Lithuania (LT)	66
4.1.18.	Luxembourg (LU).....	71
4.1.19.	Malta (MT).....	73
4.1.20.	The Netherlands (NL).....	75
4.1.21.	Poland (PL).....	85
4.1.22.	Portugal (PT)	98
4.1.23.	Romania (RO).....	101
4.1.24.	Slovak Republic (SK)	103
4.1.25.	Slovenia (SI)	108
4.1.26.	Spain (ES).....	112
4.1.27.	Sweden (SE)	116
4.2.	Answers from Liaison Prosecutors	120

4.2.1.	Albania (AL)	120
4.2.2.	Georgia (GE)	124
4.2.3.	Montenegro (ME)	125
4.2.4.	North Macedonia (MK)	127
4.2.5.	Norway (NO).....	130
4.2.6.	Serbia (RS)	132
4.2.7.	Switzerland (CH)	136
4.2.8.	Ukraine (UA).....	138
4.2.9.	United Kingdom (UK)	139
4.2.10.	United States of America (US).....	141

1. Background

Issues related to the interception of telecommunication have been, and still are, omnipresent in Eurojust's casework. The applicable EU law, the international law and the corresponding national laws have raised several questions on different aspects related to the interception of telecommunication.

Over the years, several desks opened related operational topics. In 2016, National Members and representatives of the Desks exchanged views and discussed Eurojust's experience in the context of cross-border interception of telecommunication at a College thematic discussion, particularly in light of the relevant provisions of the 2000 MLA Convention. As a follow-up to this thematic discussion, the College requested in its outcome report that the Judicial Cooperation Instruments (JCI) Team would follow-up on relevant Eurojust cases on interception of telecommunication, bugging of a car and the use of Trojan horse-like devices for interception.

After the entry into force of the EIO Directive, which largely copied the corresponding provisions on interception of the 2000 MLA Convention, issues have remained. Both the [Joint Note of Eurojust and the EJM on the practical application of the EIO \(2019\)](#) and the [Report on Eurojust's casework in the field of the EIO \(2020\)](#) confirmed recurrent issues and challenges in the application of the interception of telecommunication.

The JCI Team concluded that, while there is definitely already some relevant information available via the EJM website, the issues are still recurrent and impact the daily operational casework. The team members identified the need to address these recurrent issues by creating access to concise and operational information on basic requirements in other countries related to these investigative/surveillance measures. Such information is crucial, particularly in urgent cases, as national authorities often request support from Eurojust before issuing a LoR or an EIO and need precisely that information to proceed with their request under strict deadlines.

Main issues identified

A first series of issues relates to the scope of the EIO Directive. At EU level, there is no explicit regulation of certain surveillance measures (e.g. bugging of a car, GPS tracking or surveillance through a Trojan-horse-like device or audio surveillance in private places) and no uniform interpretation of the terms 'surveillance' or 'interception of telecommunication'. Yet the EIO Directive is applicable to the cross-border execution of any type of investigative measure to gather or use evidence ordered by a judicial authority, with the exception of the setting up of joint investigation teams and cross-border surveillance, as referred to in the Convention implementing the Schengen Agreement.¹ In light of this broad scope, the EIO Directive could be applicable to the mentioned surveillance² measures, if the aim of the requested measures is to gather evidence and a judicial authority issued or validated them. If these measures fall indeed within the scope of the EIO Directive, the next question would be whether they fall under the general regime of the EIO Directive or under one of the provisions related to specific

¹ On the scope of the EIO Directive, see: [Joint Note of Eurojust and the EJM on the practical application of the EIO \(2019\)](#), p. 5.

² Surveillance is understood here in the broadest sense as monitoring the movement of persons and objects, covering a wide array of activities and capabilities, as well as methods and techniques, including audio surveillance, visual surveillance, tracking surveillance and data surveillance.

investigative measures, particularly the interception of telecommunication (Articles 30-31 EIO Directive).³

In relation hereto, Eurojust's casework raises *inter alia* the following issues:

- Scope of Article 31 EIO Directive and the use of Annex C: does this provision and annex cover all types of communications or only those with telephone devices? Does it cover in particular:
 - GPS tracking device installed in the issuing Member State and crossing a border;
 - Bugged car which is crossing a border;
 - Trojan horse like software installed on a portable electronic device which is crossing a border;
 - Audio/video surveillance in private places.
- For each of the abovementioned measures the following questions are often raised:
 - Use of Annex A or Annex C and, related hereto, possibility of ex-post notification;
 - Specific conditions under national law;
 - Competent authorities.

A second series of issues follows from differences in national legal provisions and technical standards on the interception of telecommunication. In this regard, Eurojust's casework raises *inter alia* the following issues:

- Duration of the interception in the respective Member States/countries (time frames and possibilities of an extension).
- Technical possibilities to channel the intercepted conversations in real-time to the issuing authority (in accordance with Article 30(6) EIO Directive for EU Member States).

Since Articles 30-31 EIO Directive mirror largely Articles 17-22 of the 2000 MLA Convention, the majority of the abovementioned issues on the scope of the EIO DIR apply *mutatis mutandis* also to the 2000 MLA Convention - and are thus relevant to Ireland and Denmark.

Finally, also in relation to third countries, there is often a need in some cases to obtain urgently information on the main issues mentioned above (e.g. competent authorities; specific conditions). Therefore, the JCI Team suggested extending this operational topic to the Liaison Prosecutors/UK Representative.

Scope and approach

On 16 November 2021, the College approved the Operational Topic on Interception of Telecommunication with the aim to prepare from an operational perspective, an internal Eurojust document on the abovementioned interception measures. Related questionnaires were sent out to the National Desks, the Representative of Denmark and the Eurojust Liaison Prosecutors. In March 2022, the respondents were also approached with the question, whether the answers provided can be shared

³ Article 30 (interception of telecommunications with technical assistance of another Member State, need for an EIO, Annex A prior to the execution of the measure); Article 31 (interception of telecommunications without technical assistance of another Member State, no need for an EIO, only need for a notification by means of Annex C, prior, during or after the interception). Unlike Article 30, this provision is not about executing an order; there is no issuing and no executing Member State, but only an intercepting and a notified Member State. On the question of the meaning and scope of 'interception of telecommunication', see also [Report on Eurojust's casework in the field of the EIO \(2020\)](#) Eurojust Report in the field of the EIO, p. 44-46.

with the EJN (uploading on the restricted area on the EJN website) and home authorities on a case by case basis. No objections were raised in this respect by the respondents.

The Compilation of replies will be updated on a need basis, for example when additional replies are received.

2. Questionnaire

Against the background and the abovementioned issues and in view of supporting National Desks, Liaison Prosecutors and their national authorities when dealing with urgent requests for interception of telecommunication, a questionnaire was prepared which covers five different measures (GPS tracking, bugging of a car, surveillance through Trojan horse software, audio/video surveillance in a private place and interception of telecommunication abroad). The questionnaire had to be answered from the perspective of executing/requested/notified state.

An additional question on the scope of Article 31 EIO Directive and the use of Annex C had to be answered only by National Desks (EU Member States applying the EIO Directive).

The questions read as follows:

a.) GPS tracking installed in the issuing country and crossing the border (no need for technical assistance):

1. Which tool to be used (e.g. Annex A⁴/Annex C⁵/LoR/Notification in accordance with Art 20 of the 2000 MLA Convention)?⁶
2. What are the conditions for this measure to be executed in your country upon request of an issuing state (e.g. for which crimes is gps tracking allowed, possibility of an ex-post notification)?
3. Which authority in your country is in charge?

b.) Bugging of a car– installed in issuing country and crossing a border (no need for technical assistance):

1. Which tool to be used (e.g. Annex A⁷/Annex C⁸/LoR/Notification in accordance with Art 20 of the 2000 MLA Convention)?⁹
2. What are the conditions for this measure to be executed in your country upon request of an issuing state (e.g. for which crimes is the bugging of a car allowed, possibility of an ex-post notification)?
3. Which authority in your country is in charge?

c.) Surveillance through Trojan horse software installed on portable electronic devices and crossing the border:

⁴ Only applicable to EU Member States, with the exception of Denmark and Ireland.

⁵ Only applicable to EU Member States, with the exception of Denmark and Ireland.

⁶ In addition, the Liaison Prosecutors were requested to indicate the possible existence of bilateral/multilateral agreements.

⁷ Only applicable to EU Member States, with the exception of Denmark and Ireland.

⁸ Only applicable to EU Member States, with the exception of Denmark and Ireland.

⁹ In addition, the Liaison Prosecutors were requested to indicate the possible existence of bilateral/multilateral agreements.

1. Is surveillance through Trojan horse software a legal form of interception in your country?
2. In case of affirmative answer, what are the conditions for this measure?
3. In case of a negative answer, what could possible alternative measures be?
4. Which tool to be used (e.g. Annex A¹⁰/Annex C¹¹/LoR/Notification in accordance with Art 20 of the 2000 MLA Convention)?¹²
5. Which authority in your country is in charge?

d.) Audio/video surveillance in a private place:

1. Does your national legislation provide for the possibility of carrying out audio/video surveillance in a private place?
2. In case of affirmative answer, what are the conditions for this measure and which authority is competent to execute it?
3. In case of a negative answer, what could possible alternative measures be?

e.) Interception of telecommunication abroad:

1. What are the conditions for an interception of telecommunication to be executed in your country upon request of an issuing state (maximum duration, which crimes, urgent cases, extension/prolongation)?
2. Which authority is competent to execute this measure?
3. Is it technically possible to channel the intercepted telecommunication to the issuing state in real-time?¹³¹⁴

f.) Scope of Article 31 EIO Directive and use of Annex C:¹⁵

1. Are there any other types of interception of telecommunication for which your home authorities would deem an Annex C notification as sufficient?
2. Which is the competent authority to receive an Annex C notification?
3. What are the accepted languages for Annex C notifications, in particular when urgency is given?

3. Summary of replies

A total of 19 National Desks (AT, BE, BG, CZ, DE, EE, EL, ES, FI, HU, IT, LT, LV, NL, PL, PT, SE, SI, SK), the Representative for DK and seven Liaison Prosecutors (AL, ME, MK, NO, RS, CH and UK) replied to the abovementioned questionnaire. From the answers it is apparent that different approaches exist in the countries, for example as to which tool to use for GPS tracking and bugging of a car, the legal possibilities to conduct a surveillance through Trojan horse software and audio/video surveillance in a private place and the technical possibilities to channel intercepted telecommunication to the issuing state in real-time.

¹⁰ Only applicable to EU Member States, with the exception of Denmark and Ireland.

¹¹ Only applicable to EU Member States, with the exception of Denmark and Ireland.

¹² In addition, the Liaison Prosecutors were requested to indicate the possible existence of bilateral/multilateral agreements.

¹³ For EU Member States, with the exception of Denmark and Ireland, see also Article 30 (6) EIO DIR.

¹⁴ In addition, the Liaison Prosecutors were requested to indicate the possible existence of bilateral/multilateral agreements.

¹⁵ Questions only applicable to EU Member States, with the exception of Denmark and Ireland.

Below summary provides a short overview on some findings emerging from the replies received. More detailed information, in particular on the conditions for a specific measure and the authorities in charge can be found in the full responses per country under Heading 4.

GPS tracking installed in the issuing country and crossing the border (no need for technical assistance) – which tool to be used?

Issuing state applies the EIO DIR: Eight respondents noted that for such a measure, an Annex A form is required (AT, BE, CZ, DE, LV, NL, PL, ES). One respondent specified that this Annex A form does not apply to cross-border surveillance¹⁶ (NL); in such a case, a request on the basis of Art. 40 Schengen Convention would need to be submitted in case of urgency. Another respondent confirmed that both, an Annex A form and Annex C notification, are possible (ES).

Nine respondents indicated that an Annex C notification is sufficient for such a measure (BG, EE, FI, EL, HU, LT, PT, SI, ES).

One respondent underlined that no request is needed, and that the measure can be carried out directly by the other Member State without notification (IT). Also another respondent highlighted that in general, there is no need for an EIO/LoR as GPS tracking is considered to fall under the competence of the Law Enforcement Agencies (SE). Another respondent noted that if a Member State submits a respective EIO, the EIO will be assessed as a request for legal assistance under the relevant international treaties governing cross-border surveillance (SK) as in accordance with point 9 of the Preamble to the EIO Directive, SK does not apply the EIO to cross-border surveillance. Also another respondent made reference to Art. 40 of the Schengen Convention and the need to contain all necessary information, especially in urgent cases (FI).

Bugging of a car– installed in issuing country and crossing a border (no need for technical assistance) – which tool to be used?

Issuing state applies the EIO DIR: Nine respondents answered that an Annex A form is needed for the bugging of a car installed in the issuing country and crossing a border (AT, CZ, FI, DE, LV, NL, PL, SK, SE). One of the respondents noted that an Annex A form is to be used, but that the executing authorities may also accept an Annex C notification (ES). An Annex C notification was indicated as sufficient by nine respondents (BE, BG, EE, EL, HU, IT, LT, PT, SI).

Surveillance through Trojan horse software installed on portable electronic devices and crossing the border – is it a legal form of interception in your country?

EU Member States and third countries: 17 respondents replied that it is possible according to their national legislation to conduct a surveillance through Trojan horse software installed on portable electronic devices (DK, EE, FI, DE, HU, IT, LT, NL, PL, PT, SK, ES, SE; AL, NO, RS, CH). Another respondent added that this measure is to be seen as a starting point (DK). One respondent underlined that according to the prevailing view in legal literature it is not possible to use Trojan horse software in order to collect data by means of controlling the microphone and/or the camera of an electronic device (DE). One respondent noted that this measure is not provided as such in the national legislation, but that it is

¹⁶ In this context, a cross-border surveillance is understood to mean 1. an observation of persons started in a certain country that is continuously monitored across the border of another (neighbouring) country. This also applies to observation via a GPS tracker that is continuously monitored. 2. an observation started in another country of persons traveling by plane, train or boat to NL, whereby the observation was continued in that means of transport, or the persons involved were observed until they were (guaranteed) on board that means of transport and the means of transport then goes directly to NL without any stopovers.

considered as a technical means of intercept (BE). Another respondent answered that surveillance through Trojan horse software on portable devices is not an investigation procedure in their country, but could be used as tactical method, with an Annex A form as a requirement (LV). One country stated that their home authorities should be contacted to discuss the requirements (UK).

Six respondents informed that the use of Trojan horse software is not allowed in their country (AT, BG, CZ, EL, SI; MK).

Additional information on the tool to be used when the issuing state applies the EIO DIR: eight respondents informed that an Annex A form is needed (FI, DE, LT, NL, PL, PT, ES, SE), while two respondents referred to Annex C notifications (HU, SK). Another two respondents informed that depending on whether technical assistance is needed, either an Annex A form or Annex C notification is required (IT, LT).

Audio/video surveillance in a private place – does your national legislation provide for this possibility?

EU Member States and third countries: 21 respondents answered that an audio/video surveillance in a private place is possible (AT, BE, BG, CZ, DK, EE, HU, IT, LV, LT, NL, PL, PT, SK, SI, ES, SE; AL, CH, , MK, UK). Two respondents noted that only audio surveillance and not video surveillance is allowed (FI, DE). One respondent informed that video surveillance in a private place is allowed, although video-surveillance in a private home is not allowed; however, a police officer may observe through a window inside a private home using binoculars (NO).

Two respondents underlined that an audio/video surveillance in a private place is not possible in their country (EL, RS), because of a constitutional guarantee of inviolability of home (RS).

Interception of telecommunication abroad - technical possibility to channel the intercepted telecommunication to the issuing state in real-time?

EU Member States and third countries: 13 respondents answered that a real-time transmission of intercepted telecommunication to the issuing state is possible (BE, BG, CZ, DK, DE, HU, IT, NL, PT, SK; NO, RS, CH) while five respondents gave a negative answer (EE, PL, SI, ES; MK).

One respondent added that even though legally possible, in practice a real-time transmission is not feasible (PT). Another respondent highlighted that a real-time transfer of content data is only possible in cases of organised crime or terrorism (CH). It was specified by one respondent that direct electronic transmission may be possible provided that the issuing state holds a secure communication end-point that is compatible with the system of the own national authority performing the interception and technically recording data (HU). Two respondents underlined that it depends on case by case (LV, LT). One respondent who gave a negative reply, explained that this is due to a dedicated software their police uses for the interception of communication and that investigators produce transcripts and reports with their observations, save them on a storage medium and hand it over to a competent authority (SI).

One respondent said that even though it is technically possible, it has never been done; in addition, it would depend on the target company, the requesting country, the amount and quality of the data; it would also require a separate connection to be built between the telecommunications interception systems of the requesting country and the implementing country, and need to ensure that the target and content are in accordance with the warrant (FI).

Another respondent (SE) highlighted different scenarios: with EU Member States in practice, there would be no direct transmission. In urgent cases, the material could be transmitted with 30 – 60 minutes delay (a well functioning contact between the technicians who operate the interception systems in each country is needed). A real-time transmission would be possible with DK, IE, Iceland and NO – however, with the same practical limitations.

One country noted that their home authorities should be contacted to discuss the requirements (UK).

Accepted languages for Annex C notifications, in particular when urgency is given (EU Member States applying the EIO DIR):


12 respondents replied that an Annex C notification in English language would be accepted, either in general or in urgent cases, or depending on the circumstances on a case by case basis (AT, BE, BG, FI, DE, EL, HU, LV, LT, NL, SI, SE). Three respondents referred to certain additional languages accepted in their country (BE, FI, HU).

Six respondents indicated that an Annex C notification is not accepted in English language (CZ, IT, PL, PT, SK, ES). However, four respondents noted that with respect to a neighboring country they accept notifications in each others languages (CZ and SK; PT and ES).

4. Overview of full responses to the questionnaire

4.1. Answers from National Desks and the Representative for Denmark


4.1.1. Austria (AT)

AUSTRIA 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Annex A EIO DIR. 2. The crime must be punishable with more than one year of imprisonment. 3. Prosecutor.
DK or IE as issuing state	<ol style="list-style-type: none"> 1. LoR. 2. The crime must be punishable with more than one year of imprisonment. 3. Prosecutor.
Issuing state is a third State	<ol style="list-style-type: none"> 1. LoR. 2. The crime must be punishable with more than one year of imprisonment. 3. Prosecutor.
Bugging of a car	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Annex A EIO DIR 2. Video and audio surveillance of persons is permissible, <ul style="list-style-type: none"> - if and so long there is strong suspicion that the person affected by the surveillance has kidnapped or otherwise taken control of another person and if the surveillance is limited to events and statements at the time and the place of the deprivation of liberty, - if the surveillance is limited to events and statements that are meant to be noted by an undercover investigator or another person aware of the surveillance or if the events or statements can be directly noted by such a person and if the surveillance appears to be necessary to make inquiries about a felony (maximum prison sentence more than 3 years), - if the inquiry about a criminal offence punishable by imprisonment for more than ten years or a terrorist offence or the inquiry about or prevention of a felony committed or planned as part of a criminal organization or terrorist association or the investigation of the whereabouts of a person accused of any of these offences would otherwise be pointless or significantly obstructed and <ol style="list-style-type: none"> a. if the person under surveillance him/herself is under a strong suspicion of the offence, or b. because of particular material facts it is believed that contact by a person under such a strong suspicion may be made to the person under surveillance. <p>It is important to note that the investigative measure can only be ordered in advance and not retroactively</p> 3. Prosecutor, but a judge has to grant the warrant.

DK or IE as issuing state	<ol style="list-style-type: none"> 1. LoR. 2. See above 3. Prosecutor, but a judge has to grant the warrant.
Issuing state is a third State	<ol style="list-style-type: none"> 1. LoR. 2. See above 3. Prosecutor, but a judge has to grant the warrant.
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. No. 2. Not applicable 3. Telephone/Internet communication surveillance; use of hidden microphones or cameras; GPS tracking devices. 4. Not applicable 5. Not applicable
DK or IE as issuing state	All as above.
Issuing state is a third State	All as above.
Audio/video surveillance in a private place	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Yes. 2. See answers under b). 3. Not applicable
DK or IE as issuing state	<ol style="list-style-type: none"> 1. Yes. 2. See answers under b). 3. Not applicable
Issuing state is a third State	<ol style="list-style-type: none"> 1. Yes. 2. See answers under b). 3. Not applicable
Interception of telecommunication abroad	
Issuing state	1. No maximum duration, but the duration has to be reasonable. Crimes with a punishment of more than one year or terrorism or OCG crimes. No special regulation for urgent cases. Prolongation is possible, if success is probable.

applies EIO DIR	2. Prosecutor, but the warrant has to be granted by a judge. 3. Yes.
DK or IE as issuing state	All as above.
Issuing state is a third State	All as above.
Scope of Article 31 EIO Directive and use of Annex C	
1. No. 2. The locally competent prosecutor's office. 3. In principle, Annexes A and C have to be translated into German unless the issuing state itself accepts a transmission in German (see AT notification of 23/6/2019). In urgent cases, most prosecutor's offices would probably accept an English version but there is no obligation.	

4.1.2. Belgium (BE)


BELGIUM 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	<p>1. Annex A EIO DIR.</p> <p>2. This is a technical observation that can only be authorised when there are serious indications that the offences are of such a nature as to lead to a principal correctional sentence of one year or more (and when the needs of the investigation so require and other means of investigation do not appear to be sufficient to ascertain the truth).</p> <p>The notification must be made in advance.</p> <p>3. PPO is the competent authority to authorise such a technical observation.</p>
DK or IE as issuing state	
Issuing state is a third State	
Bugging of a car	
Issuing state applies EIO DIR	<p>1. Annex C EIO DIR (might be sufficient in principle, and would be appropriate with an explanation about the reasons already taken into consideration for issuing such an investigating measure).</p> <p>2. The Belgian Code of criminal procedure states (Article 90ter §6) that a competent foreign authority may, in the context of a criminal investigation, temporarily intercept, take note and record communications not accessible to the public (or data from a computer system) when the person concerned by this measure is on Belgian territory and if the following conditions are met:</p> <p>1° this measure does not involve the technical intervention of an actor located in Belgium</p> <p>2° the foreign authority concerned has notified this measure to a Belgian judicial authority</p> <p>3° this possibility is provided for by an instrument of international law binding Belgium and the requesting State</p> <p>4° the decision of the investigating judge (referred to in § 7) has not yet been communicated to the foreign authority concerned.</p> <p>The data collected under this paragraph may only be used if the competent Belgian judicial authority authorizes the measure.</p> <p>Article 90ter § 7 of the Belgian Code of criminal procedure, indicates that : as soon as the public prosecutor receives the notification referred to in § 6, first paragraph, 2°, he or she shall immediately refer the matter to the investigating judge.</p> <p>The Investigating Judge to whom a notification (referred to in paragraph 6, subparagraph 1, 2°) is referred authorises the measure in question if it is admissible under the provisions of this article. (The investigating Judge will verify if the measure is requested for one of the offences listed in the Belgian penal Code (under Article 90ter §2 to §4) and will determine</p>

	<p>under which conditions the interception of the telecommunications may take place, for instance in terms of duration).</p> <p>If the investigating judge does not authorize the measure referred to in § 6, he or she shall also inform the foreign authority that the intercepted data must be destroyed without being used.</p> <p>3. The notification must be made immediately to the prosecutor, who will immediately refer the matter to the investigating judge.</p>
DK or IE as issuing state	
Issuing state is a third State	
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	<p>1. Surveillance through Trojan horse is not provided as such in the Belgian legislation. The Trojan horse is however to be considered as a technical means of intercept, take note and record communications not accessible to the public (or data from a computer system).</p> <p>As a matter of consequence, the answers to questions one, two and three of point b), related to the conditions for the measure, the tool to be used and the competent authority, also applies to this case.</p>
DK or IE as issuing state	
Issuing state is a third State	
Audio/video surveillance in a private place	
Issuing state applies EIO DIR	<p>1. Yes, but video surveillance and audio surveillance are two different things that must be distinguished.</p> <p>2. The PPO is the competent authority to issue an authorization of video surveillance in a private place, with the exception of a “home” (by home is meant a place and its annexes which are not public and which serve as a accommodation, a permanent or temporary residence or a place of business for a physical or legal entity who uses it as a shelter for a part of his private life).</p> <p>The investigating Judge is the competent authority to issue an authorization of video surveillance (observation) in a private place considered as a “home” (see above). He is the only competent authority to issue a wiretap order in a private place.</p> <p>Video surveillance (observation) might be carried out in a private place considered as a “home”, for a period of 3 months, under the following conditions :</p> <ul style="list-style-type: none"> - when there are serious indications that the punishable acts constitute or would constitute an offence referred to in Article 90ter, §§ 2 to 4, of the Belgian Code of

	<p>criminal procedure , or are or would be committed within the framework of a criminal organization (referred to in Article 324bis of the Belgian penal Code);</p> <ul style="list-style-type: none"> - only if the needs of the investigation require such measure and if other means of investigation do not appear to be sufficient to ascertain the truth. <p>Audio surveillance /interception private communication order might be issued, for a period of one month (renewable but not extendable above 6 months) by the investigating Judge on top of the authorization of observation, in a private place considered as a “home”, under the following conditions :</p> <ul style="list-style-type: none"> - The measure may only be ordered in respect of persons suspected, on the basis of specific evidence, of having committed the offence, or in respect of means of communication (or computer systems) regularly used by a suspect, or in respect of places presumed to be frequented by him. It may also be ordered in respect of persons presumed, on the basis of specific facts, to be in regular communication with a suspect; - In respect with the principles of proportionality and subsidiarity : only in exceptional cases, when the needs of the investigation require so, if there are serious indications that it concerns an offence referred to in Article 90ter paragraph 2 of the Belgian Code of criminal procedure , and if the other means of investigation are not sufficient to establish the truth; <p>3. /</p>
DK or IE as issuing state	
Issuing state is a third State	
Interception of telecommunication abroad	
Issuing state applies EIO DIR	<p>1. Interception of telecommunication may be executed in Belgium upon request of an issuing state, under the following conditions :</p> <ul style="list-style-type: none"> - The measure may only be ordered in respect of persons suspected, on the basis of specific evidence, of having committed the offence, or in respect of means of communication (or computer systems) regularly used by a suspect, or in respect of places presumed to be frequented by him. It may also be ordered in respect of persons presumed, on the basis of specific facts, to be in regular communication with a suspect; - In respect with the principles of proportionality and subsidiarity : only in exceptional cases, when the needs of the investigation so require, if there are serious indications that it concerns an offence referred to in Article 90ter paragraph 2 of the Belgian Code of criminal procedure , and if the other means of investigation are not sufficient to establish the truth; - For a duration of one month, renewable, with a maximum total period of 6 months. And if renewed, with the indication of the specific circumstances that justify the extension of the measure. <p>2. The Investigating Judge is the competent authority to execute the measure.</p> <p>Belgian legislation provides for exceptions in cases of flagrante delicto, for which the PPO is competent.</p>

	3. Yes.
DK or IE as issuing state	
Issuing state is a third State	
Scope of Article 31 EIO Directive and use of Annex C	
1. No 2. See answers below. 3. Accepted languages for Annex C are : English, French, Dutch and German.	


4.1.3. Bulgaria (BG)

<div style="text-align: center;"> BULGARIA  </div>	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	<p>1. Annex C EIO DIR.</p> <p>2. GPS tracking is a technical method according to art. 7 of the Bulgarian Law on Special Intelligence Means, which can be executed for the crimes according to art. 172, para 2 of the Criminal Procedure Code: „172(2) (Supplemented, SG No. 60/2011, SG No. 17/2013, SG No. 42/2015, SG No. 39/2016) Special intelligence means shall be used where this is required for the investigation of serious criminal offences of intent under Chapter one, Chapter two, Sections I, II, IV, V, VIII, and IX, Chapter three, Section III, Chapter five, Sections I - VII, Chapter six, Section II - IV, Chapter eight, Chapter eight "a", Chapter nine "a", Chapter eleven, Sections I - IV, Chapter twelve, Chapter thirteen, and Chapter fourteen, as well as with regard to criminal offences under Article 219, para 4, proposal 2, Article 220, Paragraph 2, Article 253, Article 308, Paragraphs 2, 3, and 5, sentence two, Article 321, Article 321a, Article 356k and 393 of the Special Part of the Criminal Code, where the relevant circumstances cannot be established in any other way or this would be accompanied by exceptional difficulties.“</p> <p>The notification must be made in advance, during or immediately after the set-off.</p> <p>3. The District, Specialized or Military district prosecutor's office is the competent authority to rule on the notification under Article 9, para (1), p.1 of the European Investigation Order Act.</p>
DK or IE as issuing state	<p>1. LoR – Art. 20 of the 2000 EU MLA Convention</p> <p>2. Art. 172, para 2 of the Criminal Procedure Code corresponding to art. 3 of the Law on Special Intelligence Means</p> <p>3. The competent body to receive the LoR on the 2000 EU MLA Convention is the District Po, Specialized or Military district Po and the competent court to allow such technical observation is the respective District Court, Specialized or Military district Court. Article 6 of the MLA Convention is applicable, relevant to Article 13 of the Bulgarian Law on Special Intelligence Means.</p> <p>When that investigative measure constitutes a form of a Cross-border observations (continuing) within the meaning of the Second Additional Protocol ECMA the competent body to receive the LoR is the Supreme Po and the competent authority to allow such technical observation is the Sofia City Court.</p>
Issuing state is a third State	<p>1. LoR – The functional (regulating procedure and technology) and sectoral (determining the counteraction at the supranational level of a certain type of crime) conventions are applicable. Examples of the first type are the 1959 ECMA, the 2001 ECMA Second Protocol and others. Examples of the second type are the UN Convention on Transnational Organized Crime (UNTC), the Council of Europe Convention on Cybercrime (Budapest Convention) and others. May apply reciprocity. With regard to requests from the United Kingdom of Great Britain and Northern Ireland (UK), Title VIII of Part Three of the Trade and Cooperation Agreement between the UK and the EU (TCA) should also apply.</p> <p>2. Art. 172, para 2 of the Criminal Procedure Code</p> <p>3. The competent body to receive the LoR is the Supreme Po and the competent authority to allow such technical observation is the Sofia City Court.</p>

Bugging of a car	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Annex C EIO DIR. 2. The statement in item I.2 applies 3. The answers in point II.2 are given from this perspective.
DK or IE as issuing state	<ol style="list-style-type: none"> 1. The same answer like on a) 2. 3.
Issuing state is a third State	<ol style="list-style-type: none"> 1. The same answer like on a) 2. 3.
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. The legislation of Bulgaria does not contain a regulation on surveillance through Trojan horse software.
DK or IE as issuing state	
Issuing state is a third State	
Audio/video surveillance in a private place	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Yes, special intelligence means through the method of surveillance - visually and through technical means, can be applied to sites - Art. 5, art. 12, p. 3 and p. 4 of the Law on Special Intelligence Means. The method is applicable when requested by the EIO, Annex A to the EIO Directive. 2. The condition is to be allowed by the court, at the request of a body under Art. 13 of the Law on Special Intelligence Means, being applied by the bodies under art. 20 - State Agency for Technical Operations, Specialized Directorate for Technical Operations of the State Agency for National Security and the Ministry of Interior. 3.
DK or IE as issuing state	<ol style="list-style-type: none"> 1. The method is applicable according to p. IV.2, when it is requested with a LoR according the 2000 MLA Convention, and if it is allowed by the court. 2. 3.


Issuing state is a third State	<ol style="list-style-type: none"> 1. The method is applicable according to p. IV.2, when this has been requested by a classic LoR under the 1959 ECMA and its protocols, under one of the "sectoral" conventions, by bilateral agreement or on the basis of the principle of reciprocity and if execution of the request has been allowed, and if the court has given its permission. 2. 3.
Interception of telecommunication abroad	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. The interception of telecommunications with technical assistance by the executing State takes place in compliance with the approved EIO - Annex A to the EIO Directive. Their recording / transmission / forwarding takes place in the execution of the EIO and a court permit for the application of a method under the Law on Special Intelligence Means. The terms are determined in Article 21 of the Law - for a duration of 20 days, renewable, with a maximum total period of 6 months. If renewed - with the indication of the specific circumstances that justify the extension of the measure. 2. The EIO is accepted by the respective district / military or specialized PO under Art. 9, para 1, p. 1 of the European Investigation Order Act or the respective district / military or the specialized criminal court under art. 9, para. 1 p. 2 of the Law. 3. Yes. According to Art. 34, para. 6, p.1 of the Law.
DK or IE as issuing state	<ol style="list-style-type: none"> 1. In execution of a LoR under the 2000 MLA Convention, followed by a court's permission to apply a method under the Law on Special Intelligence Means . 2. 3.
Issuing state is a third State	<ol style="list-style-type: none"> 1. The method is applied when requested by a classic LoR under the 1959 ECMA and its protocols, under one of the "sectoral" conventions, under a bilateral agreement or on the basis of the principle of reciprocity when execution of the request is allowed, and if the court has given permission. In relations with the UK, Title VIII of Part Three of the Trade and Cooperation Agreement between the UK and the EU (TCA) should also apply. 2. 3.
Scope of Article 31 EIO Directive and use of Annex C	
<ol style="list-style-type: none"> 1. The notification in Annex C shall be used most appropriately in the case of authorized and initiated interception of electronic correspondence in an intercepting country, when the e-mail address is used / accessed from the territory of another country. In this case, the interception of messages generated during the person's stay in the other country can continue unhindered and without technical assistance. 2. Again - the relevant district / military or specialized PO under Art. 9, para 1, p. 1 of the European Investigation Order Act or the respective district / military or the specialized criminal court under art. 9, para. 1 p. 2 of the Law. 3. Bulgarian and English - as for EIO. 	

4.1.4. Croatia (HR)

CROATIA 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Bugging of a car	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	

Audio/video surveillance in a private place	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Interception of telecommunication abroad	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Scope of Article 31 EIO Directive and use of Annex C	
Relevant documents	

4.1.5. Cyprus (CY)

CYPRUS 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Bugging of a car	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	

Audio/video surveillance in a private place	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Interception of telecommunication abroad	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Scope of Article 31 EIO Directive and use of Annex C	
Relevant documents	

4.1.6. Czech Republic (CZ)


CZECH REPUBLIC	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	<p>1. Annex A EIO DIR.</p> <p>2. GPS tracking is not considered as interception of telecommunication traffic under Czech law, but as surveillance of persons and items. The EIO is recognised and executed according to Art. 387 and 388¹(that implemented Art 28 of the EIO Directive) in compliance with Art. 63² of the Act on International Judicial Cooperation in Criminal Matters, plus the conditions in Art. 158d³ (1), (2), (4) of the Criminal Procedure Code of the Czech Republic:</p> <p>a) a priori request – Annex A of the EIO. GPS tracking (even without police officers escorting the vehicle being followed) is considered as crossborder surveillance, because the vehicle being followed is in a different state from the one in which the criminal proceedings are being conducted.</p> <p>b) Urgent cases – The Directive does not provide legal framework for urgent cases – carrying out crossborder surveillance before the EIO is delivered. Therefore, in order to be able to respond to cases where a tracked vehicle unexpectedly crosses the state border, we assume that what is not covered by the Directive can be covered by international treaties (according to Art 34(1) of the EIO Directive, this Directive replaces only corresponding provisions of the Convention implementing the Schengen Agreement). Therefore, we apply in these urgent situations Art 40 (2) of the Convention implementing the Schengen Agreement or bilateral treaties with AT, DE and SK (that we notified to the Commission according to Art 34(4) of the EIO Directive).</p> <p>It means that the foreign police authority can cross a border without previous approval, but have an obligation to terminate surveillance if they do not receive the authorization within 5 hours - see Art 40(2) of the Convention implementing the Schengen Agreement (bilateral treaties prolonged these time limits – with AT - 24 hours, DE – 12 hours, the hours between 9 p.m. and 9 a.m. do not count, and SK – 12 hours) after crossing the state border or if the competent Czech authority asks so – the Regional Prosecutor’s Office in Prague may grant a post facto authorization of such surveillance on the basis of a LoR.</p> <p>c) The EIO Directive also does not address situations where a Member State carries out GPS tracking that does not require technical or personnel assistance from another State and only discovers after checking the records that the tracked vehicle has already been on the territory of another State. This situation usually comes to light some time after the surveillance has been carried out. Given that GPS tracking is also considered cross-border surveillance and that the recordings are used as evidence in criminal proceedings, we needed to work out, at least with neighbouring countries, how to ensure that the recordings obtained in this way could also be used as evidence in criminal proceedings.</p> <p>We found the solution in the “request for consent with using of record of surveillance that was gained only via technical devices of requesting state without technical or personal support of the requested state” that is stipulated in our bilateral treaties with Austria, Germany and Slovakia:</p> <p>Austria – the request for consent is regulated in Art 28(6)(7) of the bilateral treaty.</p> <p>Germany – the request for consent Art 19(4) of the bilateral treaty</p> <p>Slovakia - the request for consent is regulated in Art 9(9) of the bilateral treaty.</p> <p>d) conditions for the approval</p>

	<ul style="list-style-type: none"> • such a surveillance can be used only in criminal proceedings concerning an intentional criminal offence (Sec. 158b(1) of the CPC) details of the item or person to be monitored, • for a maximum period of 6 months (renewable for a further 6 months repeatedly). • such a surveillance will not be used for any other purpose than for <u>acquiring matters substantial for criminal proceedings</u> (Sec. 158b(2) of the CPC) • it may be used <u>only when the purpose in question may not be reached in other ways or if reaching it would otherwise be considerably more complicated</u> (Sec. 158b(2) of the CPC) • rights and liberties of persons may be restricted only in an absolutely necessary extent. <p>3. the Regional Public Prosecutor's Office in Prague⁴ - the approval is given by the public prosecutor.</p>
DK or IE as issuing state	<p>1. LoR</p> <p>2. same as above - the CZ national legal framework for cross-border surveillance - without treaty only „technical“ surveillance is possible – based on reciprocity (DK and IE made a reservation concerning Art 17 of the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters)</p> <p>3. the Regional Public Prosecutor's Office in Prague</p>
Issuing state is a third State	<p>1. LoR</p> <p>2. same as above</p> <p>CoE states:</p> <ul style="list-style-type: none"> ➤ the CR ratified the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters and applies Article 17 (Cross-border observations) ➤ cross border surveillance is possible with all CoE states that also ratified this Additional protocol and did not make a reservation concerning Art 17 <p>all other states - the CZ national legal framework for cross-border surveillance - without treaty only „technical“ surveillance is possible based on reciprocity (otherwise, surveillance involving police officers crossing national borders is only possible with non-EU countries on the basis of an international treaty - „technical“ surveillance is possible only based on reciprocity)</p> <p>3.</p> <p>a) the Supreme Public Prosecutor's Office ⁵</p> <p>b) the Regional Public Prosecutor's Office in Prague – <i>in case of States under the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, where direct cooperation applies.</i></p>
Bugging of a car	
Issuing state applies EIO DIR	<p>1. Annex A EIO DIR</p> <p>2. Art. 387 and 388 in compliance with Art. 63 of the Act on International Judicial Cooperation in Criminal Matters, plus the conditions in Art. 158d ⁶ (1), (3), (4) of the Criminal Procedure Code of the Czech Republic:</p> <ul style="list-style-type: none"> • such a surveillance can be used only in criminal proceedings concerning an intentional criminal offence (Sec. 158b(1) of the CPC) • details of the item or person to be monitored,


	<ul style="list-style-type: none"> • for a maximum period of 6 months (renewable for a further 6 months repeatedly), can be done only on the bases of court order, • such a surveillance will not be used for any other purpose than for acquiring matters substantial for criminal proceedings (Sec. 158b(2) of the CPC) • it may be used only when the purpose in question may not be reached in other ways or if reaching it would otherwise be considerably more complicated (Sec. 158b(2) of the CPC) • rights and liberties of persons may be restricted only in an absolutely necessary extent. • if a police authority ascertains that the accused person is communicating with his defence counsel, it is obliged to destroy the record containing this communication and not to use facts learned in this connection in any way. <p>3) Art. 158d(5) of the Criminal Procedure Code of the Czech Republic: such a surveillance cannot be initiated without a court order, therefore this is possible only a priori, there is no option in domestic criminal proceedings to receive the court order retrospectively. However, bilateral treaties with Austria, Germany and Slovakia that stipulate the special procedure for consent with using of record of such surveillance that was gained only via technical devices of requesting state without technical or personal support of the requested state refer only to “technical devices of requesting state without technical or personal support of the requested state” and do not distinguish between technical devices that only monitor the person and those that not only monitor the person but also record his/her (non-telecommunication) conversation. Pursuant to Article 10 of the Constitution of the Czech Republic, these international treaties take precedence over national law if they provide otherwise. On the other hand, so far, we have no experience of how the court would assess this case and whether it would give consent in such a case. Therefore, we recommend that also these states should rather deal with the surveillance with “a spatial interception” in the vehicle in advance. That is, they should ask the Czech Republic for this form of cooperation before the vehicle enters the Czech Republic.</p> <p>3. the EIO has to be sent to the Regional Public Prosecutor's Office in Prague, the prosecutor issues a motion, which is sent to the Regional Court in Prague for decision</p>
DK or IE as issuing state	<ol style="list-style-type: none"> 1. LoR 2. same as above 3. LoR has to be sent to the Regional Public Prosecutor's Office in Prague the prosecutor issues a motion, which is sent to the Regional Court in Prague for decision
Issuing state is a third State	<ol style="list-style-type: none"> 1. LoR 2. same as above 3. <ol style="list-style-type: none"> a) the Supreme Public Prosecutor's Office b) the Regional Public Prosecutor's Office in Prague – <i>in case of States under the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, where direct cooperation applies</i>
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. This measure is not used to gain evidence in the Czech Republic 2. ----- 3. There is no alternative measure 4. -----

	5. -----
DK or IE as issuing state	1. This measure is not used to gain evidence in the Czech Republic 2. ----- 3. there is no alternative measure 4. ----- 5. -----
Issuing state is a third State	1. This measure is not used to gain evidence in the Czech Republic 2. ----- 3. There is no alternative measure 4. ----- 5. -----
Audio/video surveillance in a private place	
Issuing state applies EIO DIR	1. YES 2. Art. 158d (1), <u>(3)</u> , (4) of the Criminal Procedure Code of the Czech Republic: <ul style="list-style-type: none"> such a surveillance can be used only in criminal proceedings concerning an intentional criminal offence (Sec. 158b(1) of the CPC) details of the item or person to be monitored, for a maximum period of 6 months (renewable for a further 6 months repeatedly), can be done only on the bases of court order, such a surveillance will not be used for any other purpose than for acquiring matters substantial for criminal proceedings (Sec. 158b(2) of the CPC) it may be used only when the purpose in question may not be reached in other ways or if reaching it would otherwise be considerably more complicated (Sec. 158b(2) of the CPC) rights and liberties of persons may be restricted only in an absolutely necessary extent. if a police authority ascertains that the accused person is communicating with his defence counsel, it is obliged to destroy the record containing this communication and not to use facts learned in this connection in any way. <p>Art. 158d(5) of the Criminal Procedure Code of the Czech Republic: - surveillance <u>cannot be initiated without a court order</u>. In these cases, the above-mentioned consent procedure cannot be applied in relation to Austria, Germany and Slovakia, as it only applies to surveillance initiated in the territory of one State, which continues to the territory of the other State.</p> <p>Competent authority:</p> <p>a) the EIO has to be sent to the Regional Public Prosecutor's Office according to the location of the private place, the prosecutor issues a motion, which is sent to the Regional Court for decision (in pre-trial proceeding)</p> <p>b) the EIO has to be sent to the Regional Court according to the location of the private place, where the judge makes a decision (in trial proceeding)</p> 3. -----

DK or IE as issuing state	<p>1. YES</p> <p>2. same as above</p> <p>Competent authority</p> <p>a) the LoR has to be sent to the Regional Public Prosecutor's Office according to the location of the private place, the prosecutor issues a motion, which is sent to the Regional Court for decision (in pre-trial proceeding)</p> <p>b) the LoR has to be sent to the Regional Court according to the location of the private place, where the judge makes a decision (in trial proceeding)</p> <p>3. ----</p>
Issuing state is a third State	<p>1. YES</p> <p>2. same as above</p> <p>Competent authority:</p> <p>a) the Supreme Public Prosecutor's Office (in pre-trial proceeding) / the Ministry of Justice⁷(in trial proceeding)</p> <p>b) the Regional Public Prosecutor's Office according to the location of the private place the prosecutor issues a motion, which is sent to the Regional Court for decision (in pre-trial proceeding) / the Regional Court according to the location of the private place (in trial proceeding) – <i>in case of States under the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters, where direct cooperation applies</i></p> <p>3. ----</p>
Interception of telecommunication abroad	
Issuing state applies EIO DIR	<p>1. Art. 88⁸ of the Criminal Procedure Code of the Czech Republic:</p> <ul style="list-style-type: none"> - the criminal proceedings has to be carried out for a crime for which the law prescribes a sentence of imprisonment with the upper limit of at least eight years / or for specific crimes (Art. 88 (1) CPC) / or for another intentional criminal offence, for prosecution of which is the Czech Republic bound by an international treaty, - only if there is a reasonable belief that it shall transmit information essential for criminal proceedings and the pursued purpose cannot be achieved in other ways, or if reaching this purpose would otherwise be considerably more complicated, - it can be done <u>only on the bases of court order</u> (exception according to Art. 88 (5) CPC - without an order: for specific crimes, if the user of the intercepted station consents with it) - for a maximum period of 4 months (renewable for a further 4 months repeatedly), <p>2. a) the competent Regional Public Prosecutor's Office⁹ (in pre-trial proceeding)</p> <p>b) the competent Regional Court¹⁰ (in trial proceeding)</p> <p>3. YES, it is possible but it depends on the technical possibilities (also Art. 391 (2)¹¹ of the Czech Act on International Judicial Cooperation)</p>
DK or IE as issuing state	<p>1. same as above</p> <p>2. a) the competent Regional Public Prosecutor's Office (in pre-trial proceeding)</p> <p>b) the competent Regional Court (in trial proceeding)</p> <p>3. it depends on the technical possibilities</p>


Issuing state is a third State	<ol style="list-style-type: none"> 1. same as above 2. a) the Supreme Public Prosecutor's Office (in pre-trial proceeding) / the Ministry of Justice (in trial proceeding) b) the competent Regional Public Prosecutor's Office (in pre-trial proceeding) / the competent Regional Court (in trial proceeding) – <i>in case of states under the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters</i> 3. it depends on the technical possibilities
Scope of Article 31 EIO Directive and use of Annex C	
<ol style="list-style-type: none"> 1. No, only border crossing interception of telecommunication without technical support (typically the interception of a mobile phone, which can be carried out without technical assistance from another state). 2. a) the Regional Public Prosecutor's Office in Prague (in pre-trial proceeding) b) the Regional Court in Prague (in trial proceeding) 3. Czech language, Slovak language (even in urgent cases the Czech language is required, since the court has to decide in 96 hours after the request was delivered – the conditions of the standard interception described in Art. 88 CPC must be met, therefore the Annex C must be filled in with many details, otherwise additional information is requested) 	
Relevant documents	
<div style="text-align: center;">  CZ Annex </div>	

4.1.7. Denmark (DK)

DENMARK 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	1. LoR 2. A crime where it is legally possible to get a sentence of at least 1 ½ of imprisonment. Ex post procedure should normally be possible. 3. Prosecutor/judge
Issuing state is a third State	1. LoR 2. A crime where it is legally possible to get a sentence of at least 1 ½ of imprisonment. Ex post procedure should normally be possible. 3. Prosecutor/judge
Bugging of a car	
Issuing state applies EIO DIR	1. LoR 2. The rules are a little complex, but basically at least minimum 6 years of imprisonment legally possible. Ex post procedure should normally be possible. 3. Prosecutor/judge
Issuing state is a third State	1. LoR 2. The rules are a little complex, but basically at least minimum 6 years of imprisonment legally possible 3. Prosecutor/judge
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	1. As a starting point yes 2. Could depend on the nature of the software, but generally 6 years of imprisonment possible 3. n/a 4. LoR 5. Prosecutor/judge
Issuing state is a third State	1. As a starting point yes 2. Could depend on the nature of the software, but generally 6 years of imprisonment possible 3. n/a 4. LoR 5. Prosecutor/judge

Audio/video surveillance in a private place	
Issuing state applies EIO DIR	<p>1. Yes</p> <p>2. Again normally minimum 6 years, but there are exceptions allowing the measure in less serious cases. The conditions for video surveillance are in some cases not so strict – it depends on the intrusiveness (inside a home for instance it is the more difficult to get a court order.</p> <p>3. n/a</p>
Issuing state is a third State	<p>1. Yes</p> <p>2. Again normally minimum 6 years, but there are exceptions allowing the measure in less serious cases. The conditions for video surveillance are in some cases not so strict – it depends on the intrusiveness (inside a home for instance it is the more difficult to get a court order.</p> <p>3. n/a</p>
Interception of telecommunication abroad	
Issuing state applies EIO DIR	<p>1. Normally six years of imprisonment legally possible, meaning that most serious crimes are covered. 4 weeks at a time is the maximum allowed. No overall maximum</p> <p>2. Judge on the request of a prosecutor (as for all the other measures mentioned above). Police/prosecutor can act in periculum in mora situations.</p> <p>3. It should be</p>
Issuing state is a third State	<p>1. Normally six years of imprisonment legally possible, meaning that most serious crimes are covered. 4 weeks at a time is the maximum allowed. No overall maximum</p> <p>2. Judge on the request of a prosecutor (as for all the other measures mentioned above). Police/prosecutor can act in periculum in mora situations.</p> <p>3. It should be</p>

4.1.8. Estonia (EE)


<div>ESTONIA</div> <div>  </div>	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	<p>1. Annex C EIO DIR.</p> <p>2.</p> <p>§ 126¹. General conditions for conduct of surveillance activities</p> <p><i>(2) Surveillance activities are permitted on the bases provided for in this Code if collection of data by other activities or taking of evidence by other procedural operations is impossible, is impossible on time or is especially complicated or if this may prejudice criminal proceedings in the case.</i></p> <p>§ 126². Bases for conduct of surveillance activities</p> <p><i>(1) The Police and Border Guard Board, the Security Police Board, the Tax and Customs Board, the Military Police and the Prisons Department of the Ministry of Justice and prisons (hereinafter surveillance agency) may conduct surveillance activities on the following bases:</i></p> <ol style="list-style-type: none"> <i>1) a need to collect information about the preparation of a criminal offence for the purpose of detection and prevention thereof;</i> <i>2) the execution of an order on declaring a person a fugitive;</i> <i>3) a need to collect information in confiscation proceedings pursuant to the provisions of Chapter 16¹ of this Code;</i> <i>4) a need to collect information in criminal proceedings about a criminal offence.</i> <p><i>(2) On the basis of the provisions of clauses (1) 1) and 4) of this section, surveillance activities may be conducted in the event of criminal offences specified in §§ 89-93¹, 95-97, 99, 100¹, 101-104, 106-108, 110-114, 116, 118 and 120, subsection 121 (2), §§ 133-137, 138¹ and 141-146, § 157³, subsections 151 (2) and (4), subsection 161 (2), §§ 162, 163, 172-179, 183-185, 187-190, 194, 195, 199 and 200, subsections 201 (2) and (3), subsections 202 (2) and (3), §§ 204, 206-214, 216¹-217, 217², 222, 227, 231-238, 241, 243, 244, 246, 250, 251, 255 and 256, clause 258 2), §§ 259, 259¹ and 263, subsections 266 (2) and (4), §§ 274, 290¹, 291, 291¹, 294, 296, 298-299, 300, 300¹, 302, 303, 310-313 and 315-316¹, subsection 321 (2), §§ 326-328, 331, 331³, 333-334, 335, 336, 340 and 347, subsections 356 (1) and (3), subsections 357 (1) and (3), subsections 361 (1) and (3), subsections 364 (2)-(3), §§ 375-376², 384, 389¹, 391, 393, 394 and 394¹, subsections 398 (2) and (4), subsections 398¹ (2) and (4), §§ 400, 402³, 402⁴, 403-407, 414-416, 418, 418¹, 421¹, 421², 434, 435 and 437-439, subsections 440 (3) and §§ 446 and 449 of the Penal Code.</i></p> <p><i>(3) On the basis of this Code, surveillance activities may be conducted in respect of the following persons:</i></p> <ol style="list-style-type: none"> <i>1) on the basis specified in clause (1) 1) of this section in respect of the person in the case of whom there are serious reasons to believe that he or she commits the criminal offence specified in subsection (2) of this section;</i> <i>2) on the basis specified in clause (1) 2) of this section in respect of the person who is declared to be a fugitive;</i> <i>3) on the basis specified in clause (1) 3) of this section in respect of the person who owns or possesses the assets which are the object of confiscation proceedings;</i> <i>4) on the basis specified in clause (1) 4) of this section in respect of the person who is a suspect in criminal proceedings or with respect to whom there is justified reason to believe that he or she has committed or commits the specified criminal offence.</i> <p><i>(4) The surveillance activities conducted on the basis provided for in clauses (1) 2)-4) of this section may be also conducted in respect of the person with regard to whom there is good</i></p>

	<p>reason to believe that he or she interacts with the person specified in clauses (3) 2)-4) of this section, communicates information to him or her, provides assistance to him or her or allows him or her to use his or her means of communication, and if the conduct of surveillance activities in respect of such person may provide the data required for the achievement of the objective of the surveillance activities.</p> <p>(a) § 126⁴. Grant of permission for surveillance activities</p> <p>(1) Surveillance activities may be conducted with a written permission of the Prosecutor's Office or a preliminary investigation judge. The preliminary investigation judge shall decide the grant of permission by an order on the basis of a reasoned application of the Prosecutor's Office. The preliminary investigation judge shall consider a reasoned request submitted by the Prosecutor's Office without delay and grant or refuse to grant permission for the conduct of the surveillance activities by an order.</p> <p>(2) In cases of urgency, surveillance activities requiring the permission of the Prosecutor's Office may be conducted with the permission of the Prosecutor's Office issued in a format which can be reproduced in writing. A written permission shall be formalised within 24 hours as of the commencement of surveillance activities.</p> <p>(3) In the case of immediate danger to the life, physical integrity or physical freedom of a person or to proprietary benefits of high value and requesting a permission or execution thereof on time is impossible, surveillance activities requiring the permission of a court may be conducted, in cases of urgency, with the permission of the court issued in a format which can be reproduced in writing. A written application and permission shall be formalised within 24 hours as of the commencement of surveillance activities.</p> <p>(4) A permission issued in cases of urgency in a format which can be reproduced in writing shall contain the following information:</p> <ol style="list-style-type: none"> 1) the issue of the permission; 2) the date and time of issue of the permission; 3) surveillance activities for which the permission is issued; 4) if known, the name of the person with regard to whom the surveillance activities are conducted; 5) the term of the permission for surveillance activities. <p>(5) If covert entry into a building, premises, vehicle, enclosed area or computer system is necessary for conduct of surveillance activities or in order to install or remove technical appliances necessary for surveillance, the Prosecutor's Office shall apply for a separate permission of a preliminary investigation judge for such purpose.</p> <p>(6) The duration of surveillance activities conducted with respect to a specific person on the basis provided for in clauses 126² (1) 1), 3) and 4) of this Code in the same proceedings must not exceed one year. In exceptional cases, the Prosecutor General may authorise or apply to a court for authorisation to conduct surveillance activities for more than one year. In a criminal case dealt with under Council Regulation (EU) 2017/1939, the relevant authorization is granted, or application made, by a European Prosecutor or a European Delegated Prosecutor.</p> <p>3. Office of the Prosecutor General</p>
DK or IE as issuing state	<p>1. MLA 2000 Art 20</p> <p>2. General conditions stipulated in the CCP § 126¹ – 126⁴</p> <p>3. Central authority is Ministry of Justice, Office of the Prosecutor General in charge of the execution</p>
Issuing state is a third State	<p>See DK or IE</p>

Bugging of a car	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. See replies to question a.) 2. 3.
DK or IE as issuing state	<ol style="list-style-type: none"> 1. See replies to question a.) 2. 3.
Issuing state is a third State	<ol style="list-style-type: none"> 1. See replies to question a.) 2. 3.
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Yes. 2. § 126⁴ (5) <i>If covert entry into a building, premises, vehicle, enclosed area or computer system is necessary for conduct of surveillance activities or in order to install or remove technical appliances necessary for surveillance, the Prosecutor's Office shall apply for a separate permission of a preliminary investigation judge for such purpose.</i> (See also general conditions stipulated in CCP § 1261, § 1262, § 1264 (question a)) 3. – 4. Annex C 5. Office of the Prosecutor General
DK or IE as issuing state	<ol style="list-style-type: none"> 1. Yes 2. CCP § 126⁴ (5) 3. – 4. Art 20 of the 2000 MLA Convention 5. Ministry of Justice
Issuing state is a third State	See DK or IE
Audio/video surveillance in a private place	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Yes 2. . Annex A. <p>General conditions - see replies to the question a)). Maximum duration is one year, in exceptional cases more than one year. A preliminary investigation judge grants permission for the surveillance activities specified in this section for up to two months. After expiry of</p>

	<p>the specified term, the preliminary investigation judge may extent this term by up to two months.</p> <p>Competent authority to execute the request is Office of the Prosecutor General.</p> <p>3. -</p>
DK or IE as issuing state	<p>1. Yes</p> <p>2. MLA 2000 Art 18.</p> <p>General conditions - see replies to the question a)). Maximum duration is one year, in exceptional cases more than one year. A preliminary investigation judge grants permission for the surveillance activities specified in this section for up to two months. After expiry of the specified term, the preliminary investigation judge may extent this term by up to two months.</p> <p>3. -</p>
Issuing state is a third State	See DK or IE
Interception of telecommunication abroad	
Issuing state applies EIO DIR	<p>1. Annex A.</p> <p>For general conditions, list of crimes see reply to the question a). Maximum duration is one year, in exceptional cases more than one year. A preliminary investigation judge grants permission for the surveillance activities specified in this section for up to two months. After expiry of the specified term, the preliminary investigation judge may extent this term by up to two months.</p> <p>2. Office of the Prosecutor General</p> <p>3. No.</p>
DK or IE as issuing state	<p>1. MLA 2000 Art 18.</p> <p>For general conditions, list of crimes see reply to the question a). Maximum duration is one year, in exceptional cases more than one year. A preliminary investigation judge grants permission for the surveillance activities specified in this section for up to two months. After expiry of the specified term, the preliminary investigation judge may extent this term by up to two months.</p> <p>2. Central authority is Ministry of Justice, Office of the Prosecutor General in charge</p> <p>3. No.</p>
Issuing state is a third State	See DK or IE
Scope of Article 31 EIO Directive and use of Annex C	
<p>1. -</p> <p>2. -</p> <p>3. -</p>	

4.1.9. Finland (FI)

FINLAND 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Annex C EIO Directive; Other: Schengen Art 40 (need to contain all the necessary information and specially in urgent cases) 2. Chapter 10 Section 21 Finnish Coercive Measures Act (FCMA): A criminal investigation authority may direct technical monitoring at an object, substance or property that is the object of an offence or presumably in the possession of the suspect, when there is reason to suspect the person of an offence for which the most severe punishment provided is imprisonment for at least one year. 3. National Bureau of Investigation is the competent authority to be contacted by an issuing state. <p>Chapter 10 Section 22 (2) FCMA: An official with the power of arrest (prosecutor and head of investigation, LEA) decides on technical monitoring of other than individuals.</p> <p>A warrant may be issued and a decision made for at the most one month at a time.</p>
DK or IE as issuing state	<ol style="list-style-type: none"> 1. LoR and Notification in accordance with Art 20 of the 2000 MLA Convention 2. As above 3. As above
Issuing state is a third State	<ol style="list-style-type: none"> 1. LoR 2. As above 3. As above <p>- Finland applies the Mutual Legal Assistance Agreement between the European Union and the United States of America signed on 25 June 2003 and there are a few other bilateral agreements (But do not contain specific rules for the situations covered by the questionnaire – concerns all sections a, b, c, d, e)</p>
Bugging of a car	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Annex A EIO Directive 2. Chapter 10 Section 16 FCMA – On-site interception and its prerequisites <ol style="list-style-type: none"> (1) On-site interception refers to the listening, recording and other processing with a technical device, procedure or program. (2) A criminal investigation authority may direct on-site interception at a suspect in an offence outside of premises used as a permanent residence. The interception may be conducted by directing it at premises or at another place where the suspect can be presumed to be or visit. (3) An additional prerequisite for on-site interception is that there are grounds to suspect the subject of the interception of: <ol style="list-style-type: none"> (1) an offence for which the most severe punishment provided is imprisonment for at least four years; (2) a narcotics offence;

	<p>(3) preparation of an offence committed with terrorist intent;</p> <p>(4) an aggravated customs offence;</p> <p>(5) preparation of the taking of a hostage; or</p> <p>(6) preparation of aggravated robbery.</p> <p><i>Section 18 – Decision on on-site interception</i></p> <p>(1) The court decides on on-site interception in domestic premises and on onsite interception directed at a person who has lost his or her liberty as a result of an offence.</p> <p>(2) An official with the power of arrest (prosecutor and head of investigation, LEA) decides on on-site interception other than that referred to in subsection 1.</p> <p>(3) A warrant may be issued and a decision made for at the most one month at a time.</p> <p>3. National Bureau of Investigation is the competent authority to be contacted by an issuing state</p>
DK or IE as issuing state	<p>1. LoR</p> <p>2. As above</p> <p>3. As above</p>
Issuing state is a third State	<p>1. LoR</p> <p>2. As above</p> <p>3. As above</p>
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	<p>1. Yes.</p> <p>2. According to Finnish legislation, it is possible to use malware or “Trojan Horse”. This is, in principle, a matter of technical surveillance. The scope of technical surveillance also includes e.g. listening to calls if the communication is initiated by the phone holder himself. The same goes for other communications.</p> <p><i>Chapter 10 Section 26 (1) FCMA A criminal investigation official has the right to install a device, procedure or program to be used in technical surveillance in the object, substance, property, premises or other place that is targeted, or into an information system, if the performance of the surveillance requires this. In so doing the criminal investigation official has the right, in order to install, take into use or remove a device, procedure or program, to enter covertly the premises or other place or information system referred to above and to bypass, uninstall or in another corresponding manner temporarily avert or hamper the protection on the objects or the information system. Separate provisions apply to search of a domicile.</i></p> <p>(2) A device, procedure or program for technical surveillance may be installed in premises used as a permanent residence only if the court has granted a warrant for this on the request of an official with the power of arrest.</p> <p>3. -</p> <p>4. Annex A - EIO</p> <p>5. (Section 24) (1) FCMA The court decides on technical surveillance of a device at the request of a head of investigation or prosecutor. If the matter does not brook delay, an official with the power of arrest (police officer or prosecutor) may decide on technical surveillance of a device until such time as the court has decided on the request for the issuing of the warrant. The matter</p>


	<p><i>shall be submitted for the decision of the court as soon as possible, but at the latest within 24 hours of the initiation of the use of the coercive measure.</i></p> <p><i>(2) The warrant may be issued for at most one month at a time.</i></p>
DK or IE as issuing state	<ol style="list-style-type: none"> 1. As above 2. As above 3. As above 4. LoR 5. As above
Issuing state is a third State	<ol style="list-style-type: none"> 1. As above 2. As above 3. As above 4. LoR 5. As above
Audio/video surveillance in a private place	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Yes, audio surveillance is possible, but video surveillance is not 2. <i>(Section 17) FCMA A criminal investigation authority may be granted permission to direct on-site interception at premises used as a permanent residence and in which a person suspected in an offence is presumed to reside (on-site interception in domestic premises). A further prerequisite is that there are grounds to suspect him or her of:</i> <ol style="list-style-type: none"> <i>(1) genocide, preparation of genocide, a crime against humanity, an aggravated crime against humanity, a war crime, an aggravated war crime, torture, violation of a prohibition against chemical weapons, violation of a prohibition against biological weapons, violation of a prohibition against anti-infantry mines; (468/2011)</i> <i>(2) endangerment of the sovereignty of Finland, incitement to war, treason, aggravated treason, espionage, aggravated espionage;</i> <i>(3) high treason, aggravated high treason;</i> <i>(4) aggravated sexual abuse of a child;</i> <i>(5) manslaughter, murder, killing;</i> <i>(6) aggravated trafficking in persons;</i> <i>(7) aggravated robbery;</i> <i>(8) aggravated sabotage, aggravated endangerment of health, a nuclear device offence, hijacking;</i> <i>(9) an offence committed with terrorist intent, preparation of an offence committed with terrorist intent, directing of a terrorist group, promotion of the activity of a terrorist group, provision of training for the commission of a terrorist offence, recruitment for the commission of a terrorist offence, financing of terrorism, as referred to in Chapter 34(a), section 1, subsection 1, paragraphs 2-7 or subsection 2 of the Criminal Code;</i> <i>(10) an aggravated narcotics offence.</i> <p>National Bureau of Investigation is the competent authority to be contacted by an issuing state.</p>

	<p><i>Section 18 (1) FCMA The court decides on on-site interception in domestic premises and on onsite interception directed at a person who has lost his or her liberty as a result of an offence, on the request of an official with the power of arrest.</i></p> <p><i>(2) An official with the power of arrest decides on on-site interception other than that referred to in subsection 1.</i></p> <p><i>(3) A warrant may be issued and a decision made for at the most one month at a time.</i></p> <p>3. -</p>
DK or IE as issuing state	<p>1. As above</p> <p>2. As above</p> <p>3. As above</p>
Issuing state is a third State	<p>1. As above</p> <p>2. As above</p> <p>3. As above</p>
Interception of telecommunication abroad	
Issuing state applies EIO DIR	<p>1.The same as for domestic coercive measures.</p> <p>According to FCMA Chapter 10 Section 3 and 5</p> <p><i>Section 3 – Telecommunications interception and its prerequisites</i></p> <p><i>(1) Telecommunications interception refers to the monitoring, recording and other processing of a message sent to or transmitted from a network address or terminal end device through a public communications network referred to in the Telecommunications Services Act or a communications network connected thereto, in order to determine the contents of the message and the identifying data connected to it referred to in section 6. Telecommunications interception may be directed only at a message that originates from or is intended for a suspect in an offence.</i></p> <p><i>(2) A criminal investigation authority may receive permission for telecommunications interception directed at a network address or terminal end device in the possession of or otherwise presumably used by a suspect in an offence, when there are grounds to suspect him or her of:</i></p> <p><i>(1) genocide, preparation of genocide, a crime against humanity, an aggravated crime against humanity, a war crime, an aggravated war crime, torture, violation of a prohibition against chemical weapons, violation of a prohibition against biological weapons, violation against a prohibition against anti-infantry mines; (1468/2011)</i></p> <p><i>(2) endangerment of the sovereignty of Finland, incitement to war, treason, aggravated treason, espionage, aggravated espionage, disclosure of a national secret, unlawful gathering of intelligence;</i></p> <p><i>(3) high treason, aggravated high treason, preparation of high treason;</i></p> <p><i>(4) aggravated distribution of a sexually offensive picture depicting a child;</i></p> <p><i>(5) sexual abuse of a child, aggravated sexual abuse of a child;</i></p> <p><i>(6) manslaughter, murder, homicide, preparation of an aggravated offence directed against life or health as referred to in Chapter 21, section 6a of the Criminal Code and in accordance with sections 1, 2 and 3 of said Chapter; (438/2013)</i></p>

	<p>(7) arrangement of aggravated illegal entry into the country, aggravated deprivation of liberty, trafficking in persons, aggravated trafficking in persons, kidnapping, preparation of kidnapping; (438/2013)</p> <p>(8) aggravated robbery, preparation of aggravated robbery, aggravated extortion; (438/2013)</p> <p>(9) aggravated concealment of illegally obtained goods, professional concealment of illegally obtained goods, aggravated money laundering;</p> <p>(10) criminal mischief, criminal traffic mischief, aggravated sabotage, aggravated endangerment of health, a nuclear device offence, hijacking;</p> <p>(11) an offence committed with terrorist intent, preparation of an offence committed with terrorist intent, directing of a terrorist group, promotion of the activity of a terrorist group, provision of training for the commission of a terrorist offence, recruitment for the commission of a terrorist offence, financing of terrorism, as referred to in Chapter 34(a), section 1, subsection 1, paragraphs 2-7 or subsection 2 of the Criminal Code;</p> <p>(12) aggravated damage to property;</p> <p>(13) aggravated fraud, aggravated usury;</p> <p>(14) aggravated counterfeiting;</p> <p>(15) aggravated impairment of the environment; or</p> <p>(16) an aggravated narcotics offence. (1146/2013)</p> <p>(3) A warrant for telecommunications interception may be issued also when there are grounds to suspect a person of the following in connection with commercial or professional activity:</p> <p>(1) aggravated giving of a bribe;</p> <p>(2) aggravated embezzlement;</p> <p>(3) aggravated tax fraud, aggravated assistance fraud;</p> <p>(4) aggravated forgery;</p> <p>(5) aggravated dishonesty by a debtor, aggravated dishonesty by a debtor;</p> <p>(6) aggravated taking of a bribe, aggravated abuse of public office;</p> <p>(7) aggravated regulation offence;</p> <p>(8) aggravated abuse of insider information, aggravated market price distortion; or</p> <p>(9) an aggravated customs offence.</p> <p>(4) An additional prerequisite to the issuing of the warrant referred to above in subsection 3 is that the offence was committed in order to obtain especially large benefit and the offence has been committed in an especially methodical manner.</p> <p>(5) A warrant for telecommunications interception may also be issued if there are grounds to suspect someone of aggravated pandering in which especially large benefit is sought and the offence has been committed in an especially methodical manner or the offence is one referred to in Chapter 20, section 9a, subsection 1, paragraph 3 or 4 of the Criminal Code.</p> <p>Section 5 – The decision on telecommunications interception and on other corresponding obtaining of information</p> <p>(1) The court decides on telecommunications interception and on the obtaining of information referred to in section 4 on the request of an official with the power of arrest.</p> <p>(2) The warrant for telecommunications interception and for obtaining the information referred to in section 4, subsection 2 may be given for at most one month at a time. (1146/2013)</p> <p>(3) The request and warrant for telecommunications interception and for the obtaining of information as an alternative to telecommunications interception shall specify:</p>
--	---


	<p>(1) the suspected offence and the time of its commission;</p> <p>(2) the person suspected in the offence;</p> <p>(3) the facts on the basis of which the person is suspected of an offence and which fulfil the prerequisites for telecommunications interception or for the obtaining of information as an alternative to telecommunications interception;</p> <p>(4) the validity of the warrant for telecommunications interception or for the obtaining of the information referred to in section 4, subsection 2, including the exact time;</p> <p>(5) the network address or terminal end device that is the object of the measure;</p> <p>(6) the official with the power of arrest who is directing and supervising the performance of the telecommunications interception or of the obtaining of information as an alternative to telecommunications interception;</p> <p>(7) possible restrictions on and conditions for the telecommunications interception or the obtaining of information as an alternative to telecommunications interception. (1146/2013)</p> <p>2. National Bureau of Investigation is the competent authority to be contacted by an issuing state.</p> <p>3. It depends at on the target company, the requesting country, the amount and quality of the data. The provision of real-time data has never been done.</p> <p>Technically it is possible. However, this requires a separate connection to be built between the telecommunications interception systems of the requesting country and the implementing country, and also need to ensure that the target and content are in accordance with the warrant.</p>
DK or IE as issuing state	<p>1. As above</p> <p>2. -- // --</p> <p>3. -- // --</p>
Issuing state is a third State	<p>1. As above</p> <p>2. -- // --</p> <p>3. -- // --</p>
Scope of Article 31 EIO Directive and use of Annex C	
<p>1. No</p> <p>2. National Bureau of Investigation is the competent authority to be contacted by an issuing state.</p> <p>3. English, Swedish and Finnish are always accepted.</p>	

4.1.10. France (FR)

FRANCE 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Bugging of a car	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	

Audio/video surveillance in a private place	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Interception of telecommunication abroad	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Scope of Article 31 EIO Directive and use of Annex C	
Relevant documents	

4.1.11. Germany (DE)

<div>GERMANY</div> 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	<p>1. Annex A EIO Directive</p> <p>2. Section 91c paragraph 2, 59 paragraph 3 Act on International Mutual Assistance in Criminal Matters (IRG; please find English version here: https://www.gesetze-im-internet.de/englisch_irg/index.html) → According to Section 100h Paragraph 1 Sentence 1 Number 2 German Criminal Code of Procedure (GCCP; please find English version here: https://www.gesetze-im-internet.de/englisch_stpo/index.html):</p> <ul style="list-style-type: none"> - initial suspicion of offence of substantial significance, - other means of establishing the facts or determining an accused's whereabouts would offer less prospect of success or would be more difficult, - only admissible against the suspect; these measures can only be directed against a third person if it is to be assumed, on the basis of certain facts, that they are in contact with an accused person or that such contact will be established; - in case of a longer-term observation (meaning an observation that lasts for a continuous period exceeding 24 hours or takes place on more than two days, section 163f paragraph 1 sentence 1 GCCP): a court order has to be issued before implementing the measures on German territory unless the crossing of the border happens unexpectedly and suddenly. - <u>Ex-post authorisation</u>: depending on the Federal State and individual PPO as this is not explicitly regulated; Exemption: Article 19 Section 4 of the German-Czech Supplementary Treaty to EU Convention of 2.2.2000 as amended by the Amendment Treaty of 28.4.2016 allows explicitly an ex-post-notification. <p>3. In general, these measures can be issued by court, PPO or police. In case of a longer-term observation, these measures can only be issued by court; in exigent circumstances also by the PPO and its investigators.</p>
DK or IE as issuing state	<p>1. LoR</p> <p>2. Same as under "Issuing state applies EIO DIR" => paragraph 77 IRG subsection 1 refers to the GCCP</p> <p>3. Same as under "Issuing state applies EIO DIR" => paragraph 77 IRG subsection 1 refers to the GCCP</p>
Issuing state is a third State	<p>1. LoR</p> <p>2. Same as under "Issuing state applies EIO DIR" => paragraph 77 IRG subsection 1 refers to the GCCP</p> <p>3. Same as under "Issuing state applies EIO DIR" => paragraph 77 IRG subsection 1 refers to the GCCP; depending on the third state, the request might need to be directed to a superior authority first; kindly refer to the country section of the Administrative Rules for the International Cooperation in Criminal Matters (RiVAST) and the bilateral agreements mentioned there: https://www.bmj.de/</p>
Bugging of a car	

Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Annex A EIO Directive 2. Section 91c paragraph 2, 59 paragraph 3 Act on International Mutual Assistance in Criminal Matters => According to section 100f paragraph 1 and 2 GCCP: <ul style="list-style-type: none"> - (qualified) initial suspicion of a crime (referring to the catalogue of serious offences of section 100a paragraph 2 GCCP), - other means of establishing the facts or determining the accused's whereabouts would offer no prospect of success or would be much more difficult - admissible against the suspect; these measures can only be directed against a third person if it is to be assumed, on the basis of certain facts, that they are in contact with an accused person or that such contact will be established, - (no further requirements in Police Conventions) - Ex-post authorisation: case-by-case decision depending on Federal State and individual PPO because not explicitly regulated; in case PPO considers it to be possible: court order is required; some PPO consider it necessary to obtain a court order within three days. 3. in general: court order is required (section 100f paragraph 4, section 100e paragraph 1 sentence 1 GCCP); in urgent cases: can be ordered by PPO, but it has to be confirmed within three days by the competent court (section 100f paragraph 4, section 100e paragraph 1 sentence 2 GCCP).
DK or IE as issuing state	<ol style="list-style-type: none"> 1. LoR 2. Same as under "Issuing state applies EIO DIR" => paragraph 77 IRG subsection 1 refers to the GCCP 3. Same as under "Issuing state applies EIO DIR" => paragraph 77 IRG subsection 1 refers to the GCCP
Issuing state is a third State	<ol style="list-style-type: none"> 1. LoR 2. Same as under "Issuing state applies EIO DIR" => paragraph 77 IRG subsection 1 refers to the GCCP. 3. Same as under "Issuing state applies EIO DIR" => paragraph 77 IRG subsection 1 refers to the GCCP; depending on the third state the request might need to be directed to a superior authority first; kindly refer to the country section of the Administrative Rules for the International Cooperation in Criminal Matters (RiVAST) and the bilateral agreements mentioned there: https://www.bmj.de/
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Yes but according to the <u>prevailing view in legal literature</u> it is not possible to use Trojan horse software in order to collect data by means of controlling the microphone and/or the camera of an electronic device. 2. a) According to section 100a sentence 2 GCCP telecommunications may also be intercepted and recorded in such a manner that technical means are used to interfere with the information technology systems used by the person concerned if this is necessary to enable interception and recording in unencrypted form in particular. Conditions: <ul style="list-style-type: none"> - (qualified) initial suspicion of a crime (referring to the catalogue of serious offences of section 100a paragraph 2 GCCP) which is also of particular severity in the individual case,

	<ul style="list-style-type: none"> - other means of establishing the facts or determining the accused's whereabouts would be much more difficult or would offer no prospect of success, - the measures may be directed against the suspect or against persons that receive or transmit messages intended for or originating from the suspect or the suspect uses their telephone connection or information technology system, - maximum duration of three months (Section 100e Paragraph 1 Sentence 4 GCCP); possibility of prolongation for further three months (more than once; principle of proportionality). - urgent cases: such as imminent danger of loss of evidence; <p>b) According to section 100b GCCP technical means may be used even without the knowledge of the person concerned to gain covert access to an information technology system used by the person concerned and to extract data from that system ('covert remote search of information technology systems'). Conditions:</p> <ul style="list-style-type: none"> - (qualified) initial suspicion of a crime (referring to the catalogue of serious offences of section 100b paragraph 2 GCCP) which is also of particular severity in the individual case, - other means of establishing the facts or determining the accused's whereabouts would be significantly more difficult or offer no prospect of success, - admissible against the suspect; interference with the information technology systems of other persons is only permissible if the accused uses the other person's information technology systems and the interference with the accused's information technology systems alone will not lead to the establishment of the facts or to the determination of the whereabouts of a co-accused, - inadmissible in case the measures would only lead to findings in the core area of the private conduct of life, - Inadmissible against persons that have the right to refuse testimony on professional grounds according to section 53 GCCP. - order is limited to a maximum duration of one month, can be extended by the regional court for up to six months. If the duration of the order has been extended for a total period of six months, the higher regional court has to decide about any further extension orders. <p>3. ---</p> <p>4. Annex A</p> <p>5.</p> <p>a) According to section 100a sentence 2 GCCP: in general court order is required (Section 100e Paragraph 1 Sentence 1 GCCP); in urgent cases: can be ordered by PPO, but it has to be confirmed within three days by the competent court (Section 100e Paragraph 1 Sentence 2 GCCP).</p> <p>b) According to section 100b GCCP these measures may only be ordered by a special division of the regional court stipulated in section 74a Paragraph 4 of the Courts Constitution Act in the district in which the public prosecution office is located. In exigent circumstances, the order may be made by the presiding judge which becomes ineffective unless it is confirmed by the criminal division within three working days.</p>
DK or IE as issuing state	<p>1. Same as under "Issuing state applies EIO DIR" => paragraph 77 IRG subsection 1 refers to the GCCP</p> <p>2. Same as under "Issuing state applies EIO DIR" => paragraph 77 IRG subsection 1 refers to the GCCP.</p>


	<p>3. ---</p> <p>4. LoR</p> <p>5. Same as under “Issuing state applies EIO DIR” => paragraph 77 IRG subsection 1 refers to the GCCP.</p>
Issuing state is a third State	<p>1. Same as under “Issuing state applies EIO DIR” => paragraph 77 IRG subsection 1 refers to the GCCP.</p> <p>2. See above (paragraph 77 IRG subsection 1 refers to the GCCP).</p> <p>3. ---</p> <p>4. LoR</p> <p>5. Same as under “Issuing state applies EIO DIR” => paragraph 77 IRG subsection 1 refers to the GCCP; depending on the third state the request might need to be directed to a superior authority first; kindly refer to the country section of the Administrative Rules for the International Cooperation in Criminal Matters (RiVAST) and the bilateral agreements mentioned there: https://www.bmj.de/</p>
Audio/video surveillance in a private place	
Issuing state applies EIO DIR	<p>1. Yes, but only audio surveillance.</p> <p>2. According to section 100c GCCP:</p> <ul style="list-style-type: none"> - (qualified) initial suspicion of a crime (referring to the catalogue of serious offences of section 100b paragraph 2 GCCP) which is also of particular severity in the individual case, - it is assumed that the surveillance will result in the recording of statements by the accused which would be of significance in establishing the facts or determining the whereabouts of a co-accused, - other means of establishing the facts or determining a co-accused’s whereabouts would be disproportionately more difficult or would offer no prospect of success, - the measures may be directed against the suspect on his private premises or the private premises of other persons if the suspect is present on those premises and applying the measure on the accused’s premises alone will not lead to the establishment of the facts or to the determination of a co-accused person’s whereabouts; - inadmissible in case the measures would only lead to findings in the core area of the private conduct of life, - inadmissible against persons that have the right to refuse testimony on professional grounds according to section 53 GCCP. - Competent authority: These measures may only be ordered by a special division of the regional court stipulated in section 74a Paragraph 4 of the Courts Constitution Act in the district in which the public prosecution office is located. In exigent circumstances, the order may be made by the presiding judge which becomes ineffective unless it is confirmed by the criminal division within three working days (section 100e paragraph 2 GCCP). <p>Furthermore, the order is limited to a maximum duration of one month, can be extended by the regional court for up to six months. If the duration of the order has been extended for a total period of six months, the higher regional court has to decide about any further extension orders.</p> <p>3. ---</p>

DK or IE as issuing state	<p>1. Yes, but only audio surveillance.</p> <p>2. Same as under “Issuing state applies EIO DIR” => paragraph 77 IRG subsection 1 refers to the GCCP.</p> <p>3. ---</p>
Issuing state is a third State	<p>1. Yes, but only audio surveillance.</p> <p>2. Same as under “Issuing state applies EIO DIR” => paragraph 77 IRG subsection 1 refers to the GCCP; depending on the third state the request might need to be directed to a superior authority first; kindly refer to the country section of the Administrative Rules for the International Cooperation in Criminal Matters (RiVAST) and the bilateral agreements mentioned there: https://www.bmj.de/</p> <p>3. ---</p>
Interception of telecommunication abroad	
Issuing state applies EIO DIR	<p>1. According to section 100a GCCP:</p> <ul style="list-style-type: none"> - (qualified) initial suspicion of a crime (referring to the catalogue of serious offences of section 100a paragraph 2 GCCP) which is also of particular severity in the individual case, - other means of establishing the facts or determining the accused’s whereabouts would be much more difficult or would offer no prospect of success, - the measures may be directed against the suspect or against persons that receive or transmit messages intended for or originating from the suspect or the suspect uses their telephone connection or information technology system, - maximum duration of three months (Section 100e Paragraph 1 Sentence 4 GCCP); possibility of prolongation for further three months (more than once; principle of proportionality). - urgent cases: such as imminent danger of loss of evidence; <p>2. in general: court order is required (Section 100e Paragraph 1 Sentence 1 GCCP); in urgent cases: can be ordered by PPO, but it has to be confirmed within three days by the competent court (Section 100e Paragraph 1 Sentence 2 GCCP)</p> <p>3. Yes</p>
DK or IE as issuing state	<p>1. Same as under “Issuing state applies EIO DIR” => paragraph 77 IRG subsection 1 refers to the GCCP</p> <p>2. Same as under “Issuing state applies EIO DIR” => paragraph 77 IRG subsection 1 refers to the GCCP.</p> <p>3. Yes.</p>
Issuing state is a third State	<p>1. LoR</p> <p>2. See above (paragraph 77 IRG subsection 1 refers to the GCCP); Depending on the third state; depending on the third state the request might need to be directed to a superior authority first; kindly refer to the country section of the Administrative Rules for the International Cooperation in Criminal Matters (IRG) and the bilateral agreements mentioned there: https://www.bmj.de/</p> <p>3. Yes.</p>

Scope of Article 31 EIO Directive and use of Annex C

1. No.
2. According to section 92d of the Act on International Mutual Assistance in Criminal Matters, the competency of the respective PPO depends on the issuing state (e. g. incoming request from Italy => PPO München I).
3. German, in urgent cases it is possible to ask the competent PPO whether they accept English.


4.1.12. Greece (EL)

GREECE 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Annex C EIO DIR 2. The removal of the privilege of telecommunications is allowed for the specific crimes described in art. 4 of Act 2225/1994. 3. The Public Prosecutor of Appeals
DK or IE as issuing state	<ol style="list-style-type: none"> 1. An MLA request will be needed. 2. Such an MLA request shall be executed according to the European Convention on Mutual Assistance in Criminal Matters is a 1959 and under the conditions designated in art. 4 of Act 2225/1994. 3. The MoJ.
Issuing state is a third State	<ol style="list-style-type: none"> 1. An MLA request will be needed. 2. Such an MLA request shall be executed according to the European Convention on Mutual Assistance in Criminal Matters is a 1959 and under the conditions designated in art. 4 of Act 2225/1994. As for the USA, such a request may be executed under the MLA Convention in criminal cases between Greece and the USA of 26 May 1999 and under the conditions designated in art. 4 of Act 2225/1994. 3. The MoJ.
Bugging of a car	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Annex C EIO DIR 2. The removal of the privilege of telecommunications is allowed for the specific crimes described in art. 4 of Act 2225/1994. 3. The Public Prosecutor of Appeals
DK or IE as issuing state	<ol style="list-style-type: none"> 1. An MLA request will be needed. 2. Such an MLA request shall be executed according to the European Convention on Mutual Assistance in Criminal Matters is a 1959 and under the conditions designated in art. 4 of Act 2225/1994. 3. The MoJ.
Issuing state is a third State	<ol style="list-style-type: none"> 1. An MLA request will be needed. 2. Such an MLA request shall be executed according to the European Convention on Mutual Assistance in Criminal Matters is a 1959 and under the conditions designated in art. 4 of Act 2225/1994. As for the USA, such a request may be executed under the MLA Convention in criminal cases between Greece and the USA of 26 May 1999 and under the conditions designated in art. 4 of Act 2225/1994. 3. The MoJ.

Surveillance through Trojan horse software	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. No 2. N/A 3. N/A 4. N/A 5. N/A
DK or IE as issuing state	<ol style="list-style-type: none"> 1. No 2. N/A 3. N/A 4. N/A 5. N/A
Issuing state is a third State	<ol style="list-style-type: none"> 1. No 2. N/A 3. N/A 4. N/A 5. N/A
Audio/video surveillance in a private place	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. No 2. 3. N/A
DK or IE as issuing state	<ol style="list-style-type: none"> 1. No 2. 3. N/A
Issuing state is a third State	<ol style="list-style-type: none"> 1. No 2. 3. N/A
Interception of telecommunication abroad	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Telecommunications interception is justified mainly for organised crime, drug trafficking, corruption crimes, homicide, serious bodily harm and sexual crimes, smuggling, it is ordered by the competent judicial council and lasts for 2 months; it can be renewed, but not for time exceeding 10 months in total. 2. The Public Prosecutor of Appeals. 3. N/A

DK or IE as issuing state	<p>1. Telecommunications interception is justified mainly for organised crime, drug trafficking, corruption crimes, homicide, serious bodily harm and sexual crimes, smuggling, it is ordered by the competent judicial council and lasts for 2 months; it can be renewed, but not for time exceeding 10 months in total.</p> <p>2. The MoJ.</p> <p>3. N/A</p>
Issuing state is a third State	<p>1. Telecommunications interception is justified mainly for organised crime, drug trafficking, corruption crimes, homicide, serious bodily harm and sexual crimes, smuggling, it is ordered by the competent judicial council and lasts for 2 months; it can be renewed, but not for time exceeding 10 months in total.</p> <p>2. The MoJ.</p> <p>3. N/A</p>
Scope of Article 31 EIO Directive and use of Annex C	
<p>1. N/A</p> <p>2. The Public Prosecutor of Appeals</p> <p>3. Greek or English</p>	

4.1.13. Hungary (HU)


HUNGARY 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Annex C EIO DIR 2. Utilising GPS tracking shall be carried out in the framework of a discreet surveillance, which is a covert investigation tool legislated under Section 215 Subsection (5) of Act XC of 2017 on Criminal Proceedings Code (HU CoCP). Judicial or prosecutorial authorisation is not required and it may be performed in investigations conducted into any crimes. General rules on covert investigation tools apply: utilisation of these tools can take place if <ul style="list-style-type: none"> - it is reasonably assumed that the information or evidence to be obtained is essential to achieve the goal of the criminal proceedings and it cannot be obtained by any other means - the utilisation of the covert investigation tool does not lead to the disproportional restriction of fundamental rights of the concerned person or other person, , in relation to the law enforcement goal to be achieved, - by utilisation of the covert investigation tool the acquisition of information or evidence relating to a crime is probable. 3. Metropolitan Chief Prosecutor's Office.
DK or IE as issuing state	<ol style="list-style-type: none"> 1. Notification in accordance with Art 20 of the 2000 MLA Convention 2. Same rules as above 3. Metropolitan Chief Prosecutor's Office
Issuing state is a third State	<ol style="list-style-type: none"> 1. MLA request 2. Same rules as above 3. Competent County Chief PPO or the Metropolitan Chief PPO under the provisions on jurisdiction of HU CoCP; Metropolitan Chief PPO in case the jurisdiction cannot be established
Bugging of a car	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Annex C EIO DIR 2. Bugging of a car shall be carried out in the framework of a secret surveillance of premises, which is a covert investigation tool legislated under Section 232 Subsection (3) of HU CoCP. It can be utilised, with the exclusion of places open to the public, in private homes or other premises, fenced or encircled areas and, with the exclusion of means of public transport, in vehicles. Judicial authorization is required. Besides general rules on covert investigation tools [see point a)], provisions regarding covert investigation tools requiring judicial authorization apply: utilisation of these tools can take place if the crime into which the investigation is conducted is <ul style="list-style-type: none"> - punishable by a maximum of 5 years imprisonment or more - punishable by a maximum of 3 years imprisonment, provided that the crime is intentionally committed and constitute one or more the below offences <ul style="list-style-type: none"> • crimes committed at commercial scale or within a criminal association

	<ul style="list-style-type: none"> • abuse of drug precursors, counterfeiting medicines, abuse of performance-enhancing substances, counterfeiting of sanitary articles • sexual abuse, recruitment to prostitution, facilitation of prostitution, exploitation of prostitution, exploitation of child prostitution, child pornography • violation of environment, violation of nature, poaching, organization of animal fights, infringement of waste management • crimes against justice (excluding breach of seal) • corruption crimes (excluding omission of reporting a corruption crime) • crime against elections, referenda or European citizens' initiative, unlawful employment of a third-country national, organization of illegal gambling • insider dealing, market manipulation <p>-abuse of classified data, abuse of official position, violence against a representative of a public authority, violence against an internationally protected person, counterfeiting of non-cash means of payments, unlicensed financial activity, organization of pyramid schemes.</p> <p>3. Metropolitan Chief Prosecutor's Office</p>
DK or IE as issuing state	<p>1. Notification in accordance with Art 20 of the 2000 MLA Convention</p> <p>2. Same rules as above</p> <p>3. Metropolitan Chief Prosecutor's Office</p>
Issuing state is a third State	<p>1. MLA request</p> <p>2. Same rules as above</p> <p>3. Competent County Chief PPO or the Metropolitan Chief PPO under the provisions on jurisdiction of HU CoCP; Metropolitan Chief PPO in case the jurisdiction cannot be established</p>
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	<p>1. Yes</p> <p>2. Surveillance through Trojan horse shall be carried out in the framework of a secret surveillance of information systems, which is a covert investigation tool legislated under Section 232 Subsection (1) of HU CoCP. The portable electronic device on which the Trojan software installed can be placed, with the exclusion of places open to the public, in private homes or other premises, fenced or encircled areas and, with the exclusion of means of public transport, in vehicles as well as in the device used by the concerned person. Judicial authorization is required.</p> <p>The conditions for this measure are the same as those applicable to secret surveillance of premises [see at point b)].</p> <p>3.</p> <p>4. Annex C</p> <p>5. Metropolitan Chief Prosecutor's Office</p>
DK or IE as issuing state	<p>1. Yes</p> <p>2. Same rules as above</p> <p>3.</p> <p>4. Notification in accordance with Art 20 of the 2000 MLA Convention</p> <p>5. Metropolitan Chief Prosecutor's Office</p>

Issuing state is a third State	<ol style="list-style-type: none"> 1. Yes 2. Same rules as above 3. 4. MLA request 5. Competent County Chief PPO or the Metropolitan Chief PPO under the provisions on jurisdiction of HU CoCP; Metropolitan Chief PPO in case the jurisdiction cannot be established
Audio/video surveillance in a private place	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Yes 2. Audio/video surveillance in a private place shall be carried out in the framework of secret surveillance of premises, which is a covert investigation tool legislated under Section 232 Subsection (3) of HU CoCP. It can be utilised, with the exclusion of places open to the public, in private homes or other premises, fenced or encircled areas and, with the exclusion of means of public transport, in vehicles. Judicial authorization is required. <p>The conditions for this measure are the same as those applicable to secret surveillance of premises and secret surveillance of information systems [see at point b) and c)].</p> <p>The competent authority is the County Chief PPO or the Metropolitan Chief PPO based on the provisions on jurisdiction of HU CoCP; Metropolitan Chief PPO in case the jurisdiction cannot be established.</p>
DK or IE as issuing state	<ol style="list-style-type: none"> 1. Yes 2. See above. <p>The competent authority is the County Chief PPO or the Metropolitan Chief PPO based on the provisions on jurisdiction of HU CoCP; Metropolitan Chief PPO in case the jurisdiction cannot be established.</p>
Issuing state is a third State	<ol style="list-style-type: none"> 1. Yes 2. See above. <p>The competent authority is the County Chief PPO or the Metropolitan Chief PPO based on the provisions on jurisdiction of HU CoCP; Metropolitan Chief PPO in case the jurisdiction cannot be established.</p>
Interception of telecommunication abroad	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Interception of telecommunication shall be carried out as a covert investigation tool legislated under Section 232 Subsection (5) of HU CoCP. Judicial authorization is required. <p>Conditions are the same as described at point a) (general rules) and point b) (particular rules on covert investigation tools requiring judicial authorization).</p> <p>An interception shall be authorized for a maximum period of 90 days, and it may be prolonged for further 90 days on occasion, as long as the ultimate 360 days of maximum duration is reached. The motion for prolongation shall be submitted 5 days before deadline of expiration at the latest.</p> <p>The interception may be extended to other electronic communications services and information systems. Upon the motion of the prosecutor, the court shall accordingly modify its initial order.</p>


	<p>In case of urgency the prosecutor is entitled to order the interception for a maximum of 120 hours. In this instance, within 72 hours from the prosecutorial order, the prosecutor shall file a motion to the court for subsequently ordering the interception.</p> <p>2. Competent County Chief PPO or the Metropolitan Chief PPO under the provisions on jurisdiction of HU CoCP; Metropolitan Chief PPO in case the jurisdiction cannot be established</p> <p>3. Direct electronic transmission may be possible provided that the issuing state holds a secure communication end-point that is compatible with the system of the HU authority performing the interception and technically recording data. In this regard, prior consultation is necessary in each case.</p>
DK or IE as issuing state	<p>1. See above</p> <p>2. Competent County Chief PPO or the Metropolitan Chief PPO under the provisions on jurisdiction of HU CoCP; Metropolitan Chief PPO in case the jurisdiction cannot be established</p> <p>3. Direct electronic transmission may be possible provided that the issuing state holds a secure communication end-point that is compatible with the system of the HU authority performing the interception and technically recording data. In this regard, prior consultation is necessary in each case.</p>
Issuing state is a third State	<p>1. See above</p> <p>2. Competent County Chief PPO or the Metropolitan Chief PPO under the provisions on jurisdiction of HU CoCP; Metropolitan Chief PPO in case the jurisdiction cannot be established</p> <p>3. Direct electronic transmission may be possible provided that the issuing state holds a secure communication end-point that is compatible with the system of the HU authority performing the interception and technically recording data. In this regard, prior consultation is necessary in each case.</p>
Scope of Article 31 EIO Directive and use of Annex C	
<p>1. No</p> <p>2. Metropolitan Chief Prosecutor's Office</p> <p>3. English, French, German</p>	

4.1.14. Ireland (IE)


IRELAND 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Bugging of a car	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	

Audio/video surveillance in a private place	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Interception of telecommunication abroad	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Scope of Article 31 EIO Directive and use of Annex C	
Relevant documents	


4.1.15. Italy (IT)

ITALY 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	1. None – it can be carried out directly by the other Member State without notifying the Italian authorities 2. none 3. none
DK or IE as issuing state	1. none 2. none 3. none
Issuing state is a third State	1. none 2. none 3. none
Bugging of a car	
Issuing state applies EIO DIR	1. Annex C EIO DIR 2. according to the Italian procedure the bugging of a car is allowed only if the crime investigated is a serious crime ; the list of the crimes is mentioned in art. 266 code of procedure : - any intentional offence punished with a penalty of imprisonment above 5 years in its maximum; - offences against the public administration committed by a public official where the penalty provided is imprisonment for a maximum of at least five years; - drug offences; - offences related to weapons and explosives; - smuggling; - offences of insult, threat, usury, abusive financial activity, insider trading, market abuse or harassment committed by telephone; - other offences (e.g., distribution of pornographic material; stalking; trade in harmful food substances; counterfeiting; trade in counterfeited products; etcetera). 3. territorially competent District Public Prosecutor Office sends immediately the notification to the investigative judge who checks if the crime which the issuing State is investigating on allows , in the domestic procedure , the use of this investigative measure.
DK or IE as issuing state	1. Notification ex art. 20 MLA Convention 2000 2. the conditions are the same of european investigation order as mentioned above 3. the competent Authorities are the same of european investigation order as mentioned above

Issuing state is a third State	1. none 2. none 3. none
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	1. Yes 2. Same as for interception of lett. B (Art. 266 CCP) ; 3. 4. Annex C (no need for technical assistance) or annex A 5. District Public Prosecutor Office and investigative judge territorially competent
DK or IE as issuing state	1. Yes 2. Same as for interception of lett. B (Art. 266 CCP) 3. 4. art. 20 MLA Convention 2000 5. District Public Prosecutor Office and investigative judge territorially competent
Issuing state is a third State	1. Yes 2. Same as for interception of lett. B (Art. 266 CCP) 3. 4. rogatory letter 5. District Public Prosecutor Office and investigative judge territorially competent (according to art. 724 cpp) : "The Public Prosecutor, upon receipt of the documents transmitted by the Minister of Justice or directly by the foreign authority in accordance with international conventions in force for the State, if the letters rogatory have as their object the acquisition of evidence to be carried out in front of the judge or activities that according to Italian law must be carried out by the judge, shall submit his requests to the judge for preliminary investigations."
Audio/video surveillance in a private place	
Issuing state applies EIO DIR	1. Yes 2. Same as for interception of lett. B (Art. 266 CCP) ; District Public Prosecutor Office and investigative judge territorially competent
DK or IE as issuing state	1. Yes 2. Same as for interception of lett. B (Art. 266 CCP) ; District Public Prosecutor Office and investigative judge territorially competent
Issuing state is a third State	1. Yes 2. Same as for interception of lett. B (Art. 266 CCP) ; District Public Prosecutor Office and investigative judge territorially competent (art. 724 CPP)

Interception of telecommunication abroad	
Issuing state applies EIO DIR	<p>1. CONDITIONS : a domestic order by the issuing State authorizing the interception CRIMES Same as for interception of lett. B (Art. 266 CCP) ; DURATION - Organized crime and terrorism (art. 13 Law no. 203/91): 40 days, which may be extended for further periods of 20 days - Other serious crimes (art. 267 CCP): 15 days, which may be extended for further periods of 15 days</p> <p>2. District Public Prosecutor Office and investigative judge territorially competent</p> <p>3. Yes from the perspective of Italy as executing State</p>
DK or IE as issuing state	<p>1. the same of european investigation order as mentioned above on the base of MLA Convention 2000</p> <p>2. the same of european investigation order as mentioned above on the base of MLA Convention 2000</p> <p>3. the same of european investigation order as mentioned above on the base of MLA Convention 2000</p>
Issuing state is a third State	<p>1. CONDITIONS : a domestic order by the issuing State authorizing the interception CRIMES Same as for interception of lett. B (Art. 266 CCP) ; DURATION - Organized crime and terrorism (art. 13 Law no. 203/91): 40 days, which may be extended for further periods of 20 days - Other serious crimes (art. 267 CCP): 15 days, which may be extended for further periods of 15 days</p> <p>2. District Public Prosecutor Office and investigative judge territorially competent (art. 724 CPP)</p> <p>3. Yes from the perspective of Italy as executing State</p>
Scope of Article 31 EIO Directive and use of Annex C	
<p>1. The Italian legislator considers interception of telecommunications (audio and data) and interception of live communications between present persons as measures entailing an equivalent interference with the rights of the individuals concerned. Therefore, the two investigative measures are governed by the same rules – both in domestic and in cross-border contexts.</p> <p>2. territorially competent District Public Prosecutor Office and investigative judge</p> <p>3. Italian</p>	
Relevant documents	
 <p>IT - accordi MLA con Paesi partner.dc</p>	

4.1.16. Latvia (LV)


LATVIA 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	<p>1. Annex A EIO DIR</p> <p>In accordance with the DIRECTIVE 2014/41/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 3 April 2014 regarding the European Investigation Order in criminal matters, annex C should to be issued only, if interception of telecommunications is without technical assistance (phone number, IP number or e-mail). In this case is necessary explanation are GPS tracking and bugging of a car includes in definition telecommunications. In practise are cross – border differences. Some of countries are issued Annex A, is who prefers article 40 of the Schengen Convention. In order to exclude the differences in practise between member states, there is a need for a broad interpretation of the term telecommunications, what constitutes telecommunications within the meaning of the Directive. After providing of explanation, will be clear which form should to be used.</p> <p>In the same time, is not allowed that issuing country does not inform member state about planning/ongoing actions.</p> <p>2. Should to be issued Annex A EIO in accordance with the DIRECTIVE 2014/41/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 3 April 2014 regarding the European Investigation Order in criminal matters.</p> <p>GPS trucking (in accordance with the Criminal Procedure Law, Article 224. - Surveillance of an Object) is a special investigation procedure and shall be permitted only in investigating less serious, serious or especially serious crimes.</p> <p>3. The State Police of Latvia.</p>
DK or IE as issuing state	<p>1. Should to be issued legal aid request in accordance with the Convention on Mutual Assistance in Criminal Matters between the EU countries established by the Council in accordance with Article 34 of the Treaty on European Union.</p> <p>2. GPS trucking (in accordance with the Criminal Procedure Law, Article 224. - Surveillance of an Object) is a special investigation procedure and shall be permitted only in investigating less serious, serious or especially serious crimes.</p> <p>3. The State Police of Latvia.</p>
Issuing state is a third State	<p>1. Bilateral/multilateral agreements between issuing and executing country. Should be issued legal aid request.</p> <p>2. In accordance with the Criminal Procedure Law, Article 224 - Surveillance of an Object - is a special investigation procedure and shall be permitted only in investigating less serious, serious or especially serious crimes.</p> <p>3. Reciprocity – Prosecutor General’s Office.</p> <p>Bilateral/multilateral agreements - Prosecutor General’s Office or the State Police, depending on the notification.</p>
Bugging of a car	
Issuing state	<p>1. Annex A EIO DIR</p>

applies EIO DIR	<p>2. Should to be issued Annex A EIO in accordance with the DIRECTIVE 2014/41/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 3 April 2014 regarding the European Investigation Order in criminal matters.</p> <p>Bugging of car (in accordance with the Criminal Procedure Law, Article 221- Audio-control of a Site). Only in investigating less serious, serious or especially serious crimes.</p> <p>3. The State Police of Latvia.</p>
DK or IE as issuing state	<p>1. Should to be issued legal aid request in accordance with the Convention on Mutual Assistance in Criminal Matters between the EU countries established by the Council in accordance with Article 34 of the Treaty on European Union.</p> <p>2. Bugging of car (in accordance with the Criminal Procedure Law, Article 221- Audio-control of a Site). Only in investigating less serious, serious or especially serious crimes.</p> <p>3. The State Police of Latvia.</p>
Issuing state is a third State	<p>1. Agreement/Convention between issuing and executing country. Should be issued legal aid request.</p> <p>2. In accordance with the Criminal Procedure Law, Article 221. - Surveillance of an Object or a Site - is a special investigation procedure and shall be permitted only in investigating less serious, serious or especially serious crimes.</p> <p>3. Reciprocity – Prosecutor General’s Office.</p> <p>Bilateral/multilateral agreements - Prosecutor General’s Office or the State Police, depending on the notification.</p>
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	<p>1. Surveillance through Trojan horse software on portable devices is not investigation procedure in the Republic of Latvia, but could be used like as tactical method. The implementation of this measure depends on the circumstances of the case and it is necessary to assess each possible case separately.</p> <p>2. -----</p> <p>3. Control of Data Located in an Automated Data Processing System or Control of the Content of Transmitted Data.</p> <p>4. Annex A of DIRECTIVE 2014/41/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 3 April 2014 regarding the European Investigation Order in criminal matters</p> <p>5. The State Police of Latvia.</p>
DK or IE as issuing state	<p>1. Surveillance through Trojan horse software on portable devices is not investigation procedure in the Republic of Latvia, but could be used like as tactical method. The implementation of this measure depends on the circumstances of the case and it is necessary to assess each possible case separately.</p> <p>2. -----</p> <p>3. Control of Data Located in an Automated Data Processing System or Control of the Content of Transmitted Data.</p> <p>4. Convention on Mutual Assistance in Criminal Matters between the EU countries established by the Council in accordance with Article 34 of the Treaty on European Union.</p> <p>5. The State Police of Latvia.</p>

Issuing state is a third State	<ol style="list-style-type: none"> 1. Surveillance through Trojan horse software on portable devices is not investigation procedure in the Republic of Latvia, but could be used like as tactical method. The implementation of this measure depends on the circumstances of the case and it is necessary to assess each possible case separately. 2.----- 3. Control of Data Located in an Automated Data Processing System or Control of the Content of Transmitted Data. 4. Bilateral/multilateral agreements between issuing and executing country. Should be issued legal aid request. 5. Reciprocity – General Prosecution’s office. <p>Bilateral/multilateral agreements - General Prosecution’s office or the State Police, depending on the notification.</p>
Audio/video surveillance in a private place	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. In accordance with the Criminal Procedure Law, competent authority could provide audio/video surveillance in private place. 2. The audio-control (audio/video surveillance in a private place) of a publicly inaccessible site without the information of the owner, possessor, and visitors of such site shall be performed, on the basis of a decision of an investigating judge, if there are grounds to believe that the conversations, other sounds, or occurrences taking place at such site, may contain information regarding facts included in circumstances to be proven. The audio-control or video-control of a publicly inaccessible site shall be performed only if the acquisition of necessary information is not possible without such operation.
DK or IE as issuing state	<ol style="list-style-type: none"> 1. In accordance with the Criminal Procedure Law, competent authority could provide audio/video surveillance in private place. 2. The audio-control (audio/video surveillance in a private place) of a publicly inaccessible site without the information of the owner, possessor, and visitors of such site shall be performed, on the basis of a decision of an investigating judge, if there are grounds to believe that the conversations, other sounds, or occurrences taking place at such site, may contain information regarding facts included in circumstances to be proven. The audio-control or video-control of a publicly inaccessible site shall be performed only if the acquisition of necessary information is not possible without such operation.
Issuing state is a third State	<ol style="list-style-type: none"> 1. In accordance with the Criminal Procedure Law, competent authority could provide audio/video surveillance in private place. 2. The audio-control (audio/video surveillance in a private place) of a publicly inaccessible site without the information of the owner, possessor, and visitors of such site shall be performed, on the basis of a decision of an investigating judge, if there are grounds to believe that the conversations, other sounds, or occurrences taking place at such site, may contain information regarding facts included in circumstances to be proven. The audio-control or video-control of a publicly inaccessible site shall be performed only if the acquisition of necessary information is not possible without such operation.
Interception of telecommunication abroad	
Issuing state	<ol style="list-style-type: none"> 1. In accordance with the Latvian Criminal procedure law, the performance of a Control of Means of Communication (interception of telecommunication) shall be permitted only in investigating less serious, serious or especially serious crimes and shall be performed on the basis of a decision of an investigating judge. Control of Means of Communication shall not

applies EIO DIR	<p>exceed 30 days. An investigating judge may extend such term, if there are grounds for such extension.</p> <p>2. International Cooperation department of Central Criminal police department of State police of Latvia.</p> <p>3. Case by case.</p>
DK or IE as issuing state	<p>1. In accordance with the Latvian Criminal procedure law, the performance of a Control of Means of Communication (interception of telecommunication) shall be permitted only in investigating less serious, serious or especially serious crimes and shall be performed on the basis of a decision of an investigating judge. Control of Means of Communication shall not exceed 30 days. An investigating judge may extend such term, if there are grounds for such extension.</p> <p>2. International Cooperation department of Central Criminal police department of State Police of Latvia.</p> <p>3. Case by case.</p>
Issuing state is a third State	<p>1. In accordance with the Latvian Criminal procedure law, the performance of a Control of Means of Communication (interception of telecommunication) shall be permitted only in investigating less serious, serious or especially serious crimes and shall be performed on the basis of a decision of an investigating judge. Control of Means of Communication shall not exceed 30 days. An investigating judge may extend such term, if there are grounds for such extension.</p> <p>2. Reciprocity – Prosecutor General’s Office.</p> <p>Bilateral/multilateral agreements - Prosecutor General’s Office or the State Police of Latvia, depending on the notification.</p> <p>3. Case by case.</p>
Scope of Article 31 EIO Directive and use of Annex C	
<p>1. No.</p> <p>2. State police of the Republic of Latvia.</p> <p>3. Latvian/English</p>	

4.1.17. Lithuania (LT)

LITHUANIA 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Annex C EIO DIR 2. Such a secret measure is applied in the Republic of Lithuania in accordance with the provisions of Articles 158 (Actions of Covert Pre-trial Investigation Officers) and 160 (Secret Surveillance) of the Code of Criminal Procedure (CCP). <p>Requirements for the application of this measure:</p> <p>Court Order, issued by an Investigative Judge by a request of a Prosecutor, is required. In a request of a Prosecutor the need of use of technical means (GPS) for the surveillance must be indicated. If the surveillance is implemented in conjunction with the access to a private place (car), the Court order to access a car is also mandatory. The number of accesses, persons implementing it must be indicated in a Prosecutor's request and Court Order. As well as the purposes of the access (like "GPS installation"). Judge must review and ascertain if the "target" has any kind of immunity or the car belongs or is run by the person having an immunity from criminal proceedings. The past measure is not possible investigating misdemeanours and mild crimes.</p> <p>It is possible to use this measure without Court Order in urgent cases by the decision of a prosecutor or even the officer of pre-trial investigation body (for the latter – only without access to a place, just pure surveillance). In such a case the Court approval of executed measure has to be issued in 72 hours after the moment of a decision to apply measure (Article 160 (1) of CCP).</p> <ol style="list-style-type: none"> 3. Police Department under the Ministry of the Interior (Saltoniskiu str. 19, LT-08105, Vilnius, Lithuania; email: info@policija.lt)
DK or IE as issuing state	<ol style="list-style-type: none"> 1. Notification in accordance with Art 20 of the 2000 MLA Convention. 2. The same like in previous paragraph. 3. Police Department under the Ministry of the Interior (Saltoniskiu str. 19, LT-08105, Vilnius, Lithuania; email: info@policija.lt)
Issuing state is a third State	<ol style="list-style-type: none"> 1. Request for a Mutual Legal Assistance in all cases has to reach Lithuania (Prosecutor General's Office) prior implementing the measure despite the need of technical assistance. 2. The same like in previous paragraph. 3. Prosecutor General's Office (Rinktinės str. 5A, LT-01515 Vilnius, Lithuania; email: generaline.prokuratura@prokuraturos.lt)
Bugging of a car	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Annex C EIO DIR 2. Conditions for this measure: <p>Court Order, issued by an Investigative Judge by a request of a Prosecutor. The definition of the activities in Lithuania are:</p>

	<p>- “Control of the information that is transferred by electronic means” (Art. 154 of CCP), that allows to listen and record conversations via electronic means (installing device with SIM card in a car, for example)</p> <p>- “Control of the conversations of the suspect without his knowledge (=secret activities)” (Art. 158 of CCP), that allows to listen and record conversation face-to-face of persons inside the car</p> <p>- “Secret access to a car” (= secret activities) (Art. 158 of CCP) to install a bug / device.</p> <p>The number of accesses, persons implementing it must be indicated in a Prosecutor’s request and Court Order. Duration of a covert measure. A person (persons) which is a target of an interception. Identification data of car. The purposes of the access (like “Bug/Device installation”). Judge must review and ascertain if the “target” has any kind of immunity or the car belongs or is run by the person having an immunity from criminal proceedings.</p> <p>The measures described in Article 158 of CCP are not possible investigating misdemeanours and mild crimes.</p> <p>The measure described in Article 154 of CCP is not possible investigating misdemeanours and some of the mild crimes, except there is a danger of violence or other illegal activity (not specified) against witnesses, victims, experts or their relatives.</p> <p>It is possible to use measures without Court Order in urgent cases. By the decision of a Prosecutor. In such a case the Court approval to executed measure has to be issued in 72 hours after the moment of a decision to apply measure (Article 160 (1) of CCP).</p> <p>3. Police Department under the Ministry of the Interior (Saltoniskiu str. 19, LT-08105, Vilnius, Lithuania; email: info@policija.lt)</p>
DK or IE as issuing state	<p>1. Notification in accordance with Art 20 of the 2000 MLA Convention. Please note that Lithuania has no experience in this field with mentioned countries.</p> <p>2. The same like in previous paragraph.</p> <p>3. Police Department under the Ministry of the Interior (Saltoniskiu str. 19, LT-08105, Vilnius, Lithuania; email: info@policija.lt)</p>
Issuing state is a third State	<p>1. Request for a Mutual Legal Assistance in all cases has to reach Lithuania (Prosecutor General’s Office) prior implementing the measure despite the need of technical assistance.</p> <p>2. The same like in previous paragraph.</p> <p>3. Prosecutor General’s Office (Rinktinės str. 5A, LT-01515 Vilnius, Lithuania; email: generaline.prokuratura@prokuraturos.lt)</p>
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	<p>1. Yes, it is a legal form of interception in Lithuania.</p> <p>2. Legally used upon Court order, like it is explained above, describing Articles 154, 158 of CCP. Such surveillance can only be carried out in the investigation of grave, serious or less serious crimes.</p> <p>3. n/a</p> <p>4. If no need for technical assistance – Annex C, if assistance needed – Annex A.</p> <p>5. For Annex C - Police Department under the Ministry of the Interior (Saltoniskiu str. 19, LT-08105, Vilnius, Lithuania; email: info@policija.lt), for Annex A – PPO according to competence.</p>


DK or IE as issuing state	<p>1. Yes, it is a legal form of interception in Lithuania.</p> <p>2. Legally used upon Court order, like it is explained above, describing Articles 154, 158 of CCP. Such surveillance can only be carried out in the investigation of grave, serious or less serious crimes.</p> <p>3. n/a</p> <p>4. If no need for technical assistance – Notification in accordance with Art 20 of the 2000 MLA Convention., if assistance needed – MLA Request.</p> <p>5. For Notification in accordance with Art 20 of the 2000 MLA Convention - Police Department under the Ministry of the Interior (Saltoniskiu str. 19, LT-08105, Vilnius, Lithuania; email: info@policija.lt), for MLA Request – PPO according to competence.</p>
Issuing state is a third State	<p>1. Yes, it is a legal form of interception in Lithuania.</p> <p>2. Legally used upon Court order, like it is explained above, describing Articles 154, 158 of CCP. Such surveillance can only be carried out in the investigation of grave, serious or less serious crimes.</p> <p>3. n/a</p> <p>4. MLA Request.</p> <p>5. Prosecutor General's Office (Rinktinis str. 5A, LT-01515 Vilnius, Lithuania; email: generaline.prokuratura@prokuraturos.lt)</p>
Audio/video surveillance in a private place	
Issuing state applies EIO DIR	<p>1. Yes.</p> <p>Article 160 of CCP regulates the activity that has a legal definition “Secret surveillance” in Lithuania. In case of the need for that to get into a private place (to install technical means secretly, for instance), in addition, another article, i.e. Article 158 (Actions of Covert Pre-trial Investigation Officers) of CCP shall apply.</p> <p>2. Conditions for this measure: Court Order, issued by an Investigative Judge by a request of a Prosecutor. In a request of a Prosecutor the need of use of technical means (audio/video) for the surveillance must be indicated. If the surveillance, or a very similar secret activities so-called in Lithuania “Control of premises”, “Control of conversations”, etc. are implemented in conjunction with the access to a private place (premises, car), the Court order to access a private place is also mandatory. The number of accesses, persons implementing it must be indicated in a Prosecutor's request and Court Order. As well as the purposes of the access (like “installation”). Judge must review and ascertain if the “target” has any kind of immunity or the “place” belongs or is run by the person having an immunity from criminal proceedings. The past measure is not possible investigating misdemeanours and mild crimes.</p> <p>It is possible to use measure without Court Order in urgent cases. By the decision of a prosecutor or even the officer of pre-trial investigation body (for the latter – only without access to a place, just pure surveillance). In such a case the Court approval to executed measure has to be issued in 72 hours after the moment of a decision to apply measure (Article 160 (1) of CCP).</p> <p>Executing authority might be any from the list of the pre-trial institutions. In most cases it is the Police (for majority of crimes), Special Investigation Service (for corruption related crimes), Criminal Service of the Customs (for smuggling related crimes) and Service for Financial crimes investigation.</p>

DK or IE as issuing state	<ol style="list-style-type: none"> 1. The same like in a previous paragraph. 2. The same like in a previous paragraph.
Issuing state is a third State	<ol style="list-style-type: none"> 1. The same like in a previous paragraph. 2. The same like in a previous paragraph.
Interception of telecommunication abroad	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Conditions for an interception of telecommunication: <p>Court Order, issued by an Investigative Judge by a request of a Prosecutor. Article 154 of CCP regulates it. The definition of the activity is “Control of the information that is transferred by electronic means”.</p> <p>The measure is not possible investigating misdemeanours and some of the mild crimes, except there is a danger of violence or other illegal activity (not specified) against witnesses, victims, experts or their relatives.</p> <p>Maximum period of application – 6 months. In complex cases it can be prolonged up to 9 months.</p> <p>Worth to know that interception in Lithuania is allowed by the Court Order to intercept a “person” and covers all his/her phone numbers, email addresses, etc. that he/she uses during the validity of a Court Order. It means that there is no need to get a new Court Order if a person changes SIM card, device, account, etc.</p> <p>It is possible to use measure without Court Order in urgent cases by the decision of a prosecutor. In such a case the Court approval for executed measure has to be issued in 72 hours after the moment of a decision to apply measure (Article 160 (1) of CCP).</p> 2. Executing authority might be any from the list of the pre-trial institutions. In most cases it is the Police (for majority of crimes), Special Investigation Service (for corruption related crimes), Criminal Service of the Customs (for smuggling related crimes) and Service for Financial crimes investigation. 3. In the event of such a need, this should be discussed on a case-by-case basis . PPO has no competence to handle it.
DK or IE as issuing state	<ol style="list-style-type: none"> 1. The same like in a previous paragraph. 2. The same like in a previous paragraph. 3. The same like in a previous paragraph.
Issuing state is a third State	<ol style="list-style-type: none"> 1. The same like in a previous paragraph. 2. The same like in a previous paragraph. 3. The same like in a previous paragraph.
Scope of Article 31 EIO Directive and use of Annex C	
<ol style="list-style-type: none"> 1. The definition of the measure in Lithuania is “Control of the information that is transferred by electronic means”. It has a bit wider meaning than “interception of telecommunication”, because covers all ways of the control, including using landlines, mobile, email, messengers, etc. Lithuania has no covert measure specifically only for the interception of telecommunication. Instead of term “telecommunication”, Lithuania uses term “information that is transferred by electronic means”. Everything else is listed above. 	

2. Police Department under the Ministry of the Interior (Saltoniskiu str. 19, LT-08105, Vilnius, Lithuania; email: info@policija.lt).


3. Lithuanian and English. However, priority is given to Lithuanian.

4.1.18. Luxembourg (LU)

LUXEMBOURG 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Bugging of a car	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	


Audio/video surveillance in a private place	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Interception of telecommunication abroad	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Scope of Article 31 EIO Directive and use of Annex C	
Relevant documents	

4.1.19. Malta (MT)

MALTA 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Bugging of a car	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	

Audio/video surveillance in a private place	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Interception of telecommunication abroad	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Scope of Article 31 EIO Directive and use of Annex C	
Relevant documents	

4.1.20. The Netherlands (NL)

<div> <div>THE NETHERLANDS</div>  </div>	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	<p>1. Annex A EIO DIR</p> <p>2. Investigative powers may be applied in the execution of a European Investigation Order under the same conditions as they may be applied in a Dutch investigation into the same facts on the basis of the Dutch Code on Criminal Procedure. Requirements of proportionality as well as an assessment of the investigative interest are not taken into account, according to Section 5.4.7. paragraph 1 of the Dutch CCP.</p> <p>These conditions are according to Section 126G of the Dutch CCP:</p> <ul style="list-style-type: none"> - Suspicion of criminal offence - If the suspicion concerns a serious offence as described in Section 67, paragraph 1 CCP, which, given its nature or its connection with other crimes committed by the suspect, constitutes a serious violation of the legal order, the warrant may also include the entry of an enclosed place (not being a private residence). - The order needs to be in the interest of the investigation - The technical device may not be placed on a person without their consent and it may not record any confidential information. - No possibility for ex-post notification, <i>however</i>, depending on the circumstances ex-post permission can be granted for the use of specific data as evidence. - Allowed for a period of three months, with the possibility for extension. <p>3. Public prosecutor (Section 5.4.5 (1) Dutch CCP). More specifically, the public prosecutor at the Dutch national PPO (or Landelijk Internationaal Rechtshulpcentrum (LIRC)). A public prosecutor can issue a written warrant for this purpose, or in urgent case verbally, with the written warrant to follow within three days.</p> <p>NB. This EIO – Annex A does not apply to cross-border surveillance. In this context, a cross-border surveillance is understood to mean:</p> <ol style="list-style-type: none"> 1. an observation of persons started in a certain country that is continuously monitored across the border of another (neighbouring) country. This also applies to observation via a GPS tracker that is continuously monitored. 2. an observation started in another country of persons traveling by plane, train or boat to our country, whereby the observation was continued in that means of transport, or the persons involved were observed until they were (guaranteed) on board that means of transport and the means of transport then goes directly to our country without any stopovers. <p>In case of cross-border surveillance a request must be submitted on the basis of art. 40 Schengen Convention in case of urgency. Otherwise, this is possible by sending a request for legal assistance.</p>
DK or IE as issuing state	<p>1. LoR, as DK and IE are both party to the Agreement and Protocols on mutual legal assistance in criminal matters.</p> <p>2. If the request for legal assistance from a foreign State is based on a treaty, it shall be given effect as far as possible (Section 5.1.4. (2) Dutch CCP).</p> <p>If a treaty provides for direct transmission of requests to judicial authorities, the Public</p>

	<p>Prosecutor in the district where the act requested in the request is to be performed, or a Public Prosecutor with the National or Functional Public Prosecutor's Offices, shall have independent power to grant the request, unless granting the request requires a decision by Our Minister of Security and Justice pursuant to Section 5.1.5 CCP. If the request is not addressed to that Public Prosecutor, it shall be forwarded to them by the addressee without delay.</p> <p>According to Section 5.1.8. CCP, investigative powers may be used to execute a request for legal assistance from a foreign state to the extent that they could also be applied in a Dutch investigation into the same facts on the basis of the Dutch Code on Criminal Procedure. If the request is based on a treaty, requirements relating to proportionality and an assessment of the investigative interest will not be taken into consideration.</p> <p>Otherwise, see above under 2..</p> <p>3. First the Minister of Safety and Justice decides whether the request will be granted, if so, a public prosecutor will be put in charge of the further execution.</p> <p>Otherwise, see above under 3.</p> <p>NB. See above.</p>
Issuing state is a third State	<p>1. LoR</p> <p>2. If the request for legal assistance from a foreign State is based on a treaty, it shall be given effect as far as possible (Section 5.1.4. (2) CCP).</p> <p>In cases involving a request that is not based on a treaty, as well as in cases where the applicable treaty does not require compliance, a request for assistance from a competent authority of a foreign State may be granted if compliance is not contrary to a legal provision or must be refused in the public interest (Section 5.1.4. (3) CCP).</p> <p>If a treaty provides for direct transmission of requests to judicial authorities, the Public Prosecutor in the district where the act requested in the request is to be performed, or a Public Prosecutor with the National or Functional Public Prosecutor's Offices, shall have independent power to grant the request, unless granting the request requires a decision by Our Minister of Security and Justice pursuant to section 5.1.5. If the request is not addressed to that Public Prosecutor, it shall be forwarded to him by the addressee without delay. (5.1.4 (4) CCP)</p> <p>According to Section 5.1.8. CCP, investigative powers may be used to execute a request for legal assistance from a foreign state to the extent that they could also be applied in a Dutch investigation into the same facts on the basis of the Dutch Code on Criminal Procedure. If the request is based on a treaty, requirements relating to proportionality and an assessment of the investigative interest will not be taken into consideration.</p> <p>Otherwise, see above under 2.</p> <p>3. First the Minister of Safety and Justice decides whether the request will be granted, if so, a public prosecutor will be put in charge of the further execution.</p> <p>Otherwise, see above under 3.</p> <p>NB. See above.</p>
Bugging of a car	
Issuing state applies EIO DIR	<p>1. Annex A EIO DIR</p> <p>2. Investigative powers may be applied in the execution of a European Investigation Order under the same conditions as they may be applied in a Dutch investigation into the same facts on the basis of the Dutch Code on Criminal Procedure. Requirements of proportionality as</p>

	<p>well as an assessment of the investigative interest are not taken into account, according to Section 5.4.7. paragraph 1 of the Dutch CCP.</p> <p>These conditions are, according to Section 126l CCP:</p> <ul style="list-style-type: none"> - Suspicion of a crime as described in Section 67 (1) CCP - The crime, given its nature or its connection with other crimes committed by the suspect, constitutes a serious violation of the legal order. - The investigation urgently requires the recording of confidential communications by means of technical aid. - The public prosecutor has the authority to order an investigating officer. <p>If it concerns confidential communication that takes place in a private residence (including a car), stricter requirements apply. In such cases it has to concern an offence punishable by at least 8 years in prison.</p> <p>When the execution of the domestic warrant requires the entry of a private residence without the consent of the person entitled to use the premises, the offence must carry a statutory term of imprisonment of at least eight years.</p> <p>No possibility for ex-post notification.</p> <p>Bugging is allowed for a period of 4 weeks, with the possibility of extension.</p> <p>3. Public prosecutor (Section 5.4.5 (1) Dutch CCP), following prior written authorization granted by the examining magistrate. If it includes the entry of a private residence (e.g. car), this shall be explicitly stated in the warrant.</p> <p>Urgent cases: public prosecutor following prior verbal authorization by the examining magistrate (except if the entry of a private residence applies). The examining magistrate will confirm in writing within three days.</p>
DK or IE as issuing state	<p>1. LoR, as DK and IE are both party to the Agreement and Protocols on mutual legal assistance in criminal matters</p> <p>2. If the request for legal assistance from a foreign State is based on a treaty, it shall be given effect as far as possible (Section 5.1.4. (2) Dutch CCP).</p> <p>If a treaty provides for direct transmission of requests to judicial authorities, the Public Prosecutor in the district where the act requested in the request is to be performed, or a Public Prosecutor with the National or Functional Public Prosecutor's Offices, shall have independent power to grant the request, unless granting the request requires a decision by Our Minister of Security and Justice pursuant to Section 5.1.5 CCP. If the request is not addressed to that Public Prosecutor, it shall be forwarded to them by the addressee without delay.</p> <p>According to Section 5.1.8. CCP, investigative powers may be used to execute a request for legal assistance from a foreign state to the extent that they could also be applied in a Dutch investigation into the same facts on the basis of the Dutch Code on Criminal Procedure. If the request is based on a treaty, requirements relating to proportionality and an assessment of the investigative interest will not be taken into consideration.</p> <p>Otherwise, see above under 2.</p> <p>3. First the Minister of Safety and Justice decides whether the request will be granted, if it will be granted, a public prosecutor will be put in charge.</p> <p>Otherwise, see above under 3.</p>
Issuing state is a third State	<p>1. LoR</p>

	<p>2. If the request for legal assistance from a foreign State is based on a treaty, it shall be given effect as far as possible (Section 5.1.4. (2) CCP).</p> <p>In cases involving a request that is not based on a treaty, as well as in cases where the applicable treaty does not require compliance, a request for assistance from a competent authority of a foreign State may be granted if compliance is not contrary to a legal provision or must be refused in the public interest (Section 5.1.4. (3) CCP).</p> <p>If a treaty provides for direct transmission of requests to judicial authorities, the Public Prosecutor in the district where the act requested in the request is to be performed, or a Public Prosecutor with the National or Functional Public Prosecutor's Offices, shall have independent power to grant the request, unless granting the request requires a decision by Our Minister of Security and Justice pursuant to section 5.1.5. If the request is not addressed to that Public Prosecutor, it shall be forwarded to him by the addressee without delay. (5.1.4 (4) CCP)</p> <p>According to Section 5.1.8. CCP, investigative powers may be used to execute a request for legal assistance from a foreign state to the extent that they could also be applied in a Dutch investigation into the same facts on the basis of the Dutch Code on Criminal Procedure. If the request is based on a treaty, requirements relating to proportionality and an assessment of the investigative interest will not be taken into consideration.</p> <p>Otherwise, see above under 2.</p> <p>3. First the Minister of Safety and Justice decides whether the request will be granted, if it will be granted, a public prosecutor will be put in charge.</p> <p>Otherwise, see above under 3.</p>
<p style="text-align: center;">Surveillance through Trojan horse software</p>	
<p>Issuing state applies EIO DIR</p>	<p>1. Yes. Yet only for the same crimes as for interception of telecommunications (wiretapping) (see above, point 1), when used to:</p> <ul style="list-style-type: none"> * (sub a) determine certain characteristics of the device to be intercepted or the user, like the identity or location, and the recording thereof; * (sub b) enable a wiretap or recording confidential communication as referred to in art. 126l CCP or 126m CCP; * (sub c) execute an observation order (126g CCP) when the public prosecutor has determined that a technical aid can be attached to a person; <p>- only in case of crimes that carry a statutory term of imprisonment of at least eight years or crimes designated by a general measure of governance when used for:</p> <ul style="list-style-type: none"> * (sub d) the recording of data that are or will be stored in the device, insofar as reasonably necessary to reveal the truth; * (sub e) making data inaccessible with regard to which or with the help of which the criminal offense was committed (if necessary to end the offense or to prevent new offenses); <p>2. Said surveillance is allowed according to art. 126nba of the Dutch CCP, the conditions which are stipulated in said article are as follows:</p> <ol style="list-style-type: none"> 1) The crime must, given its nature or its connection with other crimes committed by the suspect, constitute a serious intrusion of society (as described in Section 67 (1) CCP) 2) The measure is urgently required in the interest of the investigation. 3) The device must be in use by the suspect. 4) As deployed for:

	<p>* enabling a wiretap or recording confidential communication as referred to in art. 126m and 126l CCP (see also above 1 and 2);</p> <p>* the execution of an observation order as referred to in art. 126g CCP (see also below 4);</p> <p>When 126nba is applicable, depending on the situation, the requirements of the articles 126m, l or g also have to be met.</p> <p>NB. observation in a private residence through a camera is not possible.</p> <p>This type of surveillance is allowed for a period of 4 weeks, with the possibility of extension.</p> <p>NB. Under Dutch law this measure may also be used to remotely access an automated system.</p> <p>3. n/a</p> <p>4. Annex A.</p> <p>5. - Ordinary cases: The public prosecutor, following prior written authorization granted by the examining magistrate.</p> <p>- Urgent cases: it is possible to request an oral authorization from the examining judge only in the event of a request for amendment, addition or extension. A written warrant will follow within three days.</p>
DK or IE as issuing state	<p>1. See above.</p> <p>2. See above.</p> <p>3. See above.</p> <p>4. LoR.</p> <p>5. First the Minister of Safety and Justice decides whether the request will be granted, if it will be granted, a public prosecutor will be put in charge.</p>
Issuing state is a third State	<p>1. See above.</p> <p>2. See above.</p> <p>3. See above.</p> <p>4. LoR.</p> <p>5. First the Minister of Safety and Justice decides whether the request will be granted, if it will be granted, a public prosecutor will be put in charge.</p>
Audio/video surveillance in a private place	
Issuing state applies EIO DIR	<p>1. Yes, we distinguish between an enclosed place and a place of residence, i.a. a dwelling, Section 126l (2) CCP and section 126g CCP for video surveillance.</p> <p>2. Investigative powers may be applied in the execution of a European Investigation Order under the same conditions as they may be applied in a Dutch investigation into the same facts on the basis of the Dutch Code on Criminal Procedure. Requirements of proportionality as well as an assessment of the investigative interest are not taken into account, according to Section 5.4.7. (1) of the Dutch CCP.</p> <p>The conditions for this measure are according to Section 126l CCP:</p> <ul style="list-style-type: none"> - Suspicion of a serious offence as defined in section 67 (1) - The serious offence in view of its nature or the relation to other serious offences committed by the suspect constitutes a serious breach of law and order - The recording of confidential communications is urgently required in the interest of the investigation.

	<ul style="list-style-type: none"> - The public prosecutor is in charge of ordering the investigating officer as referred to in section 141 (b) and (c). - The warrant may only be issued following authorisation to be granted by the examining magistrate on application of the public prosecutor. The authorisation shall relate to all elements of the warrant. <p>When the public prosecutor wants to enter an enclosed place without the consent of the person entitled to use the premises the following condition is additionally required:</p> <ul style="list-style-type: none"> - Entering the enclosed place is in the interest of the investigation. <p>When the public prosecutor wants to enter a dwelling without the consent of the person entitled to use the premises the following conditions are additionally required:</p> <ul style="list-style-type: none"> - Entering the dwelling is urgently required and in the interest of the investigation - There needs to be a case of a serious offence which carries a statutory term of imprisonment of at least eight years. - The authorisation granted by the examining magistrate to enter the dwelling shall be explicitly stated in the warrant. - The warrant to record confidential communications shall be in accordance with the requirements in Section 126l (3) CCP. - The warrant shall be issued for a period of maximum four weeks, the term of validity may be extended for a period of maximum four weeks each time. <p>Section 126g (6) to (8) inclusive shall apply mutatis mutandis, on the understanding that the public prosecutor shall require authorisation from the examining magistrate for amendment, supplementation or extension.</p> <p>In case the public prosecutor determines that a dwelling will be entered for the purpose of executing the warrant, the warrant may not be issued verbally.</p> <p>As soon as the conditions referred to in subsection 2, second sentence, are no longer met, the public prosecutor shall determine that the execution of the warrant is terminated.</p> <p>In the case of urgent necessity, authorisation from the examining magistrate, referred to in subsections 4 and 6, may be granted verbally, unless subsection 2, second sentence is applied. In that case the examining magistrate shall put the authorisation in writing in three days.</p> <p>According to section 126g CCP video surveillance can only take place in private residences under extraordinary circumstances</p> <p>3. n/a</p>
DK or IE as issuing state	<p>1. Yes, we distinguish between an enclosed place and a place of residence, i.a. a dwelling, Section 126l (2) CCP.</p> <p>2. If the request for legal assistance from a foreign State is based on a treaty, it shall be given effect as far as possible (Section 5.1.4. (2) Dutch CCP).</p> <p>According to Section 5.1.8. CCP, investigative powers may be used to execute a request for legal assistance from a foreign state to the extent that they could also be applied in a Dutch investigation into the same facts on the basis of the Dutch Code on Criminal Procedure. If the request is based on a treaty, requirements relating to proportionality and an assessment of the investigative interest will not be taken into consideration.</p> <p>The conditions for this measure are according to Section 126l CCP:</p> <ul style="list-style-type: none"> - Suspicion of a serious offence as defined in section 67 (1) - The serious offence in view of its nature or the relation to other serious offences committed by the suspect constitutes a serious breach of law and order

	<ul style="list-style-type: none"> - The recording of confidential communications is urgently required in the interest of the investigation. - The public prosecutor is in charge of ordering the investigating officer as referred to in section 141 (b) and (c). - The warrant may only be issued following authorisation to be granted by the examining magistrate on application of the public prosecutor. The authorisation shall relate to all elements of the warrant. <p>When the public prosecutor wants to enter an enclosed place without the consent of the person entitled to use the premises the following condition is additionally required:</p> <ul style="list-style-type: none"> - Entering the enclosed place is in the interest of the investigation. <p>When the public prosecutor wants to enter a dwelling without the consent of the person entitled to use the premises the following conditions are additionally required:</p> <ul style="list-style-type: none"> - Entering the dwelling is urgently required and in the interest of the investigation - There needs to be a case of a serious offence which carries a statutory term of imprisonment of at least eight years. - The authorisation granted by the examining magistrate to enter the dwelling shall be explicitly stated in the warrant. - The warrant to record confidential communications shall be in accordance with the requirements in Section 126l (3) CCP. - The warrant shall be issued for a period of maximum four weeks, the term of validity may be extended for a period of maximum four weeks each time. <p>Section 126g (6) to (8) inclusive shall apply mutatis mutandis, on the understanding that the public prosecutor shall require authorisation from the examining magistrate for amendment, supplementation or extension.</p> <p>In case the public prosecutor determines that a dwelling will be entered for the purpose of executing the warrant, the warrant may not be issued verbally.</p> <p>As soon as the conditions referred to in subsection 2, second sentence, are no longer met, the public prosecutor shall determine that the execution of the warrant is terminated.</p> <p>In the case of urgent necessity, authorisation from the examining magistrate, referred to in subsections 4 and 6, may be granted verbally, unless subsection 2, second sentence is applied. In that case the examining magistrate shall put the authorisation in writing in three days.</p> <p>3. n/a</p>
Issuing state is a third State	<p>1. Yes, we distinguish between an enclosed place and a place of residence, i.a. a dwelling, Section 126l (2) CCP.</p> <p>2. If the request for legal assistance from a foreign State is based on a treaty, it shall be given effect as far as possible (Section 5.1.4. (2) CCP).</p> <p>In cases involving a request that is not based on a treaty, as well as in cases where the applicable treaty does not require compliance, a request for assistance from a competent authority of a foreign State may be granted if compliance is not contrary to a legal provision or must be refused in the public interest (Section 5.1.4. (3) CCP).</p> <p>According to Section 5.1.8. CCP, investigative powers may be used to execute a request for legal assistance from a foreign state to the extent that they could also be applied in a Dutch investigation into the same facts on the basis of the Dutch Code on Criminal Procedure. If the request is based on a treaty, requirements relating to proportionality and an assessment of the investigative interest will not be taken into consideration.</p> <p>The conditions for this measure are according to Section 126l CCP:</p>

	<ul style="list-style-type: none"> - Suspicion of a serious offence as defined in section 67 (1) - The serious offence in view of its nature or the relation to other serious offences committed by the suspect constitutes a serious breach of law and order - The recording of confidential communications is urgently required in the interest of the investigation. - The public prosecutor is in charge of ordering the investigating officer as referred to in section 141 (b) and (c). - The warrant may only be issued following authorisation to be granted by the examining magistrate on application of the public prosecutor. The authorisation shall relate to all elements of the warrant. <p>When the public prosecutor wants to enter an enclosed place without the consent of the person entitled to use the premises the following condition is additionally required:</p> <ul style="list-style-type: none"> - Entering the enclosed place is in the interest of the investigation. <p>When the public prosecutor wants to enter a dwelling without the consent of the person entitled to use the premises the following conditions are additionally required:</p> <ul style="list-style-type: none"> - Entering the dwelling is urgently required and in the interest of the investigation - There needs to be a case of a serious offence which carries a statutory term of imprisonment of at least eight years. - The authorisation granted by the examining magistrate to enter the dwelling shall be explicitly stated in the warrant. - The warrant to record confidential communications shall be in accordance with the requirements in Section 126l (3) CCP. - The warrant shall be issued for a period of maximum four weeks, the term of validity may be extended for a period of maximum four weeks each time. <p>Section 126g (6) to (8) inclusive shall apply mutatis mutandis, on the understanding that the public prosecutor shall require authorisation from the examining magistrate for amendment, supplementation or extension.</p> <p>In case the public prosecutor determines that a dwelling will be entered for the purpose of executing the warrant, the warrant may not be issued verbally.</p> <p>As soon as the conditions referred to in subsection 2, second sentence, are no longer met, the public prosecutor shall determine that the execution of the warrant is terminated.</p> <p>In the case of urgent necessity, authorisation from the examining magistrate, referred to in subsections 4 and 6, may be granted verbally, unless subsection 2, second sentence is applied. In that case the examining magistrate shall put the authorisation in writing in three days.</p> <p>3. n/a</p>
Interception of telecommunication abroad	
Issuing state applies EIO DIR	<p>1. Investigative powers may be applied in the execution of a European Investigation Order under the same conditions as they may be applied in a Dutch investigation into the same facts on the basis of the Dutch Code on Criminal Procedure. Requirements of proportionality as well as an assessment of the investigative interest are not taken into account, according to Section 5.4.7. (1) of the Dutch CCP.</p> <p>In addition to Section 5.4.4 of the Dutch CCP, execution of a European investigation order for the recording of telecommunications may also be refused if the recording of telecommunications would not have been authorised in a similar criminal case in the Netherlands. This means that the requirement of proportionality (section 126m CCP) applies.</p>

	<p>An order may, in consultation with the issuing authority, be executed by:</p> <ol style="list-style-type: none"> transmitting telecommunications immediately to the issuing State; or Intercepting, recording and subsequently transmitting the outcome of the interception of telecommunications to the issuing State. <p>The decision whether to accept a request for a transcription, decoding or decrypting of the recording rests with the public prosecutor.</p> <p>The conditions for this investigative power are laid down in Section 126m CCP:</p> <ul style="list-style-type: none"> - Suspicion of a serious offence as defined in section 67 (1) - The serious offence in view of its nature or the relation to other serious offences committed by the suspect constitutes a serious breach of law and order - The recording of communication not intended for the public by means of a technical device, when using the services of a communications service provider is urgently required in the interest of the investigation. - The public prosecutor is in charge of ordering the investigating officer. - The warrant may only be issued following authorisation to be granted by the examining magistrate on application of the public prosecutor. The examining magistrate may, at the request of the public prosecutor, stipulate in his authorisation that it shall apply to all numbers or other designations as referred to in subsection 2(c) that are in use by the user during the period of validity of the authorisation. - Duration of the interception is 4 weeks, with the possibility to extend. - For extension, an additional EIO is required, which should be received with sufficient time to spare before the period of interception ends. <ol style="list-style-type: none"> See above, under 1. Yes, this is possible, always assuming that it's technically possible for the issuing state as well.
DK or IE as issuing state	<ol style="list-style-type: none"> If the request for legal assistance from a foreign State is based on a treaty, it shall be given effect as far as possible (Section 5.1.4. (2) Dutch CCP). <p>According to Section 5.1.8. CCP, investigative powers may be used to execute a request for legal assistance from a foreign state to the extent that they could also be applied in a Dutch investigation into the same facts on the basis of the Dutch Code on Criminal Procedure. If the request is based on a treaty, requirements relating to proportionality and an assessment of the investigative interest will not be taken into consideration</p> <ol style="list-style-type: none"> See above. See above.
Issuing state is a third State	<ol style="list-style-type: none"> If the request for legal assistance from a foreign State is based on a treaty, it shall be given effect as far as possible (Section 5.1.4. (2) CCP). <p>In cases involving a request that is not based on a treaty, as well as in cases where the applicable treaty does not require compliance, a request for assistance from a competent authority of a foreign State may be granted if compliance is not contrary to a legal provision or must be refused in the public interest (Section 5.1.4. (3) CCP).</p> <p>According to Section 5.1.8. CCP, investigative powers may be used to execute a request for legal assistance from a foreign state to the extent that they could also be applied in a Dutch investigation into the same facts on the basis of the Dutch Code on Criminal Procedure. If the request is based on a treaty, requirements relating to proportionality and an assessment of the investigative interest will not be taken into consideration.</p>

	<p>2. See above.</p> <p>3. See above.</p>
<p align="center">Scope of Article 31 EIO Directive and use of Annex C</p>	
<p>1. Yes, for the interception of telecommunications (wiretapping) with no need of technical assistance from the other Member State.</p> <p>NB. It's important to stress that this doesn't apply to bugging. Under Dutch law this doesn't fall within the scope of 'telecommunication'.</p> <p>2. The prosecutor at the Dutch National PPO (or Landelijk International Rechtshulpcentrum (LIRC)).</p> <p>3. English and Dutch.</p>	

4.1.21. Poland (PL)

<div style="text-align: center;"> POLAND  </div>	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	<p>1. Annex A EIO DIR</p> <p>2. GPS tracking is legally permissible in relation to the following types of crimes /Article 19 (1) Act on Police of 6 April 1990/¹⁷:</p> <p>(1) against life, as defined in Articles 148-150 of the Penal Code, (homicide, infanticide, euthanasia)</p> <p>(2) defined in Article 134 (attack on the President of Republic of Poland), Article 135 Paragraph 1 (assault on the president), Article 136 Paragraph 1 (assault on the head of foreign state), article 156 Paragraphs 1 and 3 (grievous bodily harm, also resulting in a person's death), Article 163 Paragraphs 1 and 3 (causing a life-threatening event, also resulting in the death of a human being or grievous bodily harm to many people), Article 164 Paragraph 1 (immediate endangerment of life-threatening event), Article 165 Paragraphs 1 and 3 (other endangerment, also resulting in the death of a person, or grievous bodily harm to many people), Article 166 (piracy), Article 167 (placing on a ship or aircraft dangerous devices or substances), Articles 173 Paragraphs 1 and 3 (causing a disaster, also resulting in the death of a human being or grievous bodily harm to many people), Article 189 (illegal imprisonment), Article 189a (human trafficking), Article 200a (establishing a connection with a minor under the age of 15 for the purpose of producing or preserving pornographic materials), Article 200b (Condoning paedophilic behaviour), Article 211a (Kidnapping), Article 223 (active assault on a public functionary), Article 224a (Misleading a public utility institution by reporting on an event that threatens the life or health of many people or property to a considerable extent, knowing that there is no danger) Article 228 paragraphs 1 and 3-5 (accepting bribes), Article 229 paragraphs 1 and 3-5 (Offering bribes), Article 230 paragraph 1 (Peddling influence), Article 231 paragraph 1 (Exceeding authority), Article 232 (Violence and illegal threat influencing the official functions of a court of justice), Articles 233 paragraphs 1, 1a, 4 and 6 (False testimony), 234 (False accusation), 235 (fabricating false evidence), 236 § 1 (Concealing evidence of innocence), 238 (False allegations of an offence), 239 § 1 (Aiding the offender of an indictable offence or indictable fiscal offence to evade criminal liability), 240 § 1 (Not reporting an offence), 245 (Witness tampering), 246 (Unlawful duress to obtain a statement), 252 Paragraphs 1-3 (Taking a hostage), 258 (Participation in organised crime group), Articles 267 § 1-4 (Illegal access to information), 268a § 1 and 2 (Damage to databases), 269 (Computer sabotage), 269a (Disruption of work on a network), 269b § 1 (Illegal use of computers and data), 270a § 1 and 2 (Forgery of invoices), 271a § 1 and 2 (Attesting to an untruth of the invoices), 277a § 1 (Forgery and attesting to an untruth of the invoices of great value), Article 279 § 1 (Burglary), Articles 280-282 (Robbery, Aggravated theft, Extortion), 285 Paragraph 1 (Illegal connection), Article 286</p>

¹⁷ For the purpose of this questionnaire it has been assumed that GPS tracking is limited only to tracing an object or a person and does not include the surveillance of conversations (the surveillance falls into another legal regime). In this part of questionnaire have been indicated the types of crimes included in Article 19 (1) Act on Police, since this Act defines main (common) types of crimes in relation to which GPS tracking is allowed by law. However, this activity may be conducted within the discreet surveillance in Poland on the basis of the other Acts, which regulate functioning other competent services, as for examples : Article 30 of the Act of 24 May 2002 on the Internal Security Agency, Article 9g of the Act of 12 October 1990 on Border Guard, Article 34 of the Act of 12 April 2019 on Military Intelligence and Counterintelligence Service or Article 120 of the Act of 16 November 2016 on National Revenue Administration. Types of crimes described in above mentioned Acts are mainly the same as indicated in the Act on Police. Nevertheless, particular provisions of the said acts may foresee admissibility of GPS tracking additionally in relation to other crimes, specific in terms of realisation tasks characteristic of particular service. When in doubt the authority or competent service of issuing state should consult Polish service or judicial authority whether the GPS tracking is legally admissible in relation to the specific crime outside the list given in the questionnaire.

	<p>(Fraud), 287 § 1 (Computer fraud) 296 (Abuse of trust), 296a § 1 and 2 (Corruption of managers), 299 Paragraphs 1-6 (Money laundering) and in Article 310 Paragraphs 1, 2 and 4 (Counterfeiting) of the Penal Code,</p> <p>(2a) defined in the Articles 46(1), (2) and (4) and in Article 48 (1) and (2) of the Act of 25 June 2010 on sport (corruption in sport, dishonest participation in mutual bet, paid protection in sport)</p> <p>(2b) defined in the Articles 178-183 (e.g. trading in financial instruments without the required licence or authorisation) of the Act of 29 July 2005 on Financial Instrument Trading and in article 99-100 of the Act of 29 July 2005 on Public Offering, the Conditions Governing the Introduction of Financial Instruments to Organised Trading, and on Public Companies</p> <p>(3) against economic turnover defined in Article 297-306 (Financial fraud, Insurance fraud, Money laundering, Frustration of creditors, Bankruptcy fraud, Corruption of creditors, Unreliable documentation of business activity, Exploitation, Hindering a public tender, Identification marks) of the Penal Code, resulting in property loss or directed against property, if the damage is in excess of the multiple of fifty minimum wages, defined on the basis of separate provisions,</p> <p>(3a) offences against sexual liberty and decency, if a victim is a minor or if pornographic material, mentioned in Article 202 of Penal Code concern the participation of a minor</p> <p>(3b) defined in Chapter 11 of the Act of 23 July 2000 on Protection of Monuments and Custody on Monuments, in Chapter 5 of the Act of 14 July 1983 on National Archival Resource and on Archives, in Chapter 5a of the Act OF 21 November 1996 on Museums, in Chapter 11a of the Act of 27 June 1997 on Libraries, and in Chapter 6 of the Act of 25 May 2017 on Restitution of National Cultural Values</p> <p>(4) Fiscal crimes, if the value of the subject of offence or reduction of public private amount due is in excess of the multiple of fifty minimum wages, defined on the basis of separate provisions,</p> <p>(4a) fiscal offences referred to in Article 107 paragraph 1 of the Penal Fiscal Code (Organisation of illegal gambling),</p> <p>(5) illegal manufacture, possession or turnover in arms, ammunition, explosives, intoxicants, psychotropic substances and their precursors, as well as nuclear and radioactive materials,</p> <p>(6) defined in Article 8 of the Act of 6 June 1997 – Provisions implementing the Penal Code (Dz. U. No 88, item 554, as amended), (i.e. Slave trade)</p> <p>(7) defined in Article 43-46 of the Act of 1 July 2005 on collection, storage and transplantation of cells, tissues and organs (Dz. U. No 169, item 1411),</p> <p>(8) prosecuted under international contracts and agreements,</p> <p>(9) defined in (the above mentioned points 1-8) or described in the Article 45 paragraph 2 of the Penal Code or in the Article of 33 paragraph 2 of the Penal Fiscal Code – for the purpose of revealing property at risk of forfeiture.</p> <p>GPS tracking is legally permissible to document crimes referred to in Article 19 (1) or to establish the identity of those involved in the crimes or to take over the objects of crime. This activity may be ordered within a discreet surveillance of the manufacture, transport, storage and trade in crime objects, provided this does not involve a threat to human life or health /Article 19b (1) Act on Police/.¹⁸</p> <p>The mandatory requirement to carry out such activities in the Polish territory is that the competent services of the issuing state and the Polish services shall in advance agree on the</p>
--	--

¹⁸ Please see also footnote no. 17. In any other cases GPS tracking on the Polish territory is possible only on the basis of article 40 of Convention of 14 June 1985 implementing the Schengen Agreement., however in such cases this is only a cooperation between policies (services).

	<p>duration of the activities and the conditions for their performance within the scope of the request included in the EIO.</p> <p>It is possible to obtain the consent of the competent Polish authority to the interception of the GPS tracking data when it has already taken place in the Polish territory.</p> <p>3. The competent authority is circuit public prosecutor accordingly with its territorial jurisdiction. In case it is not possible to establish territorial jurisdiction EIO in the form of Annex A may be sent to the central authority (only for cases at the pre-trial stage) <i>i.e.</i> International Cooperation Office of the National Public Prosecutor's Office, ul. Postępu 3, 02676 Warsaw, Tel. + 48 22 1251490, fax: + 48 22 1251422, e-mail: sekretariat.pk.bwm@prokuratura.gov.pl</p>
DK or IE as issuing state	<p>1. Notification in accordance with Article 20 of the 2000 MLA Convention</p> <p>2. GPS tracking is legally permissible in relation to the same types (groups) of crimes and under the same conditions as indicated with regard to the issuing states, applying EIO DIR. These crimes and conditions are mainly described in the Article 19 (1) in conjunction with Article 19b (1) Act on the Police of 6 April 1990¹⁹.</p> <p>It is possible to obtain the consent of the competent Polish authority to the interception of the GPS tracking data when it has already taken place in the Polish territory.</p> <p>3. The competent authority is the circuit public prosecutor having territorial jurisdiction, while the role of contact points shall be fulfilled by the Voivodeship Police Commanders ('Komendant Wojewódzki Policji') having territorial jurisdiction. The notification may also be sent to the International Police Cooperation Bureau of the National Police Headquarters acting as National Bureau of Interpol.</p>
Issuing state is a third State	<p>1. It should be sent a request for international legal assistance</p> <p>2. GPS tracking is legally permissible in relation to the same types (groups) of crimes and under the same conditions as indicated with regard to the issuing states applying EIO DIR or the 2000 MLA Convention, are mainly described in the article 19 (1) in conjunction with article 19b (1) Act on the Police of 6 April 1990²⁰.</p> <p>It is possible to obtain the consent of the competent Polish authority to the interception of the GPS tracking data when it has already taken place in the Polish territory.</p> <p>3. Request for international legal assistance shall be sent to the circuit prosecutor's office having the territorial jurisdiction, provided that such possibility of direct communication between judicial authorities has been foreseen by the bilateral agreement or multilateral convention on mutual legal assistance in criminal matters, binding in legal relations between Poland and the issuing third State. If such multilateral convention or bilateral agreement establish communication only between central authorities, request for legal assistance shall be forwarded to the Polish Ministry of Justice or to the National Prosecutor's Office (Bureau of International Legal Cooperation), if the latter authority has been indicated in particular international treaty as a central authority on the Polish side. In case the GPS tracking data is carried out within controlled delivery on the basis of Article 18 of the Second Additional Protocol to the European Convention on Mutual Legal Assistance of 20 April 1959, the authority competent for reception of such request is Chief Police Commander ('Komendant Główny Policji'). GPS tracking data may also be carried out within special investigative techniques on the basis of sectoral conventions, binding in legal relations with third country.</p>

¹⁹ Please see also footnote no. 17 and 18

²⁰ Please see also footnote no. 17 and 18

Bugging of a car	
Issuing state applies EIO DIR	<p>1. Annex A EIO DIR</p> <p>2. Bugging of a car – installed in issuing country and crossing the Polish border is allowed, in accordance with Article 241 in conjunction with Article 237 paragraph 3-4 of the Polish Code of Criminal Procedure only when the ongoing proceedings or a justified concern as to the possibility of a new criminal offence concern:</p> <ol style="list-style-type: none"> 1) homicide; 2) causing a danger to the public or causing a catastrophe; 3) human trafficking; 4) abduction of a person; 5) ransom extortion; 6) hijacking of an aircraft or ship; 7) robbery, robbery with violence, or extortion by force; 8) attempt against the sovereignty or independence of the State; 9) attempt against the constitutional order of the State or against its supreme bodies, or against a unit of the Armed Forces of the Republic of Poland; 10) espionage or disclosure of classified information with the clause "secret" or "top secret"; 11) amassing weapons, explosives or radioactive materials; 12) counterfeiting and circulating counterfeit monies, payment means or instruments, or tradable documents entitling to receive a cash amount, commodity, cargo, or in-kind prize, or tradable documents providing for an obligation of capital contribution, contribution of interest, share in profits or statement of interest in a company; 12a) the forgery or modification of invoices or the use of invoices forged or modified within the scope of factual circumstances that might influence the determination of the amount of the public-law liabilities or their refund, or the refund of other tax liabilities, and the issuance and use of invoices certifying false information concerning factual circumstances that might influence the determination of the amount of the public liabilities or their refund, or the refund of other tax liabilities; 13) manufacturing, processing, trading, and smuggling drugs, precursors, substitutes, and psychotropic substances; 14) organised crime group; 15) property of significant value; 16) use of violence or unlawful threats in connection with criminal proceedings; 16a) giving false testimony and the presentation of a false opinion, expert opinion or translation by an expert witness, qualified expert, or translator; 16b) a false accusation of a criminal offence, fiscal offence, or fiscal delinquency against another person; 16c) producing false evidence or taking other deceptive actions directing prosecution for a crime, fiscal offence, or fiscal delinquency against another person, or taking such actions in the course of the proceedings; 16d) concealing evidence demonstrating the innocence of a person suspected of committing a criminal offence, fiscal offence, or fiscal delinquency;

	<p>16e) notifying a prosecution body of a criminal offence or fiscal offence that has not been committed;</p> <p>16f) acting as an accessory after the fact;</p> <p>16g) failure to report a criminal offence;</p> <p>17) bribery and influence peddling;</p> <p>18) procurement or facilitation of prostitution;</p> <p>19) criminal offences defined in Chapter XVI of the Act of 6 June 1997 - the Criminal Code (Journal of Laws of 2020, items 1444 and 1517), as well as in Articles 5 to 8 of the Rome Statute of the International Criminal Court, drawn up in Rome on 17 July 1998 (Journal of Laws of 2003, item 708 and of 2018, item 1753), hereinafter referred to as "Rome Statute".</p> <p>The bugging of a car and interception of communication obtained in this way shall also be allowed for the purpose of revealing property at risk of forfeiture, as referred to in Article 45 § 2 of the Criminal Code or Article 33 § 2 of the Fiscal Criminal Code.</p> <p>The bugging of a car interception of communication obtained in this way shall be permitted with regard to a suspected person, the accused, and with regard to the injured or another person whom the accused may contact or who might be connected with the perpetrator or with an imminent criminal offence.</p> <p>It is possible to obtain the consent of the competent Polish authority to the interception of communication by bugging a car, when it has already taken place on the Polish territory.</p> <p>3. The authority in charge is district court, having territorial jurisdiction, regardless of the stage of the proceeding in the issuing state. When it is not possible to establish territorial jurisdiction, the EIO may be sent to the central authority – National Prosecutor's Office, Bureau of International Legal Cooperation. If an EIO was issued at the judicial stage of the proceeding, its transmission is also possible via the Ministry of Justice. In such case, the EIO can be sent to the following address: The Ministry of Justice, Department of International Cooperation and Human Rights, ul. Chopina 1, 00-950 Warsaw, tel. + 48 22 23-90-870, fax: + 48 22 62-80-949, e-mail : dwmpc@ms.gov.pl</p>
DK or IE as issuing state	<p>1. Notification in accordance with Article 20 of the 2000 MLA Convention</p> <p>2. Bugging of a car – installed in issuing country and crossing the Polish border is allowed, in accordance with Article 241 in conjunction with Article 237 paragraph 3-4 of the Polish Code of Criminal Procedure in relation to the same types of crimes and under the same conditions as indicated with regard to the Member States applying EIO.</p> <p>It is possible to obtain the consent of the competent Polish authority to the interception of communication by bugging a car, when it has already taken place on the Polish territory.</p> <p>3. The competent authority is the circuit public prosecutor having territorial jurisdiction, while the role of contact points shall be fulfilled by the Voivodeship Police Commanders ('Komendant Wojewódzki Policji') having territorial jurisdiction. The notification may also be sent to the International Police Cooperation Bureau of the National Police Headquarters acting as National Bureau of Interpol.</p>
Issuing state is a third State	<p>1. It should be sent a request for international legal assistance.</p> <p>2. Bugging of a car – installed in issuing country and crossing the Polish border is allowed, in accordance with Article 241 in conjunction with Article 237 paragraph 3-4 of the Polish Code of Criminal Procedure in relation to the same types of crimes and under the same conditions as indicated with regard to the states applying EIO and the 2000 MLA Convention.</p> <p>3. Request for international legal assistance shall be sent to the circuit prosecutor's office having the territorial jurisdiction, provided that such possibility of direct communication between judicial authorities has been foreseen by the bilateral agreement or multilateral convention on mutual legal assistance in criminal matters, binding in legal relations between</p>

	<p>Poland and the issuing third State. If the such multilateral convention or bilateral agreement establish communication only between central authorities, request for legal assistance shall be forwarded to the Polish Ministry of Justice or to the National Prosecutor's Office (Bureau of International Legal Cooperation), if the latter authority has been indicated in particular international treaty as a central authority on the Polish side. The bugging of a car and interception of communication obtained in this way may also be carried out within special investigative techniques on the basis of sectoral conventions binding in legal relations with third country.</p>
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Surveillance through Trojan horse software is legally permissible form interception in accordance with Article 241 in conjunction with Article 237 paragraph 3-4 of the Polish Code of Criminal Procedure. 2. This form of interception may be applied under the same conditions and in relation to the same types of crimes as previously indicated with regard to bugging of a car and interception of communication obtained in this way (Article 241 in conjunction with Article 237 paragraph 3-4 of the Polish Code of Criminal Procedure). 3. Not applicable, regarding the affirmative answer to the previous point. 4. Annex A to the EIO DIR should be used. 5. The authority in charge is district court, having territorial jurisdiction, regardless of the stage of the proceeding in the issuing state. When it is not possible to establish territorial jurisdiction, the EIO may be sent to the central authority – National Prosecutor's Office, Bureau of International Legal Cooperation. If an EIO was issued at the judicial stage of the proceeding, its transmission is also possible via the Ministry of Justice, Department of International Cooperation and Human Rights.
DK or IE as issuing state	<ol style="list-style-type: none"> 1. Surveillance through Trojan horse software is legally permissible form interception in accordance with Article 241 in conjunction with Article 237 paragraph 3-4 of the Polish Code of Criminal Procedure. 2. This form of interception may be applied under the same conditions and in relation to the same types of crimes as previously indicated with regard to bugging of a car and interception of communication obtained in this way (Article 241 in conjunction with Article 237 paragraph 3-4 of the Polish Code of Criminal Procedure). 3. Not applicable, regarding the affirmative answer to the previous point. 4. Notification in accordance with Art 20 of the 2000 MLA Convention should be used. 5. The competent authority is the circuit public prosecutor having territorial jurisdiction, while the role of contact points shall be fulfilled by the Voivodeship Police Commanders ('Komendant Wojewódzki Policji') having territorial jurisdiction. The notification may also be sent to the International Police Cooperation Bureau of the National Police Headquarters acting as National Bureau of Interpol.
Issuing state is a third State	<ol style="list-style-type: none"> 1. Surveillance through Trojan horse software is legally permissible form interception in accordance with Article 241 in conjunction with Article 237 paragraph 3-4 of the Polish Code of Criminal Procedure. 2. This form of interception may be applied under the same conditions and in relation to the same types of crimes as previously indicated with regard to bugging of a car and interception of communication obtained in this way (Article 241 in conjunction with article 237 paragraph 3-4 of the Polish Code of Criminal Procedure). 3. Not applicable, regarding the affirmative answer to the previous point.

	<p>4. Request for international legal assistance should be sent.</p> <p>5. Request for international legal assistance shall be sent to the circuit prosecutor's office having the territorial jurisdiction, provided that such possibility of direct communication between judicial authorities has been foreseen by the bilateral agreement or multilateral convention on mutual legal assistance in criminal matters, legally binding in legal relations between Poland and the issuing third State. If the such multilateral convention or bilateral agreement establish communication only between central authorities, request for legal assistance shall be forwarded to the Polish Ministry of Justice or to the National Prosecutor's Office (Bureau of International Legal Cooperation), if the latter authority has been indicated in particular international treaty as a central authority on the Polish side. In case the GPS tracking data is carried out within controlled delivery on the basis of Article 18 of the Second Additional Protocol to the European Convention on Mutual Legal Assistance of 20 April 1959, the authority competent for reception of such request is Chief Police Commander ('Komendant Główny Policji'). Surveillance through Trojan horse software may also be carried out within special investigative techniques on the basis of sectoral conventions, binding in legal relations with third country.</p>
Audio/video surveillance in a private place	
Issuing state applies EIO DIR	<p>1. Polish legislation provides for the possibility of carrying out audio/video surveillance in a private place /article 19 (6) point 2 Act on the Police/21.</p> <p>2. This form of interception may be applied under following conditions and in relation to the undermentioned category of crimes , indicated in the Article 19 (1) Act on the Police :</p> <p>(1) against life, as defined in Articles 148-150 of the Penal Code, (homicide, infanticide, euthanasia),</p> <p>(2) defined in Article 134 (attack on the President of Republic of Poland), Article 135 Paragraph 1 (assault on the president), Article 136 Paragraph 1 (Assault on the head on foreign state), Article 156 Paragraphs 1 and 3 (Grievous bodily harm, also resulting in a person's death), Article 163 Paragraphs 1 and 3 (Causing a life-threatening event, also resulting in the death of a human being or grievous bodily harm to many people), Article 164 Paragraph 1 (Immediate endangerment of life-threatening event), Article 165 Paragraphs 1 and 3 (Other endangerment, also resulting in the death of a person, or grievous bodily harm to many people), Article 166 (Piracy), Article 167 (Placing on a ship or aircraft dangerous devices or substances), Articles 173 Paragraphs 1 and 3 (Causing a disaster, also resulting in the death of a human being or grievous bodily harm to many people), Article 189 (Illegal imprisonment), Article 189a (human trafficking), Article 200a (Establishing a connection with a minor under the age of 15 for the purpose of producing or preserving pornographic materials), Article 200b (Condoning paedophilic behaviour), Article 211a (Kidnapping), Article 223 (Active assault on a public functionary), Article 224a (Misleading a public utility institution by reporting on an event that threatens the life or health of many people or property to a considerable extent, knowing that there is no danger) Article 228 paragraphs 1 and 3-5 (Accepting bribes), Article 229 paragraphs 1 and 3-5 (Offering bribes), Article 230 paragraph 1 (Peddling influence), Article 231 paragraph 1 (Exceeding authority), Article 232</p>

²¹ Types of crimes have been indicated in this point of questionnaire on the basis of Act on Police, which includes the most common types of crimes when it comes to audio/video surveillance in the private place. However, this possibility is also foreseen by the Article 17 (1) and (5) point 2 of the Act of 9 June 2006 on Central Anticorruption Bureau, Article 27 (1) and (6) point 2 of the Act of 24 May 2002 on the Internal Security Agency, Article 9ge (1) and (7) point 2 of the Act of 12 October 1990 on Border Guard, Article 31 (1) and (4) point 2 of the Act of 12 April 2019 on Military Intelligence and Counterintelligence Service or Article 118 (1) and (4) point 2 of the Act of 16 November 2016 on National Revenue Administration. Types of crimes described in the above mentioned Acts and the prerequisites for this type of surveillance are mainly the same as indicated in the Act on Police. Nevertheless particular provisions of the said Acts may foresee admissibility of audio/video surveillance in a private place additionally in relation to other crimes, specific in terms of realisation tasks characteristic of particular service. When in doubt the authority or competent service of issuing state should consult Polish service or judicial authority whether the activity at issue is legally admissible in relation to the specific crime outside the list given in the questionnaire.

	<p>(Violence and illegal threat influencing the official functions of a court of justice), Articles 233 paragraphs 1, 1a, 4 and 6 (False testimony), 234 (False accusation), 235 (Fabricating false evidence), 236 § 1 (Concealing evidence of innocence), 238 (False allegations of an offence), 239 § 1 (Aiding the offender of an indictable offence or indictable fiscal offence to evade criminal liability), 240 § 1 (Not reporting an offence), 245 (Witness tampering), 246 (Unlawful duress to obtain a statement), 252 Paragraphs 1-3 (Taking a hostage), 258 (participation in organised crime group), Articles 267 § 1-4 (Illegal access to information), 268a § 1 and 2 (Damage to databases), 269 (Computer sabotage), 269a (disruption of work on a network), 269b § 1 (Illegal use of computers and data), 270a § 1 and 2 (Forgery of invoices), 271a § 1 and 2 (Attesting to an untruth of the invoices), 277a § 1 (Forgery and attesting to an untruth of the invoices of great value), article 279 § 1 (burglary), articles 280-282 (Robbery, aggravated theft, extortion), 285 Paragraph 1 (Illegal connection), Article 286 (Fraud), 287 § 1 (Computer fraud) 296 (Abuse of trust), 296 a§ 1 and 2 (Corruption of managers), 299 Paragraphs 1-6 (Money laundering) and in Article 310 Paragraphs 1, 2 and 4 (Counterfeiting) of the Penal Code,</p> <p>(2a) defined in the Articles 46(1), (2) and (4) and in article 48 (1) and (2) of the Act of 25 June 2010 on sport (corruption in sport, dishonest participation in mutual bet, paid protection in sport)</p> <p>(2b) defined in the Articles 178-183 (e.g. trading in financial instruments without the required licence or authorisation) of the Act of 29 July 2005 on Financial Instrument Trading and in article 99-100 of the Act of 29 July 2005 on Public Offering, the Conditions Governing the Introduction of Financial Instruments to Organised Trading, and on Public Companies</p> <p>(3) against economic turnover defined in Article 297-306 (Financial fraud, Insurance fraud, Money laundering, Frustration of creditors, Bankruptcy fraud, Corruption of creditors, Unreliable documentation of business activity, Exploitation, Hindering a public tender, Identification marks) of the Penal Code, resulting in property loss or directed against property, if the damage is in excess of the multiple of fifty minimum wages, defined on the basis of separate provisions,</p> <p>(3a) offences against sexual liberty and decency, if a victim is a minor or if pornographic material, mentioned in article 202 of Penal Code, concern the participation of a minor</p> <p>(3b) defined in Chapter 11 of the Act of 23 July 2000 on Protection of Monuments and Custody on Monuments, in Chapter 5 of the Act of 14 July 1983 on National Archival Resource and on Archives, in Chapter 5a of the Act OF 21 November 1996 on Museums, in Chapter 11a of the Act of 27 June 1997 on Libraries, and in Chapter 6 of the Act of 25 May 2017 on Restitution of National Cultural Values</p> <p>(4) Fiscal crimes, if the value of the subject of offence or reduction of public private amount due is in excess of the multiple of fifty minimum wages, defined on the basis of separate provisions,</p> <p>(4a) fiscal offences referred to in Article 107 paragraph 1 of the Penal Fiscal Code (organisation of illegal gambling),</p> <p>(5) illegal manufacture, possession or turnover in arms, ammunition, explosives, intoxicants, psychotropic substances and their precursors, as well as nuclear and radioactive materials,</p> <p>(6) defined in Article 8 of the Act of 6 June 1997 – Provisions implementing the Penal Code (Dz. U. No 88, item 554, as amended), (i.e. Slave trade)</p> <p>(7) defined in Article 43-46 of the Act of 1 July 2005 on collection, storage and transplantation of cells, tissues and organs (Dz. U. No 169, item 1411),</p> <p>(8) prosecuted under international contracts and agreements,</p> <p>(9) defined in (the above mentioned points 1-8) or described in the Article 45 paragraph 2 of the Penal Code or in the Article of 33 paragraph 2 of the Penal Fiscal Code – for the purpose of revealing property at risk of forfeiture.</p>
--	---

	<p>Audio/video surveillance in a private place may be ordered only in case of preliminary investigation carried out by the Police to prevent, detect, establish perpetrators, as well as obtain and record evidence of the perpetrators prosecuted by the public prosecutor, or of intentional crime: when other means appeared ineffective or there is significant probability of the means being ineffective or useless.</p> <p>The mandatory requirement to carry out such activities on the Polish territory is that the competent services of the issuing state and the Polish services shall in advance agree on the duration of the activities and the conditions for their performance within the scope of the request included in the EIO. This tool will be the most effective in connection with this form of surveillance.</p> <p>Circuit Prosecutor having territorial jurisdiction is compete to execute the EIO (Annex A to the EIO DIR), concerning this measure. If it is not possible to establish the territorial jurisdiction, the EIO may be sent to the central authority – National Prosecutor’s Office, Bureau of International Cooperation.</p> <p>3. If within carrying out audio and especially video surveillance in private place it may come to recording, by technical means, of the content of conversation or information transmissions other than telephone ones, alternatively may be applied the previously mentioned regulation, defined in Article 241 in conjunction with Article 237 paragraph 3-4 of the Polish Code of Criminal Procedure. As a consequence, this form of surveillance might be applied under the same conditions and in relation to the same types of crimes as previously indicated with regard to bugging of a car and surveillance through Trojan horse software. In such case, the EIO should be sent to the district court, having territorial jurisdiction, regardless of the stage of the proceeding in the issuing state. When it is not possible to establish territorial jurisdiction, the EIO may be sent to the central authority – National Prosecutor’s Office, Bureau of International Legal Cooperation. If an EIO was issued at the judicial stage of the proceeding, its transmission is also possible via the Ministry of Justice, Department of International Cooperation and Human Rights.</p>
DK or IE as issuing state	<p>1. Polish legislation provides for the possibility of carrying out audio/video surveillance in a private place /Article 19 (6) point 2 Act on the Police/</p> <p>2. This form of interception may be applied under following conditions and in relation to the same categories of crimes, defined in the Article 19 (1) Act on the Police²², as in relation to the Member states applying EIO DIR</p> <p>Audio/video surveillance in a private place may be ordered only in case of preliminary investigation carried out by the Police to prevent, detect, establish perpetrators, as well as obtain and record evidence of the perpetrators prosecuted by the public prosecutor, or of intentional crime: when other means appeared ineffective or there is significant probability of the means being ineffective or useless.</p> <p>Circuit Prosecutor having territorial jurisdiction is compete to execute the MLA request, concerning this measure. If it is not possible to establish the territorial jurisdiction, the MLA request may be sent to the central authority – National Prosecutor’s Office, Bureau of International Cooperation.</p> <p>3. If within carrying out audio and especially video surveillance in private place it may come to recording, by technical means, of the content of conversation or information transmissions other than telephone ones, alternatively may be applied the previously mentioned regulation, defined in Article 241 in conjunction with Article 237 paragraph 3-4 of the Polish Code of Criminal Procedure. As a consequence, this form of surveillance might be applied under the same conditions and in relation to the same types of crimes as previously indicated with regard to bugging of a car and surveillance through Trojan horse. In such case, the MLA request should be sent to the circuit public prosecutor, having territorial jurisdiction. When it is not possible to establish territorial jurisdiction, the request may be sent to the central authority – National Prosecutor’s Office, Bureau of International Legal Cooperation. If the</p>

²² Please see also footnote 21

	<p>MLA-request was issued at the judicial stage of the proceeding, it should be transmitted via the Ministry of Justice, Department of International Cooperation and Human Rights.</p>
<p>Issuing state is a third State</p>	<p>1. Polish legislation provides for the possibility of carrying out audio/video surveillance in a private place /article 19 (6) point 2 Act on the Police/.</p> <p>2. This form of interception may be applied under conditions and in relation to the category of crimes, previously indicated in relation to the Member States applying the EIO DIR and Denmark and Ireland, defined in the Article 19 (1) Act on the Police²³.</p> <p>Request for international legal assistance shall be sent to the circuit prosecutor's office having the territorial jurisdiction, provided that such possibility of direct communication between judicial authorities has been foreseen by the bilateral agreement or multilateral convention on mutual legal assistance in criminal matters, binding in legal relations between Poland and the issuing third State. If such multilateral convention or bilateral agreement establish communication only between central authorities, request for legal assistance shall be forwarded to the Polish Ministry of Justice or to the National Prosecutor's Office (Bureau of International Legal Cooperation), if the latter authority has been indicated in particular international treaty as a central authority on the Polish side. Audio/video surveillance in a private place may also be carried out within special investigative techniques on the basis of sectoral conventions, binding in legal relations with third country.</p> <p>3. If within carrying out audio and especially video surveillance in private place it may come to recording, by technical means, of the content of conversation or information transmissions other than telephone ones, alternatively may be applied the previously mentioned regulation, defined in Article 241 in conjunction with Article 237 paragraph 3-4 of the Polish Code of Criminal Procedure. As a consequence, this form of surveillance might be applied under the same conditions and in relation to the same types of crimes as previously indicated with regard to bugging of a car and surveillance through Trojan horse software (Article 241 in conjunction with Article 237 paragraph 3-4 of the Polish Code of Criminal Procedure). In such case request for international legal assistance shall be sent in the same way as described in the previous point of the questionnaire.</p>
<p style="text-align: center;">Interception of telecommunication abroad</p>	
<p>Issuing state applies EIO DIR</p>	<p>1. Interception of telecommunication is allowed in Polish jurisdiction upon the request of issuing state, in accordance with Article 237 paragraph 3-4 Polish Code of Criminal Procedure and in the light of Article 241 Polish Code of Criminal Procedure, only when the ongoing proceedings or a justified concern as to the possibility of a new criminal offence concern:</p> <ol style="list-style-type: none"> 1) homicide; 2) causing a danger to the public or causing a catastrophe; 3) human trafficking; 4) abduction of a person; 5) ransom extortion; 6) hijacking of an aircraft or ship; 7) robbery, robbery with violence, or extortion by force; 8) attempt against the sovereignty or independence of the State; 9) attempt against the constitutional order of the State or against its supreme bodies, or against a unit of the Armed Forces of the Republic of Poland; 10) espionage or disclosure of classified information with the clause "secret" or "top secret";

²³ Please see also footnote 21

	<p>11) amassing weapons, explosives or radioactive materials;</p> <p>12) counterfeiting and circulating counterfeit monies, payment means or instruments, or tradable documents entitling to receive a cash amount, commodity, cargo, or in-kind prize, or tradable documents providing for an obligation of capital contribution, contribution of interest, share in profits or statement of interest in a company;</p> <p>12a) the forgery or modification of invoices or the use of invoices forged or modified within the scope of factual circumstances that might influence the determination of the amount of the public-law liabilities or their refund, or the refund of other tax liabilities, and the issuance and use of invoices certifying false information concerning factual circumstances that might influence the determination of the amount of the public liabilities or their refund, or the refund of other tax liabilities;</p> <p>13) manufacturing, processing, trading, and smuggling drugs, precursors, substitutes, and psychotropic substances;</p> <p>14) organised crime group;</p> <p>15) property of significant value;</p> <p>16) use of violence or unlawful threats in connection with criminal proceedings;</p> <p>16a) giving false testimony and the presentation of a false opinion, expert opinion or translation by an expert witness, qualified expert, or translator;</p> <p>16b) a false accusation of a criminal offence, fiscal offence, or fiscal delinquency against another person;</p> <p>16c) producing false evidence or taking other deceptive actions directing prosecution for a crime, fiscal offence, or fiscal delinquency against another person, or taking such actions in the course of the proceedings;</p> <p>16d) concealing evidence demonstrating the innocence of a person suspected of committing a criminal offence, fiscal offence, or fiscal delinquency;</p> <p>16e) notifying a prosecution body of a criminal offence or fiscal offence that has not been committed;</p> <p>16f) acting as an accessory after the fact;</p> <p>16g) failure to report a criminal offence;</p> <p>17) bribery and influence peddling;</p> <p>18) procurement or facilitation of prostitution;</p> <p>19) criminal offences defined in Chapter XVI of the Act of 6 June 1997 - the Criminal Code (Journal of Laws of 2020, items 1444 and 1517), as well as in Articles 5 to 8 of the Rome Statute of the International Criminal Court, drawn up in Rome on 17 July 1998 (Journal of Laws of 2003, item 708 and of 2018, item 1753), hereinafter referred to as "Rome Statute".</p> <p>The surveillance and recording of the content of telephone conversations and interception of other forms of telecommunication shall also be allowed for the purpose of revealing property at risk of forfeiture, as referred to in Article 45 § 2 of the Criminal Code or Article 33 § 2 of the Fiscal Criminal Code.</p> <p>Surveillance and recording of the contents of telephone conversations and interception of other forms of telecommunication shall be permitted with regard to a suspected person, the accused, and with regard to the injured or another person whom the accused may contact or who might be connected with the perpetrator or with an imminent criminal offence.</p> <p>The surveillance and recording of telephone conversations and interception of other forms of telecommunication may be carried out for a period not exceeding 3 months, with a possibility of extension, in particularly justified cases, for a period no longer than further 3 months.</p>
--	--


	<p>2. The authority in charge is district court, having territorial jurisdiction, regardless of the stage of the proceeding in the issuing state. When it is not possible to establish territorial jurisdiction, the EIO may be sent to the central authority – National Prosecutor’s Office, Bureau of International Legal Cooperation. If an EIO was issued at the judicial stage of the proceeding, its transmission is also possible via the Ministry of Justice, Department of International Cooperation and Human Rights.</p> <p>3. It is not technically possible to channel the intercepted telecommunication to the issuing state in real-time. However, it is possible to intercept, record and subsequently transmit the outcome of interception of telecommunications to the issuing State.</p>
DK or IE as issuing state	<p>1. Interception of telecommunication is allowed in Polish jurisdiction upon the request of issuing state, in accordance with Article 237 paragraph 3-4 Polish Code of Criminal Procedure and in the light of Article 241 Polish Code of Criminal Procedure under the same conditions and with regard to the same types of crimes as in case of Member States applying the EIO. The surveillance and recording of telephone conversations and interception of other forms of telecommunication may be carried out for a period not exceeding 3 months, with a possibility of extension, in particularly justified cases, for a period no longer than further 3 months.</p> <p>However, GPS tracking is legally permissible, as mentioned before (in point a of this questionnaire), in relation to the types (groups) of crimes and under the conditions specified in the article 19 (1) in conjunction with article 19b (1) Act on the Police of 6 April 1990²⁴.</p> <p>2. The competent authority is the circuit public prosecutor having territorial jurisdiction, while the role of contact points shall be fulfilled by the Voivodeship Police Commanders ('Komendant Wojewódzki Policji') having territorial jurisdiction. The notification may also be sent to the International Police Cooperation Bureau of the National Police Headquarters acting as National Bureau of Interpol.</p> <p>3. It is not technically possible to channel the intercepted telecommunication to the issuing state in real-time. However, it is possible to intercept, record and subsequently transmit the outcome of interception of telecommunications to the issuing State.</p>
Issuing state is a third State	<p>1. Interception of telecommunication is allowed in Polish jurisdiction upon the request of issuing state, in accordance with Article 237 paragraph 3-4 Polish Code of Criminal Procedure and in the light of article 241 Polish Code of Criminal Procedure under the same conditions and with regard to the same types of crimes as in case of Member States applying the EIO and also Denmark and Ireland. The surveillance and recording of telephone conversations and interception of other forms of telecommunication may be carried out for a period not exceeding 3 months, with a possibility of extension, in particularly justified cases, for a period no longer than further 3 months</p> <p>2. Request for international legal assistance shall be sent to the circuit prosecutor’s office having the territorial jurisdiction, provided that such possibility of direct communication between judicial authorities has been foreseen by the bilateral agreement or multilateral convention on mutual legal assistance in criminal matters, binding in legal relations between Poland and the issuing third State. If the such multilateral convention or bilateral agreement establish communication only between central authorities, request for legal assistance shall be forwarded to the Polish Ministry of Justice or to the National Prosecutor’s Office (Bureau of International Legal Cooperation), if the latter authority has been indicated in particular international treaty as a central authority on the Polish side. Interception of telecommunication may also be carried out within special investigative techniques on the basis of sectoral conventions, binding in legal relations with third country.</p> <p>3. It is not technically possible to channel the intercepted telecommunication to the issuing state in real-time. However, it is possible to intercept, record and subsequently transmit the outcome of interception of telecommunications to the issuing State.</p>

²⁴ See also footnotes 17 and 18

Scope of Article 31 EIO Directive and use of Annex C

1. Pursuant to Article 589zt paragraph 1 Polish Code of Criminal Procedure, notification by a body of another Member State of the European Union (instead of an EIO), of the intention to conduct or of the completion of the interception of telecommunication on the Polish territory is limited only to surveillance and recording of the content of telephone conversations. For interception of telecommunication of any other types by another Member State on the Polish territory, Annex C. will not be deemed as sufficient.
2. Circuit public prosecutor having territorial jurisdiction is competent authority to receive an Annex C notification. In case it is not possible to establish territorial jurisdiction, the EIO may be sent to the central authority – National Prosecutor's Office, Bureau of International Legal Cooperation.
3. Accepted language for Annex C notifications is only Polish, also when urgency is given.


4.1.22. Portugal (PT)

PORTUGAL 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Annex C EIO DIR 2. GPS tracking, according to article 6 nº1 of Law 5/2002, is admissible when it is necessary for the investigation of the crimes listed in article 1 of the same law. This measure, during the investigation, has to be authorised by the Examining Judge, upon the request of the Public Prosecutor. 3. The Central Department for International Cooperation of the Judiciary Police and the Department of Investigation and Prosecution of Lisbon are the competent entities to receive the notification (art. 5 and 6, of Law 88/2017).
DK or IE as issuing state	<ol style="list-style-type: none"> 1. Art 20 of the 2000 MLA Convention 2. GPS tracking, according to article 6 nº1 of Law 5/2002, is admissible when it is necessary for the investigation of the crimes listed in article 1 of the same law. This measure, during the investigation, has to be authorised by the Examining Judge, upon the request of the Public Prosecutor. 3. Examining Judge, upon the request of the Public Prosecution Service.
Issuing state is a third State	<ol style="list-style-type: none"> 1. LoR 2. GPS tracking, according to article 6 nº1 of Law 5/2002, is admissible when it is necessary for the investigation of the crimes listed in article 1 of the same law. This measure, during the investigation, has to be authorised by the Examining Judge, upon the request of the Public Prosecutor. 3. Examining Judge, upon the request of the Public Prosecution Service.
Bugging of a car	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Annex C EIO DIR 2. Bugging of a car, according to article 6 nº1 of Law 5/2002, is admissible when it is necessary for the investigation of the crimes listed in article 1 of the same law. This measure, during the investigation, has to be authorised by the Examining Judge, upon the request of the Public Prosecutor. 3. The Central Department for International Cooperation of the Judiciary Police and the Department of Investigation and Prosecution of Lisbon are the competent entities to receive the notification (art. 5 and 6, of Law 88/2017).
DK or IE as issuing state	<ol style="list-style-type: none"> 1. Art 20 of the 2000 MLA Convention 2. Bugging of a car, according to article 6 nº1 of Law 5/2002, is admissible when it is necessary for the investigation of the crimes listed in article 1 of the same law. 3. Examining Judge, upon the request of the Public Prosecution Service.

Issuing state is a third State	<ol style="list-style-type: none"> 1. LoR 2. Bugging of a car, according to article 6 n°1 of Law 5/2002, is admissible when it is necessary for the investigation of the crimes listed in article 1 of the same law. 3. Examining Judge, upon the request of the Public Prosecution Service.
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. A Trojan insertion can take place via a “technical covert action”. 2. It has to be authorized only during the inquiry, by an Examining Judge, upon the request of the Public Prosecution Service, for a catalogue of criminal offences. 3. 4. Annex A 5. Examining Judge, upon the request of the Public Prosecution Service.
DK or IE as issuing state	<ol style="list-style-type: none"> 1. A Trojan insertion can take place via a “technical covert action”. 2. It has to be authorized only during the inquiry, by an Examining Judge, upon the request of the Public Prosecution Service, for a catalogue of criminal offences. 3. 4. Art 14 of the 2000 MLA Convention 5. Examining Judge, upon the request of the Public Prosecution Service.
Issuing state is a third State	<ol style="list-style-type: none"> 1. A Trojan insertion can take place via a “technical covert action”. 2. It has to be authorized only during the inquiry, by an Examining Judge, upon the request of the Public Prosecution Service, for a catalogue of criminal offences. 3. 4. LoR 5. Examining Judge, upon the request of the Public Prosecution Service.
Audio/video surveillance in a private place	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Yes. 2. Again, it has to be authorized only during the inquiry, by an Examining Judge, upon the request of the Public Prosecution Service, for a catalogue of criminal offences.
DK or IE as issuing state	<ol style="list-style-type: none"> 1. Yes. 2. Again, it has to be authorized only during the inquiry, by an Examining Judge, upon the request of the Public Prosecution Service, for a catalogue of criminal offences.
Issuing state is a third State	<ol style="list-style-type: none"> 1. Yes. 2. Again, it has to be authorized only during the inquiry, by an Examining Judge, upon the request of the Public Prosecution Service, for a catalogue of criminal offences.
Interception of telecommunication abroad	

Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Interception and tape recording of telephone conversations or communications may only be authorized during the inquiry where there are grounds for believing that this step is indispensable for the discovery of the truth or that the evidence would, by any other means, be impossible or very hard to collect. Such authorization shall be granted by means of a reasoned order issued by the Examining Judge and upon the request of the Public Prosecution Service, as regards a catalogue of criminal offences. The interception and the recording of any conversations or communications are authorised for a maximum time-limit of three months, renewable for equal periods, provided that the respective requirements for admissibility have been met. 2. Examining Judge, upon the request of the Public Prosecution Service. 3. according to the Portuguese law it is possible, but in practice, it is not feasible.
DK or IE as issuing state	<ol style="list-style-type: none"> 1. Interception and tape recording of telephone conversations or communications may only be authorized during the inquiry where there are grounds for believing that this step is indispensable for the discovery of the truth or that the evidence would, by any other means, be impossible or very hard to collect. Such authorization shall be granted by means of a reasoned order issued by the Examining Judge and upon the request of the Public Prosecution Service, as regards a catalogue of criminal offences. The interception and the recording of any conversations or communications are authorised for a maximum time-limit of three months, renewable for equal periods, provided that the respective requirements for admissibility have been met. 2. Examining Judge, upon the request of the Public Prosecution Service. 3. Not applicable.
Issuing state is a third State	<ol style="list-style-type: none"> 1. Interception and tape recording of telephone conversations or communications may only be authorized during the inquiry where there are grounds for believing that this step is indispensable for the discovery of the truth or that the evidence would, by any other means, be impossible or very hard to collect. Such authorization shall be granted by means of a reasoned order issued by the Examining Judge and upon the request of the Public Prosecution Service, as regards a catalogue of criminal offences. The interception and the recording of any conversations or communications are authorised for a maximum time-limit of three months, renewable for equal periods, provided that the respective requirements for admissibility have been met. 2. Examining Judge, upon the request of the Public Prosecution Service. 3. Not applicable.
Scope of Article 31 EIO Directive and use of Annex C	
<ol style="list-style-type: none"> 1. Other kinds of data collection without the need of technical assistance. 2. The Central Department for International Cooperation of the Judiciary Police and the Department of Investigation and Prosecution of Lisbon are the competent entities to receive the notification (art. 5 and 6, of Law 88/2017). 3. Portuguese (and Spanish only for EIOs received from Spain). 	

4.1.23. Romania (RO)

ROMANIA 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Bugging of a car	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	

Audio/video surveillance in a private place	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Interception of telecommunication abroad	
Issuing state applies EIO DIR	
DK or IE as issuing state	
Issuing state is a third State	
Scope of Article 31 EIO Directive and use of Annex C	
Relevant documents	

4.1.24. Slovak Republic (SK)

SLOVAK REPUBLIC	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	<p>1. Other: In the case of EU Member States that have implemented Directive 2014/41 / EU, if they send the EIO with a request for cross-border GPS tracking without technical support from the Slovak Republic, the EIO will be assessed by the Slovak judicial authorities as a request for legal assistance under the relevant international treaties governing cross-border surveillance. This is because, in accordance with point 9 of the Preamble to the Directive, the Slovak Republic does not apply the EIO to cross-border surveillance.</p> <p>2. According to the Slovak law (Section 113 of the Criminal Procedure Code), the surveillance of persons and items may be performed in the criminal proceedings on an intentional criminal offence if it can reasonably be assumed that it will reveal facts relevant to the criminal proceedings. The request has to be delivered in advance due to the need to issue an order, which is issued by the presiding judge, before the commencement of the criminal prosecution, or in the preliminary proceeding by the public prosecutor, who shall issue a warrant for surveillance in writing. Special legislation applies in the Czech Republic.</p> <p>In the case of the Czech Republic, where a bilateral agreement applies, prior consent to cross-border GPS tracking is not required. However, the consent of the competent authority (Bratislava Regional Prosecutor's Office) is required to use the result of the cross-border surveillance as an evidence. In other cases, national law regulates the situation where the case cannot be postponed and the written order cannot be obtained in advance. In this case, the order must be issued within 24 hours, otherwise the tracking must be terminated. The order allows tracking for a maximum of six months, if necessary, it can be extended in writing for another six months, even repeatedly. If the tracking lasts longer than twelve months, the order is issued by the judge for the preliminary proceeding.</p> <p>3. In the case of cross-border tracking using the GPS system without technical assistance of the executing state on the basis of a request for legal assistance, the prosecution office in charge is the district prosecutor's office in the place in which the state border of the Slovak Republic is likely to be crossed. If the requesting state will send the EIO, the competent regional prosecutor's office in charge will assess the EIO as request for legal assistance and submit the request to the competent district public prosecutor's office for execution.</p>
DK or IE as issuing state	<p>1. A request for legal assistance under the European Convention on Mutual Assistance in Criminal Matters, as amended by the Second Additional Protocol, is required.</p> <p>2. The same conditions as in the case of an EU Member State (the nature of the crime is assessed, it is necessary to ensure that a national order is issued).</p> <p>3. The prosecution office in charge is the district prosecutor's office in the place in which the state border of the Slovak Republic is likely to be crossed.</p>
Issuing state is a third State	<p>1. In the case of third States, which are the parties to the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters and the UN Conventions, a request for legal assistance must be sent in accordance with those conventions.</p> <p>2. The same conditions as in the case of an EU Member State</p> <p>3. The prosecution office in charge is the district prosecutor's office in the place in which the state border of the Slovak Republic is likely to be crossed.</p>


Bugging of a car	
Issuing state applies EIO DIR	<p>1. Annex A EIO DIR</p> <p>2. According to the Slovak law (Section 114 of the Criminal Procedure Code), in criminal proceedings for an intentional criminal offence, for which the law stipulates a prison sentence with an upper penalty limit exceeding three years, corruption or another intentional criminal offence, the performance of which is bound by an international treaty, video, audio or audio-visual recording may be carried out on the ground of issued order, if it may be reasonably assumed that facts important to the criminal proceedings will be so revealed.</p> <p>The order for the preparation of the video, audio or audiovisual recordings shall be issued in writing by the presiding judge, before the onset of the criminal prosecution or in the preliminary hearing, upon the petition of the public prosecutor, by the judge for the preliminary hearing. The period during which the preparation of video, audio or audio-visual recordings shall be performed must be determined; this period may be up to six months. The person who issued a warrant for the preparation of the video, audio or audio-visual recordings may extend its duration in writing for no more than two months, and they may even do so repeatedly. If it is a matter that cannot be deferred, the public prosecutor may, before the commencement of the criminal prosecution and in the preliminary hearing, issue the warrant; such a warrant must be confirmed by the judge for the preliminary hearing no later than 24 hours from its issue, otherwise it shall expire.</p> <p>3. The competent authority to ensure the implementation of the required investigative measure is the Regional prosecutor's office, in the district in which the "intercepted" vehicle is likely to cross the state border of the Slovak Republic.</p>
DK or IE as issuing state	<p>1. A request for legal aid is required under the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union (MLA 2000).</p> <p>2. Same as in the case of an EU Member State (the nature of the crime is assessed, it is necessary to ensure that a national order is issued).</p> <p>3. The competent authority to ensure the implementation of the required investigative measure is the District prosecutor's office, in the place in which the "intercepted" vehicle is likely to cross the state border of the Slovak Republic.</p>
Issuing state is a third State	<p>1. In the case of third countries which have ratified the European Convention on Mutual Assistance in Criminal Matters or the UN Conventions, a request for legal aid must be sent in accordance with those conventions. In the absence of an international agreement with a third country, a procedure in accordance with the principle of reciprocity is not excluded</p> <p>2. Same as in the case of an EU Member State (the nature of the crime is assessed, it is necessary to ensure that a national order is issued).</p> <p>3. The competent authority to ensure the implementation of the required investigative measure is the District prosecutor's office, in the place in which the "intercepted" vehicle is likely to cross the state border of the Slovak Republic.</p>
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	<p>1. Yes, in accordance with national law, it is possible to secure data that is transmitted in real time via a computer system as part of an investigative measure consisting in interception and recording of telecommunications operations.</p> <p>2. In criminal proceedings on a crime, corruption, criminal offences of extremism, a criminal offence of abuse of authority of a public official, a criminal offence of money laundering under Section 233 and 234 The Penal Code or another intentional criminal offence, the performance of which is bound by an international treaty, a warrant for the interception and recording of</p>

	<p>telecommunication operations may be issued if it may be reasonably assumed that it will aid in obtaining all the facts relevant to the criminal proceedings. The warrant for the interception and recording of telecommunication operations shall be issued by the presiding judge, before the onset of the criminal prosecution, or in the preliminary hearing upon the petition of the public prosecutor, by the judge for the preliminary hearing. The interception and recording period may last up to six months. In the preliminary hearing upon the petition of the public prosecutor, this period may be extended by the judge for the preliminary hearing, but always by only two months although it can be done so repeatedly.</p> <p>3. N/A</p> <p>4. Annex C - Notification under Article 31 of the EIO Directive. The notification must be sent without undue delay after the issuing authority learns that the intercepted person is, will be or was in the territory of the Slovak Republic during the interception.</p> <p>5. The Bratislava I District Court is competent for granting consent to cross-border interception of telecommunications operations, which will notify the issuing authority of the granting of consent within 96 hours of receiving notification of the interception.</p>
DK or IE as issuing state	<p>1. the same as above</p> <p>2. the same as above</p> <p>3. the same as above</p> <p>4. Notification under Article 20 of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 29 May 2000 must be sent.</p> <p>5. The relevant contact point for receiving notifications of cross-border interception is, in accordance with the declaration of the Slovak Republic to the Convention, the Presidium of the Police Force, the Office of International Police Cooperation, the Interpol National Headquarters. The district prosecutor's office is responsible for executing the application for legal aid.</p>
Issuing state is a third State	<p>1. the same as above</p> <p>2. the same as above</p> <p>3. the same as above</p> <p>4. In the case of third countries which have ratified the European Convention on Mutual Assistance in Criminal Matters or the UN Conventions, a request for legal aid must be sent in accordance with those conventions. In the absence of an international agreement with a third country, a procedure in accordance with the principle of reciprocity is not excluded.</p> <p>5. The performance of the required legal aid act will be ensured by the district prosecutor's office.</p>
Audio/video surveillance in a private place	
Issuing state applies EIO DIR	<p>1. Yes, Slovak legislation allows for the production of video, audio or video-audio records associated with direct entry into the dwelling. The said investigative act can be requested through the EIO.</p> <p>2. This investigative act is admissible only in criminal proceedings on crime, corruption, the crime of abuse of power by a public official, the crime of money laundering or another intentional criminal offense, which is bound by an international agreement, and only with the prior consent of the judge, before the commencement of criminal proceedings or in the preparatory proceedings of the judge for the preliminary proceedings. The regional prosecutor's office is in charge of the EIO execution.</p> <p>3. N/A</p>

DK or IE as issuing state	<p>1. Yes</p> <p>2. A request for legal assistance under the European Convention on Mutual Assistance in Criminal Matters is required. The district prosecutor's office in the place in which the act is to be performed is competent to execute such a request.</p> <p>3. N/A</p>
Issuing state is a third State	<p>1. Yes</p> <p>2. In the case of third countries which have ratified the European Convention on Mutual Assistance in Criminal Matters or the UN Conventions, a request for legal aid must be sent in accordance with those conventions. In the absence of an international agreement with a third country, a procedure in accordance with the principle of reciprocity is not excluded. The performance of the required action shall be ensured by the district prosecutor's office in the place in which the action is to be performed.</p> <p>3. N/A</p>
Interception of telecommunication abroad	
Issuing state applies EIO DIR	<p>1. According to the Section 115 of the Criminal Procedure Code, In criminal proceedings on a crime, corruption, criminal offences of extremism, a criminal offence of abuse of authority of a public official, a criminal offence of money laundering under Section 233 and 234 The Penal Code or another intentional criminal offence, the performance of which is bound by an international treaty, a warrant for the interception and recording of telecommunication operations may be issued if it may be reasonably assumed that it will aid in obtaining all the facts relevant to the criminal proceedings. The warrant may be issued if the purpose pursued may not be attained otherwise or if its attainment in another manner would be considerably hindered. The interception and recording period may last up to six months. In the preliminary hearing upon the petition of the public prosecutor, this period may be extended by the judge for the preliminary hearing, but always by only two months although it can be done so repeatedly. If it is a matter that cannot be deferred and the interception and recording of telecommunication operations is not associated with entry into a dwelling and a written warrant from the judge for the preliminary hearing cannot be obtained in advance, the warrant may be issued before the commencement of the criminal prosecution or in the preliminary hearing by the public prosecutor; the warrant must be confirmed by the judge for the preliminary hearing no later than 24 hours from its issue, otherwise it shall expire.</p> <p>2. The EIO needs to be delivered to the Bratislava Regional Prosecutor's Office, which will submit a proposal for the issuance of the order to the competent court.</p> <p>3. The national law presupposes the possibility that the European investigation order will be executed by direct access to the telecommunications operation in the Slovak Republic from the state of origin.</p>
DK or IE as issuing state	<p>1. the same as above</p> <p>2. The District Prosecutor's Office will be in charge of the request for legal aid issued on the grounds of the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union of 29 May 2000.</p> <p>3. the same as above</p>
Issuing state is a third State	<p>1. the same as above</p> <p>2. In the case of third countries which have ratified the European Convention on Mutual Assistance in Criminal Matters or the UN Conventions, a request for legal aid must be sent in accordance with those conventions. In the absence of an international agreement with a third country, a procedure in accordance with the principle of reciprocity is not excluded. The</p>

	<p>performance of the required action shall be ensured by the district prosecutor's office in the place in which the action is to be performed.</p> <p>3. the same as above</p>
<p align="center">Scope of Article 31 EIO Directive and use of Annex C</p>	
<p>1. Notification pursuant to Article 31 of the EIO Directive on interception of telecommunications operations may be sent only in cases falling under the legislation of Section 115 of the Criminal Procedure Code.</p> <p>2. In accordance with the Slovak legislation, the District Court of Bratislava I has jurisdiction to decide on the granting of consent to the interception and recording of telecommunications operations. Consent to the interception or its continuation may be granted only if the conditions specified in § 115 of the Criminal Procedure Code are met.</p> <p>3. The Slovak Republic accepts Annex C of the EIO Directive prepared in the Slovak language, and in the case of the Czech Republic also in the Czech language.</p>	

4.1.25. Slovenia (SI)


<div style="text-align: center;"> SLOVENIA  </div>	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	<p>1. Annex C EIO DIR</p> <p>2. The installation of GPS tracking device falls under the covert surveillance measure that is regulated in art. 149A of Criminal Procedure Act (hereinafter: CPA). The measure is ordered by a written order by the investigating judge on a written motion of the state prosecutor for specific criminal offences, defined in Art. 149a, paragraph 4:</p> <p>1) criminal offences punishable by a sentence of imprisonment of five or more years prescribed by an Act;</p> <p>2) criminal offence of abduction under Article 134, solicitation of persons under fifteen years of age for sexual purposes under Article 173a, exploitation through prostitution under Article 175, presentation, manufacture, possession and distribution of pornographic material under Article 176, illicit manufacture and trade in narcotic drugs, illicit substances in sport and illicit drug precursors under Article 186, facilitating the consumption of narcotic drugs or illicit substances in sport under Article 187, extortion and blackmail under Article 213, abuse of insider information under Article 238, unauthorised acceptance of gifts under Article 241, money laundering under Article 245, smuggling under Article 250, defrauding of public funds under Article 257a, acceptance of bribes under Article 261, giving bribes under Article 262, acceptance of proceeds of unlawful intermediation under Article 263, giving of gifts for unlawful intermediation under Article 264, criminal association under Article 294, illegal manufacturing of and trafficking in weapons or explosives under Article 307, and unlawful management of nuclear and other hazardous radioactive substances under Article 334, unlawful deprivation of liberty under Article 133, stalking under Article 134a, threats under Article 135, misuse of personal data under paragraphs three, four, five and six of Article 143, undeclared employment under paragraphs two and three of Article 199, fraud under paragraphs one, three and four of Article 211, concealment under paragraphs one, two and three of Article 217, fraud to the detriment of the European Union under Article 229, attack on information systems under paragraphs two, three and four of Article 221, forgery or destruction of business documents under Article 235, disclosure and unauthorised acquisition of trade secrets under paragraphs one, two and three of Article 236, abuse of information system under Article 237, abuse of position or trust in business activity under Article 240, forging of documents under Article 251, special case of forging of documents under Article 252, abuse of office or official rights under Article 257, the disclosure of classified information under Article 260, public incitement to hatred, violence and intolerance under Article 297, prohibition of illegal crossing of state border or territory under Article 308, pollution of drinking water under paragraphs one, three, four and six of Article 336, tainting of foodstuffs or fodder under paragraphs one, three, four and six of Article 337, and the torture of animals under paragraphs two, three and four of Article 341 of the Criminal Code;</p> <p>3) the criminal offence of assisting the perpetrator after committing the criminal offence under Article 282 of the Criminal Code, including against the persons referred to in paragraph four of Article 282 of the Criminal Code - for the offences not referred to in this paragraph.</p> <p>3. An investigating judge of competent District Court issues such order on a written motion of a state prosecutor.</p>

DK or IE as issuing state	<ol style="list-style-type: none"> 1. Notification under Art. 20(2) of MLA Convention. No other bilateral agreement exists between SI and DK/IE. 2. Please see the answer above. 3. Competent investigating judge.
Issuing state is a third State	<ol style="list-style-type: none"> 1. MLA request 2. Please see the answer above 3. Competent District Court, but the MLA Request has to be sent through MoJ. Slovenia has several bilateral agreements with third states concerning judicial cooperation in criminal matters. In case no such agreement exists, it is possible to use UN Conventions and Conventions of CoE.
Bugging of a car	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Annex C EIO DIR 2. This measure is regulated in Art. 151 of CPA, may be ordered by investigating judge on the state prosecutor's written motion and only in connection with following criminal offences: <ul style="list-style-type: none"> - criminal offences against the security of the Republic of Slovenia and its constitutional order, and crimes against humanity and international law punishable by a sentence of imprisonment of five or more years prescribed by an Act; - solicitation of persons under fifteen years of age for sexual purposes under Article 173a, exploitation through prostitution under Article 175, presentation, manufacture, possession and distribution of pornographic material under Article 176, illicit manufacture and trade in narcotic drugs, illicit substances in sport and illicit drug precursors under Article 186, abuse of insider information under Article 238, unauthorised acceptance of gifts under Article 241, defrauding of public funds under Article 257a, acceptance of bribes under Article 261, giving bribes under Article 262, acceptance of proceeds of unlawful intermediation under Article 263, giving of gifts for unlawful intermediation under Article 264, criminal association under Article 294, illegal manufacturing of and trafficking in weapons or explosives under Article 307, and unlawful management of nuclear and other hazardous radioactive substances under Article 334 of the Criminal Code; - other criminal offences punishable by a sentence of imprisonment of eight or more years prescribed by an Act. 3. Competent District Court
DK or IE as issuing state	<ol style="list-style-type: none"> 1. Notification in accordance with Art 20 of the 2000 MLA Convention. No other bilateral agreement exists between SI and DK/IE. 2. See the answer above 3. Competent District Court
Issuing state is a third State	<ol style="list-style-type: none"> 1. MLA Request 2. See the answer above 3. Competent District Court, but the MLA Request has to be sent through MoJ. Slovenia has several bilateral agreements with third states concerning judicial cooperation in criminal matters. In case no such agreement exists, it is possible to use UN Conventions and Conventions of CoE.

Surveillance through Trojan horse software	
Issuing state applies EIO DIR	1. In Slovenia we do not have either legal provision that would allow for the use of Trojan horse software or other admissible ways of attacking encryption. There were efforts to include the use of Trojan horse software into the amendments of CPA in the past but such proposals have never been endorsed by the legislator.
DK or IE as issuing state	-
Issuing state is a third State	-
Audio/video surveillance in a private place	
Issuing state applies EIO DIR	1. Yes. Issuing state shall send Annex A 2. This measure is regulated in the Art 151 of CPA – the same regime as for bugging of a car under b) applies.
DK or IE as issuing state	1. LoR according to The 2000 MLA Convention is needed. No other bilateral agreement exists between SI and DK/IE. 2. Please see answer above
Issuing state is a third State	1. MLA Request needed. Slovenia has several bilateral agreements with third states concerning judicial cooperation in criminal matters. In case no such agreement exists, it is possible to use UN Conventions and Conventions of CoE. 2. Please see answer above
Interception of telecommunication abroad	
Issuing state applies EIO DIR	1. This measure is regulated in the Art 150 of CPA and it may be ordered by the investigating judge upon written motion of the state prosecutor. Reasonable grounds for the suspicion shall exist that a particular person has committed, is committing or is preparing or organising the commission of any of the pre-defined criminal offences. At the same time, a reasonable suspicion shall exist that a particular means of communication or computer system is used or will be used by this person for communication relating to this criminal offence, whereby it may be reasonably concluded that evidence could not be collected by applying other measures or that their collection could threaten human life or health. Pre-defined criminal offences include: 1) criminal offences against the security of the Republic of Slovenia and its constitutional order, and crimes against humanity and international law punishable by a sentence of imprisonment of five or more years prescribed by an Act; 2) a criminal offence of abduction under Article 134, solicitation of persons under fifteen years of age for sexual purposes under Article 173a, exploitation through prostitution under Article 175, presentation, manufacture, possession and distribution of pornographic material under Article 176, illicit manufacture and trade in narcotic drugs, illicit substances in sport and illicit drug precursors under Article 186, facilitating the consumption of narcotic drugs

	<p>or illicit substances in sport under Article 187, extortion and blackmail under Article 213, abuse of insider information under Article 238, unauthorised acceptance of gifts under Article 241, money laundering under Article 245, smuggling under Article 250, defrauding of public funds under Article 257a, acceptance of bribes under Article 261, giving bribes under Article 262, acceptance of proceeds of unlawful intermediation under Article 263, giving of gifts for unlawful intermediation under Article 264, criminal association under Article 294, illegal manufacturing of and trafficking in weapons or explosives under Article 307, and unlawful management of nuclear and other hazardous radioactive substances under Article 334 of the Criminal Code;</p> <p>3) other criminal offences punishable by a sentence of imprisonment of eight or more years prescribed by an Act.</p> <p>Concerning the maximum duration the measure:</p> <p>The implementation of the measure may not exceed one month. However, its duration may be extended by one month at a time for valid reasons. The maximum duration may not exceed a total of six months, and of the measures referred to in the preceding Article a total of three months.</p> <p>2. The police must carry out the measure in such a way as to minimise the interference with the rights of the persons who are not suspects.</p> <p>3. According to the fact that SI Police uses dedicated software for the interception of communication it is not technically possible to channel the intercepted telecommunication to the issuing state in real-time. Investigators produce transcripts and reports with their observations, save them on a storage medium and hand it over to a competent authority.</p>
DK or IE as issuing state	<p>1. LoR according to The 2000 MLA Convention is needed. No other bilateral agreement exists between SI and DK/IE.</p> <p>2. Please see the answer above</p> <p>3. Please see the answer above</p>
Issuing state is a third State	<p>1. MLA Request needed. Slovenia has several bilateral agreements with third states concerning judicial cooperation in criminal matters. In case no such agreement exists, it is possible to use UN Conventions and Conventions of CoE.</p> <p>2. Please see the answer above</p> <p>3. Please see the answer above. Slovenia has several bilateral agreements with third states concerning judicial cooperation in criminal matters. In case no such agreement exists, it is possible to use UN Conventions and Conventions of CoE.</p>
Scope of Article 31 EIO Directive and use of Annex C	
<p>1. Currently there are no other types of interception of telecommunication.</p> <p>2. The competent authority to receive an Annex C notification may be Competent court or Competent State Prosecutor's Office – depends on the competence of the authority to order a specific measure.</p> <p>3. The competent national authorities shall receive requests made by foreign competent authorities in Slovenian or English.</p>	

4.1.26. Spain (ES)


<div> <div>SPAIN</div>  </div>	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Annex A EIO DIR; executing authorities may also accept Annex C. Actually it is the most usual way 2. For any crimes, including ex-post notifications. 3. Prosecutor's Office (unless the territorial scope is very limited and defined, it is normally a nation-wide competent Office –Audiencia Nacional PPO, Antidrug PPO, General prosecutors Office).
DK or IE as issuing state	<ol style="list-style-type: none"> 1. Either a LoR or a notification under art 20 Convention 2000 would be acceptable 2. For any crimes, including ex-post notifications 3. Prosecutor's Office (as above) and also any territorially competent investigative court that might be addressed by the issuing authority.
Issuing state is a third State	<ol style="list-style-type: none"> 1. LoR (modalities may vary depending on the applicable legal framework) 2. For any crimes, including ex-post notifications 3. via Central Authority (MoJ) unless third countries are covered by Schengen where the reply given in the previous num 3 would apply.
Bugging of a car	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Annex A EIO DIR; executing authorities may also accept Annex C 2. Ex-post notifications could be acceptable, but the investigation must concern one of the following crimes (article 579.1 Criminal procedure Act): <ol style="list-style-type: none"> a. Intentional crimes punished with a maximum sentence of, at least, three years imprisonment. b. Crimes committed as a member of a criminal group or organisation. c. Crimes of terrorism.. 3. Prosecutor's Office (unless the territorial scope is very limited and defined, it is normally a nation-wide competent Office –Audiencia Nacional PPO, Antidrug PPO, General prosecutors Office). In this case authorisation will have to be given by a judge so the execution of the EIO will have to be sent by the PPO to an investigative judge.
DK or IE as issuing state	<ol style="list-style-type: none"> 1. Either a LoR or a notification under art 20 Convention 2000 would be acceptable 2. As above 3. As addressees, Prosecutor's Office (as above) and also any territorially competent investigative court that might be addressed by the issuing authority. Authorisation will have to be given by a judge.

Issuing state is a third State	<ol style="list-style-type: none"> 1. LoR (modalities may vary depending on the applicable legal framework) 2. As above 3. via Central Authority (MoJ) unless as regards third countries covered by Schengen where the reply given in the previous num 3 would apply.
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Yes 2. according to Article 588 septies a Criminal Procedure Act. <ol style="list-style-type: none"> 1) The competent magistrate may authorise the use of identification data and codes, as well as the installation of software, allowing a remote and telematics examination, without the knowledge of the user or the owner, of the contents of a computer, electronic device, computer system, mass storage instrument or database, provided it is aimed at the investigation of any of the following criminal offences: <ol style="list-style-type: none"> a) Offences committed within criminal organisations b) Terrorist offences c) Offences committed against children or persons with legally modified capacity. d) Offences against the Constitution, treason and offences regarding national defence e) Offences committed through computer tools or by any other information technology, telecommunication or communication service. 2) The judicial decision authorizing the search shall specify: <ol style="list-style-type: none"> f) The computers, electronic devices, computer tools or parts of them, data storage media or databases, data or other digital contents that are the object of the measure g) The extent of the measure, the way on which access and capture of data or files relevant to the case shall be carried out and the software that shall be used to control de information. h) The officers designated to conduct the measure i) Where appropriate, the authorisation to make and keep copies of the computer data. j) The measures required to preserve the integrity of all data stored, as well as the inaccessibility or suppression of such data from the computer system accessed. 3) When the officers carrying out the remote search have reasons to believe that the information sought is stored in another computer system or in part of it, they may inform the magistrate who may authorise an extension of the examination terms. 3. N/A 4. Annex A EIO 5. Competent investigative judge.
DK or IE as issuing state	<ol style="list-style-type: none"> 1. Yes 2. As above 3. N/A

	4. LoR 5. As above
Issuing state is a third State	1. Yes 2. As above 3. N/A 4. LoR sent though MoJ (except for Schengen third countries) 5. As above
Audio/video surveillance in a private place	
Issuing state applies EIO DIR	1. Yes as per article 588 quarter a Criminal Procedure Act 2. According to article 588 quarter b, this measure can only be adopted by decision of the judicial authority (investigative judge) if the use of the technical devices are associated with communications which may take place in one or several specific encounters of the party under investigation with other people and which were foreseeable due to evidence arising from the investigation. They may only be authorised where the following requirements are met: a) That the facts under investigation constitute one of the following crimes: <ol style="list-style-type: none"> 1. Intentional crimes punished with a maximum sentence of, at least, three years imprisonment. 2. Crimes committed as a member of a criminal group or organisation. 3. Crimes of terrorism. b) That it can be reasonably foreseen that the use of the devices will provide essential data, with evidentiary relevance for clarification of the events and identification of their perpetrator. 3. N/A
DK or IE as issuing state	1. see above 2. see above 3. see above
Issuing state is a third State	1. see above 2. see above 3. see above
Interception of telecommunication abroad	
Issuing state applies EIO DIR	1. The authorization for the interception of telephone and telematic communications can only be granted when the inquiry focuses on some of the offences referred to in Article 579.1 Criminal Procedure Act (see above reply to b)1) or offences committed through software tools or any other information or communication technology or communication service; only on devices used by the suspect (exceptionally, also those used by the victim); duration will be of three months, extendable for successive periods of the same duration up to the maximum period of eighteen months.

	<p>2. Investigating judge (in cases of urgency in terrorism cases a provisional decision can be taken by the MoI and notified within 24 hours to the judge for validation)</p> <p>3. No</p>
DK or IE as issuing state	<p>1. as above</p> <p>2. as above</p> <p>3. as above</p>
Issuing state is a third State	<p>1. as above</p> <p>2. as above</p> <p>3. as above</p>
Scope of Article 31 EIO Directive and use of Annex C	
<p>1. No</p> <p>2. Prosecutor's Offices (if necessary they will be forward to a judge)</p> <p>3. Spanish and Portuguese, according to the general declaration made to article 5 of the EIO Directive.</p>	

4.1.27. Sweden (SE)

SWEDEN 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. In general, there is no need for an EIO/MLA. GPS tracking is considered to fall under the competence of the Law Enforcement Agencies. 2. GPS tracking is not regulated in the Swedish legislation. The general principles on proportionality and necessity apply. 3. Law Enforcement Agencies, that is the Police or Customs depending on the type of investigation.
DK or IE as issuing state	<ol style="list-style-type: none"> 1. Please see previous box above. 2. Please see previous box above. 3. Please see previous box above.
Issuing state is a third State	<ol style="list-style-type: none"> 1. Please see previous box above. 2. Please see previous box above. 3. Please see previous box above.
Bugging of a car	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Annex A EIO DIR 2. Secret audio surveillance of a vehicle is possible. There has to be a suspect and the measure must be of exceptional importance for the investigation. There must also be particular reasons to believe that the suspect will be using the vehicle. The measure should be necessary, proportionate and concern crimes where <ul style="list-style-type: none"> - the minimum sentence prescribed for the offence in question is four years imprisonment or - attempt, preparation or conspiracy to commit such an offence or - espionage of some specified kind or - any of some listed very serious offences such as inter alia THB, rape, other serious sexual offences, serious extortion, serious child pornography offences, serious drug trafficking if the offence is so severe that it will render more than four years imprisonment or - attempt, preparation or conspiracy to commit such an offence and the facts indicate that the deed will render more than four years imprisonment. 3. Permission is decided by the court after a request by the public prosecutor.
DK or IE as issuing state	<ol style="list-style-type: none"> 1. A request for mutual legal assistance in accordance with the 2000 MLA Convention. 2. Please see previous box above. 3. Please see previous box above.

Issuing state is a third State	<ol style="list-style-type: none"> 1. A request for mutual legal assistance. 2. Please see previous box above. 3. Please see previous box above.
Surveillance through Trojan horse software	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Yes, this is considered a legal form of interception according to Swedish legislation on secret data interception that is in force since April 1, 2020. This legislation makes it possible to secretly intercept data communication by technical means, inter alia by insertion of a so called 'Trojan Horse'. 2. The general conditions are that the <ul style="list-style-type: none"> - measure has to be proportionate and necessary, - the minimum sentence prescribed for the offence in question is two years imprisonment or concerns - attempt, preparation or conspiracy to commit such an offence, or - any other offence that is so severe it will render more than two years imprisonment or - the suspected offence is one of very serious crimes such as inter alia sabotage, arson, espionage, terrorism. 3. Not applicable. 4. Annex A. 5. Permission is decided by the court after a request by the public prosecutor. In urgent cases, the prosecutor can make a preliminary decision that has to be submitted to the court as soon as possible and can be revoked by the court.
DK or IE as issuing state	<ol style="list-style-type: none"> 1. Please see previous box above. 2. Please see previous box above. 3. Not applicable. 4. A request for mutual legal assistance in accordance with the 2000 MLA Convention. 5. Please see previous box above.
Issuing state is a third State	<ol style="list-style-type: none"> 1. Please see previous box above. 2. Please see previous box above. 3. Not applicable. 4. A request for mutual legal assistance. 5. Please see previous box above.
Audio/video surveillance in a private place	
Issuing state applies EIO DIR	<ol style="list-style-type: none"> 1. Secret audio surveillance and video surveillance of a private place is possible. 2. In relation to secret audio surveillance, there has to be a suspect and the measure must be of exceptional importance for the investigation. If the relevant area is the home of somebody else than the suspect, there must be exceptional reasons to believe that the suspect will visit it.

	<p>The measures should be necessary, proportionate and concern a crime where</p> <ul style="list-style-type: none"> - the minimum sentence prescribed for the offence in question is four years imprisonment or - attempt, preparation or conspiracy to commit such an offence or - espionage of some specified kind or - any of some listed very serious offences such as inter alia THB, rape, other serious sexual offences, serious extortion, serious child pornography offences, serious drug trafficking if the offence is so severe that it will render more than four years imprisonment or - attempt, preparation or conspiracy to commit such an offence and the facts indicate that the deed will render more than four years imprisonment. <p>Permission is decided by the court after a request by the public prosecutor. There is no possibility for the prosecutor to issue a preliminary decision on secret audio surveillance.</p> <p>In relation to secret video surveillance, there must be a suspect and the measure should be of exceptional importance for the investigation.</p> <p>The measure should be necessary, proportionate and concern a crime where</p> <ul style="list-style-type: none"> - the minimum sentence prescribed for the offence in question is two years imprisonment or - attempt, preparation or conspiracy to commit such an offence, or - any other offence that is so severe it will render more than two years imprisonment or - the suspected offence is one of very serious crimes such as inter alia sabotage, arson, espionage, terrorism. <p>The measure may also be allowed when there is no suspect and the measure is conducted in order to establish who the suspect is. The action can only target the scene of the crime and its surroundings. The measure must be of exceptional importance for the investigation.</p> <p>It is not permitted to enter a private home to apply technical equipment for video surveillance. From this follows that it is currently only permitted to carry out video surveillance of a private home if it can be done from the outside.</p> <p>Permission is decided by the court after a request by the public prosecutor. In urgent cases the prosecutor is allowed to issue a preliminary decision that has to be submitted to the court as soon as possible and can be revoked by the court.</p> <p>3. Not applicable.</p>
DK or IE as issuing state	<p>1. Please see previous box above.</p> <p>2. Please see previous box above.</p> <p>3. Not applicable.</p>
Issuing state is a third State	<p>1. Please see previous box above.</p> <p>2. Please see previous box above.</p> <p>3. Not applicable.</p>
Interception of telecommunication abroad	
Issuing state	<p>1. The conditions are the same as in a national case. This means for example the following.</p>

applies EIO DIR	<ul style="list-style-type: none"> - The duration should be no longer than necessary. The maximum period is one month with possibility of prolongation following a request by the prosecutor. - The investigation must concern a serious offence, i.e. the minimum penalty should be no less than two years of imprisonment or concern a specific list of crimes, e.g. sabotage, arson, terrorism and financing of terrorism. Also conspiracy, preparation and attempt to such crimes. Also any other crime than mentioned above if there are reasons to believe that the future possible penalty would be exceed two years of imprisonment. The measure should also be proportionate and necessary. - In urgent cases, the prosecutor is allowed to issue a preliminary decision that has to be submitted to the court as soon as possible and can be revoked by the court. <p>2. The competent authority is the district court in the area where the measure shall be executed. In urgent cases, the prosecutor is competent to take an interim decision awaiting the decision by the court.</p> <p>3. In practice, there is no such direct transmission today. In urgent cases, the material can be transmitted with about 30 – 60 minutes delay. To make this possible, there must be a well functioning contact between the technicians who operate the interception systems in each country since they have to establish a digital platform for the transmission.</p>
DK or IE as issuing state	<ol style="list-style-type: none"> 1. Please see above previous box. 2. Please see above previous box. 3. It is legally possible to transmit the intercepted communication in real-time in relation to DK and IE if it could be done under reassuring circumstances. But the practical limitations are the same as stated above.
Issuing state is a third State	<ol style="list-style-type: none"> 1. Please see above previous box. 2. Please see above previous box. 3. It is legally possible to transmit the intercepted communication in real-time in relation to Iceland and Norway if it could be done under reassuring circumstances. But the practical limitations are the same as stated above.
Scope of Article 31 EIO Directive and use of Annex C	
<ol style="list-style-type: none"> 1. Yes, Annex C can also be used for secret surveillance of telecommunication (e.g. who has used a phone and when it was used) and secret data interception (please see above, section c). 2. The Annex C should be received by the Swedish Prosecution Authority or the Swedish Economic Crime Authority depending on the crime type. The handling prosecutor makes an initial assessment of if there should be an objection and there after forwards it to the relevant district court for final assessment. 3. The Annex C notification should be in or translated to Swedish. In the particular case and depending on the circumstances, the competent authority may approve that the EIO is in English or translated to English. In practice, English is generally accepted in urgent cases. 	

4.2. Answers from Liaison Prosecutors

4.2.1. Albania (AL)


ALBANIA	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state EU Member State	<p>1. In accordance with the provisions of the European Convention on Mutual Assistance in Criminal Matters (MLA convention), and the Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, a LoR should be transmitted to the Albanian authorities (Ministry of Justice).</p> <p>In case of urgency, LoR may be addressed directly by the judicial authorities of the requesting Party to the judicial authorities of Albania. They shall be returned together with the relevant documents through the channels stipulated in paragraph 1 of Article 15 of the MLA Convention. Eurojust can be used as a channel of communication.</p> <p>2. Albanian legislation stipulates that the use of tracing the location shall be allowed only when there is an investigation being carried out for intent crimes, punishable with at least three years' imprisonment, in the maximum term.</p> <p>An interception may be authorised against:</p> <ul style="list-style-type: none"> a) a suspect for a criminal offence b) a person who is believed receiving or transmitting communications to the suspect person; c) a person who takes part in transactions with the suspect; c) a person whose surveillance may lead to the discovery of the location or the suspect identity. <p>3. The use of tracing the location is authorised by the court, which authorises the execution of the LoR sent by the issuing state to the Albanian judicial authorities. <u>There is not a possibility of an ex-post notification.</u></p>
Bugging of a car	
Issuing state EU Member State	<p>1. In accordance with the provisions of the MLA convention, and the Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, a LoR should be transmitted to the Albanian authorities (Ministry of Justice).</p> <p>In case of urgency, LoR may be addressed directly by the judicial authorities of the requesting Party to the judicial authorities of Albania. They shall be returned together with the relevant documents through the channels stipulated in paragraph 1 of Article 15 of the MLA Convention. Eurojust can be used as a channel of communication.</p> <p>2. Albanian legislation stipulates that the use of tracing means of the location shall be allowed only when there is an investigation being carried out for intent crimes, punishable with at least three years' imprisonment, in the maximum term.</p> <p>An interception may be authorised against:</p> <ul style="list-style-type: none"> a) a suspect for a criminal offence;

	<p>b) a person who is believed receiving or transmitting communications to the suspected person;</p> <p>c) a person who takes part in transactions with the suspect; c) a person whose surveillance may lead to the discovery of the location or the suspect's identity.</p> <p>3. The use of tracing means of the location is authorised by the court, which authorises the execution of the LoR sent by the requested state to Albania. <u>There is not a possibility of an ex-post notification.</u></p>
Surveillance through Trojan horse software	
Issuing state Member State EU	<p>1. Yes it is legal. (Article 221 of the Criminal Procedure Code)</p> <p>2. Albanian legislation stipulates that the interception of communications of a person or of a telephone number, by means of telephone, fax, computer or any other kind of means, shall be allowed only when there is an ongoing investigation:</p> <p>a) for intent crimes, punishable by at least seven years' imprisonment, in the maximum term;</p> <p>b) for each intentional criminal offence, if committed by telecommunication means or with the use of information or telematics technology.</p> <p>c) for criminal offences referred to under "a", of paragraph 1, of Article 75/a, of Albanian Criminal Procedure Code(organised crime and corruption offences)</p> <p>An interception may be ordered against:</p> <p>a) a suspect for a criminal offence;</p> <p>b) a person who is believed receiving or transmitting communications to the suspected person;</p> <p>c) a person who takes part in transactions with the suspect;</p> <p>ç) a person whose surveillance may lead to the discovery of the location or the suspect's identity</p> <p>3.</p> <p>4. In accordance with the provisions of the MLA Convention, and the Committee of Ministers Recommendations No. R (85) 10 concerning the practical application of the European Convention on Mutual Assistance in Criminal Matters in respect of letters rogatory for the interception of telecommunications, a LoR should be transmitted to the Albanian authorities(Ministry of Justice).</p> <p>In case of urgency, the LoR may be addressed directly by the judicial authorities of the requesting Party to the judicial authorities of Albania. They shall be returned together with the relevant documents through the channels stipulated in paragraph 1 of Article 15 of the MLA Convention. . Eurojust can be used as a channel of communication.</p> <p>5. Upon the request of the prosecutor for the execution of the LoR, the court shall authorise or not the interception through Trojan horse software installed on portable electronic devices upon a grounded decision. This authorisation will be granted on condition that it is indispensable for continuing with an already initiated investigation and where there is a reasonable doubt against the person, based on evidence, that he/she has committed one of the abovementioned criminal offences.</p>
Audio/video surveillance in a private place	
Issuing state EU	<p>1. Yes (Article 221 of the Criminal Procedure Code)</p>


Member State	<p>2. Albanian legislation stipulates that the secret interception by technical means of conversations in private places shall be allowed only where there is an ongoing investigation;</p> <p>a) for intent crimes, punishable by at least seven years' imprisonment, in the maximum term;</p> <p>b) for each intentional criminal offence, if committed by telecommunication means or with the use of information or telematics technology.</p> <p>c) for criminal offences referred to under "a", of paragraph 1, of Article 75/a, of the Criminal Procedural Code(the ones that fall under the competence of the Prosecution Office against organised crime and corruption);</p> <p>Upon the request of the prosecutor for the execution of the LoR, in the instances above described, the court shall authorise the interception upon a grounded decision, as long as it is indispensable for the continuance of an initiated investigation and wherever exists a reasonable doubt against a person based on evidence that he/she has committed a criminal offence.</p> <p>If any of the two persons to be intercepted is offered to carry out and record the communication, such an action can be carried out upon the authorization of the prosecutor in charge of the execution of the LoR, but he/she should always had been authorised by the court to execute the requested LoR.</p> <p>The interception decision (the court's) shall indicate the method and time limit for which it can be carried out, which cannot exceed fifteen days. Such time limit can be extended by the court for a period of 15 days, upon the reasoned request of the prosecutor, whenever it is necessary, provided for the conditions set forth in the law still exist and the outcome of the interception dictate the need for extending the time period.</p> <p>In the instance of the secret photographic or video interception or on the interception of conversations in private locations, the court may authorise the judicial police officer or the qualified specialist to access these locations secretly, acting in accordance with the decision. This authorisation shall be implemented within 15 days.</p>
Interception of telecommunication abroad	
Issuing state EU Member State	<p>1. Albanian legislation stipulates that the interception of telecommunication shall be allowed only when there is an ongoing criminal proceeding/investigation:</p> <p>a) for intent crimes, punishable by at least seven years' imprisonment, in the maximum term;</p> <p>b) for each intentional criminal offence, if committed by telecommunication means or with the use of information or telematics technology.</p> <p>c) for criminal offences referred to under "a", of paragraph 1, of Article 75/a, of this Code(crimes which fall under the competence of the prosecution office against organised crime and corruption);</p> <p>An interception may be ordered against:</p> <p>a) a suspect for a criminal offence;</p> <p>b) a person who is believed receiving or transmitting communications to the suspected person;</p> <p>c) a person who takes part in transactions with the suspect;</p> <p>ç) a person whose surveillance may lead to the discovery of the location or the suspect's identity.</p> <p>The result of the interception is valid towards all persons involved in the communication.</p>


	<p>2.1. Upon the request of the prosecutor in charge of the execution of LoR, in the instances described above, the court shall authorise the interception upon a grounded decision, as long as it is indispensable for the progressing of an initiated investigation and where a reasonable doubt exists against the person and based on evidence that he/she has committed at least one of the abovementioned criminal offences. Albanian legislation and jurisprudence considers interception as the last resort to obtain evidence. It should be used only if no other investigative measures proved satisfactory.</p> <p>2.2. If any of the two persons to be intercepted is available to carry out and register the relevant action, such action can be carried out upon authorisation of the prosecutor in charge of the execution of the LoR. However, he/she should always had received the authorisation of the court to execute the LoR whenever a request for interception is addressed through it.</p> <p>2.3. The court shall rule by reasoned decision in closed session within 24 hours of the submission of the request by the prosecutor.</p> <p>2.4. The interception decision/authorisation shall indicate the method and time limit for its execution, which cannot exceed fifteen days. Such time limit can be extended by the court for a period of 15 days, upon the reasoned request of the prosecutor, whenever it is necessary, if the conditions set forth in law still exist and the outcome of the interception dictate the need for extending the time.</p> <p>2.5 The interception actions may be performed only through equipment installed in designed locations, authorised and controlled by the prosecutor. The judicial police, under the direction and supervision of the prosecutor who executes the LoR, shall do the interception and the transcript of the minutes.</p> <p>2.6 If any of the interception requirements no longer exist, the judicial police officer shall immediately notify the prosecutor, who shall order the interruption of the interception and inform the court and the requesting foreign judicial authority.</p> <p>2.7. Intercepted communications shall be recorded and minutes shall be kept for all actions carried out. The minutes shall include transcription of the contents of intercepted communications.</p> <p>2.8. Interception of conversations or communications of those who are obliged to keep the secrecy because of their profession or duty shall not be used, except when these persons have already testified on the same facts or have disclosed such information in any other way.</p>
--	---

4.2.2. Georgia (GE)

GEORGIA 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state EU Member State	
Bugging of a car	
Issuing state EU Member State	
Surveillance through Trojan horse software	
Issuing state EU Member State	
Audio/video surveillance in a private place	
Issuing state EU Member State	
Interception of telecommunication abroad	
Issuing state EU Member State	
Relevant documents	

4.2.3. Montenegro (ME)


MONTENEGRO	
	
<p>Answer Montenegro:</p> <p>The Law on mutual legal assistance in criminal matters of Montenegro stipulates that forms of international legal assistance include: submitting documents, written materials and other cases related to the criminal proceedings in the requesting country; mutual exchange of information, as well as undertaking of individual procedural actions; hearing the accused, witness and expert, including hearing through video and telephone conference, crime scene investigation, search of premises and persons, temporary seizure of items, secret surveillance measures, DNA analysis, temporary surrender of a person deprived of liberty in order to give testimony, delivering information from penal records, information on the judgement and other procedural actions.</p> <p>Measures of secret surveillance are prescribed by the Criminal Procedure Code of Montenegro (please find under ‘relevant documents’ an excerpt of provisions of the CPC). In relation to your questions, the legal basis for cooperation with other countries are bilateral and multilateral conventions if they have been ratified by the states whose competent national authorities need international cooperation in a particular criminal case.</p> <p>In this particular case, the competent judicial authority of the a foreign state may contact the competent judicial authority of Montenegro (court or state prosecutor’s office) by letter of request (letter rogatory) through the Ministry of Justice, as the central communication authority, or directly (if for example both states have ratified the Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters), and request the implementation of certain procedural actions i.e. implementation of secret surveillance measures, which are defined by national legislation, that is CPC.</p>	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state EU Member State	
Bugging of a car	
Issuing state EU Member State	
Surveillance through Trojan horse software	
Issuing state EU Member State	
Audio/video surveillance in a private place	
Issuing state EU Member State	

Member State	
Interception of telecommunication abroad	
Issuing state EU Member State	
Relevant documents	
 Annex.Montenegro	


4.2.4. North Macedonia (MK)





NORTH MACEDONIA	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state EU Member State	<p>1. GPS tracking as a special investigative measure is not envisioned in North Macedonia. However, taking broader approach it can be considered part of the special investigative measure under article 252 paragraph 1-2 of the Criminal Procedure Code that enables surveillance and recording in homes, closed up or fenced space that belongs to the home or office space designated as private or in a vehicle and the entrance of such facilities in order to create the required conditions for monitoring of communications. This special investigative measure can be implemented on bases of court order issued by domestic courts, thus MLA request is necessary.</p> <p>2. In order this measure to be executed the following conditions must be met:</p> <ul style="list-style-type: none"> - Grounds for suspicion that a crime enlisted in Article 253 of the Criminal Procedure Code was committed must exist (full text of this article is given at the end of the questionnaire) - The measure must be ordered against a person: <ol style="list-style-type: none"> 1) who committed a criminal offense as stipulated in article 253 of this Law; 2) who undertakes activities in order to commit a criminal offense as stipulated in article 253 of this Law; and 3) who is preparing the commission of a criminal offense as stipulated in Article 253, when such preparation is punishable according to the provisions of the Criminal Code. 4) who receives or relays shipments to and from the suspect or if the suspect uses his or her communication device. <p>If the person is not able to be determined, this special investigative measure can be ordered against the object (the vehicle)</p> <ul style="list-style-type: none"> - There is no other less intrusive way to gather the evidence (explanation on the reasons due to which the data or evidence cannot be collected otherwise) - The duration of the measure is specified <p>3. The Courts (the preliminary procedure judge) on bases of written well-justified request by the prosecutor.</p>
Bugging of a car	
Issuing state EU Member State	<p>1. Bugging of a car is part of the special investigative measure under art.252 paragraph 1-2 of the Criminal Procedure Code that enables surveillance and recording in homes, closed up or fenced space that belongs to the home or office space designated as private or in a vehicle and the entrance of such facilities in order to create the required conditions for monitoring of communications. This special investigative measure can be implemented on bases of court order issued by domestic courts, thus MLA request is necessary.</p> <p>2. Same as the answer under question 1</p> <p>3. Same as the answer under question 1</p>

Surveillance through Trojan horse software	
Issuing state EU Member State	<p>1. Surveillance through Trojan horse software as such is not envisioned.</p> <p>2. /</p> <p>3. The alternative of kind of surveillance is implementation of the special investigative measure under art.252 paragraph 1-4 of the Criminal Procedure Code that enables secret access and search of computer systems.</p> <p>4. This special investigative measure can be implemented on bases of court order issued by domestic courts, thus MLA request is necessary. The conditions for issuing this special investigative measure are given in the second answer of question 1.</p> <p>5. The Courts (the preliminary procedure judge) on bases of written well-justified request by the prosecutor.</p>
Audio/video surveillance in a private place	
Issuing state EU Member State	<p>1. Yes, this special investigative measure is part of the special investigative measure under art.252 paragraph 1-2 of the Criminal Procedure Code that enables surveillance and recording in homes, closed up or fenced space that belongs to the home or office space designated as private or in a vehicle and the entrance of such facilities in order to create the required conditions for monitoring of communications.</p> <p>2. This special investigative measure can be implemented on bases of court order issued by domestic courts, thus MLA request is necessary. The conditions for issuing this special investigative measure are explained in the second answer of question 1. The competent authority for issuing this measure is the court (the preliminary procedure judge) on bases of written well-justified request by the prosecutor.</p> <p>3. /</p>
Interception of telecommunication abroad	
Issuing state EU Member State	<p>1. The conditions for granting the special investigative measure interception of communication are the following:</p> <ul style="list-style-type: none"> - Grounds for suspicion that a crime enlisted in Article 253 of the Criminal Procedure Code was committed must exist (full text of this article is given at the end of the questionnaire) - The measure must be ordered against a person: <ul style="list-style-type: none"> 1) who committed a criminal offense as stipulated in article 253 of this Law; 2) who undertakes activities in order to commit a criminal offense as stipulated in article 253 of this Law; and 3) who is preparing the commission of a criminal offense as stipulated in Article 253, when such preparation is punishable according to the provisions of the Criminal Code. 4) who receives or relays shipments to and from the suspect or if the suspect uses his or her communication device. <p>If the person is not able to be determined, this special investigative measure can be ordered against the object (telephone or IMEI number of the device)</p> - There is no other less intrusive way to gather the evidence (explanation on the reasons due to which the data or evidence cannot be collected otherwise)


	<ul style="list-style-type: none"> - The duration of the measure is specified <p>Any special investigative measure, shall last for not longer than 4 months.</p> <p>Interception of communication can be extended for a maximum additional period of up to 4 months. The preliminary procedure judge must approve the extension, upon an elaborated written request by the public prosecutor.</p> <p>For criminal offenses that entail a prison sentence of at least four years and which are suspected to have been committed by an organized group, gang or other criminal enterprise, upon a written request by the public prosecutor, and based on the assessment of the usefulness of the data obtained through the use of the measure and with a reasonable expectation that the measure may continue to result with data of interest for the procedure, the judge of the preliminary procedure may additionally extend the period for another 6 months at the most.</p> <p>2. This special investigative measure is executed by the public prosecutor or by the judicial police, under the control of the public prosecutor.</p> <p>3. Not at the moment.</p>
Relevant documents	
<div data-bbox="387 884 443 947" data-label="Image">  </div> <p>Additional information MK</p>	

4.2.5. Norway (NO)

NORWAY 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state Member State EU	<ol style="list-style-type: none"> 1. LoR. 2. Apart from the fact that a LoR are is needed, no additional conditions except for requirements in national legislation, attachment A, section 202 b (typically GPS tracker on a car) and 202 c (e.g. GPS tracker in clothing or hand baggage). 3. Prosecution service is empowered to decide under section 202 b, the court under section 202 c (however an LoR section 202 c measures is to be sent to the prosecution service, which will send a request to the court)
Bugging of a car	
Issuing state Member State EU	<ol style="list-style-type: none"> 1. From what we understand this is a question of audio surveillance in a car. LoR is the tool to use. Regarding agreements etc. see question a) number 1. 2. Please see attachment C for national legislation describing the conditions (in addition to LoR). 3. The Court is empowered to decide under normal circumstances. If delay entails a great risk that the investigation will be impaired, an order from the prosecuting authority may take the place of a court decision, but the court must always be involved within 24 hours afterwards. An LoR requesting this measure is to be sent to the prosecution service.
Surveillance through Trojan horse software	
Issuing state Member State EU	<ol style="list-style-type: none"> 1. Yes, this would be considered to be Intrusive data capture. 2. Please see attachment D for the conditions in our national legislation (in addition to a LoR). 3. N/A 4. LoR. Please see question a), section 1). 5. The Court is empowered to decide under normal circumstances. If delay entails a great risk that the investigation will be impaired, an order from the prosecuting authority may take the place of a court decision, but the court must always be involved within 24 hours afterwards. An LoR requesting this measure is to be sent to the prosecution service.
Audio/video surveillance in a private place	
Issuing state Member State EU	<ol style="list-style-type: none"> 1. Yes. (Audio surveillance in a car, question b) would be considered surveillance in a private place) Video surveillance in a private place is allowed, although video-surveillance in a private home is not allowed. 2. Please see attachment A, section 202 a for video surveillance, and attachment C for audio surveillance. The Court is empowered to decide under normal circumstances. If delay entails a great risk that the investigation will be impaired, an order from the prosecuting authority

	<p>may take the place of a court decision, but the court must always be involved within 24 hours afterwards. An LoR requesting this measure is to be sent to the prosecution service.</p> <p>3. Although video surveillance into a private home is not allowed, a police officer may observe through a window inside a private home, he/she may also use binoculars when doing so.</p>
Interception of telecommunication abroad	
Issuing state EU Member State	<p>1. Apart from a LoR, the requirements in our national legislation must be met, see attachment B. Section 216 a sets out the requirements for interception of communication, whereas section 216 b sets out the requirements for other control measures directed at communication devices.</p> <p>2. The Court is empowered to decide under normal circumstances. If delay entails a great risk that the investigation will be impaired, an order from the prosecuting authority may take the place of a court decision, but the court must always be involved within 24 hours afterwards. An LoR requesting this measure is to be sent to the prosecution service.</p> <p>3. Yes it possible, but depends on the technical arrangements in the different countries. Regarding agreements etc. see question a) number 1</p>
Relevant documents	
<div> <div>  <p>NO - Dataavlesning.docx</p> </div> <div>  <p>NO - KK mm_.docx</p> </div> <div>  <p>NO - Romavlytting.docx</p> </div> <div>  <p>NO - SKO og logger.docx</p> </div> </div>	

4.2.6. Serbia (RS)


<div style="text-align: center;"> SERBIA  </div>	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state Member State EU	<p>1. LoR is needed for provision of MLA. Republic of Serbia has ratified all the relevant international treaties of importance for MLA, both the treaties concluded within United Nations (UNTOC, UNCAC etc.), and the ones concluded under Council of Europe, in particular, Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters.</p> <p>2. MLA Law prescribes a set of conditions for provision of MLA i.e. for execution of any MLA request (Art. 7 of MLA Law, points 1-5 below), with two additional conditions provided for so-called “other forms of MLA”, i.e. minor MLA (Art. 84 of MLA law, points 6 and 7 below):</p> <ol style="list-style-type: none"> 1) that the criminal offence, in respect of which mutual legal assistance is requested, constitutes the criminal offence under the legislation of the Republic of Serbia; 2) that the proceedings for the same criminal offence have not been finally concluded before the national court, i.e. that a criminal sanction has not been completely executed; 3) that the criminal prosecution, i.e. execution of a criminal sanction is not excluded due to the statute of limitation, amnesty or pardon; 4) that the request for the provision of mutual legal assistance does not refer to a political criminal offence or an offence connected with a political criminal offence, i.e. to the criminal offence comprising exclusively violation of military duties; 5) that the provision of mutual legal assistance would not infringe the sovereignty, security, public order or other interests of essential importance for the Republic of Serbia. 6) the conditions envisaged under the Criminal Procedure Code are fulfilled; 7) no criminal proceedings are conducted against the same person before the national court for the criminal offence requiring the provision of mutual legal assistance. <p>When it comes to the conditions provided under the Criminal Procedure Code (hereafter: the CPC), it is to be noted that this measure falls into a category of so-called ‘special evidentiary actions’ – covert surveillance and recording, provided under Article 171 of the CPC. This measure (as all the other special evidentiary actions provide under the CPC, as provided under Article 161 of the CPC) may be ordered against a person for whom there are grounds for suspicion that he/she has committed a limited number of prescribed criminal offences (organised crime, war crimes, and other particularly grave offences as enumerated under Art. 162 of the CPC, integrally quoted in the text below) and only where evidence necessary for prosecution could not be obtained otherwise, or could be obtained only with great difficulty. By way of an exception, this measure can also be instituted with respect to a person for whom there are reasonable grounds to believe they are engaged in preparing to commit one of enumerated offences if the circumstances of the case are such that the offence could not be uncovered, prevented, or proven otherwise, or where doing so would entail disproportionate difficulty or serious danger.</p> <p>Two additional conditions specific for covert surveillance and recording are also provided under Article 171 of the CPC related to the purpose of this measures. Namely, acting on a reasoned motion of the public prosecutor, the court may order covert surveillance and recording of a suspect for the purpose of:</p> <ol style="list-style-type: none"> 1) detecting contacts or communication of the suspect in public places where access is limited or in premises, except in a dwelling;

	<p>2) determining the identity of a person or locating persons of things.</p> <p>The locations or premises referred to in paragraph 1 item 1) of this Article or vehicles belonging to other persons may be the object of covert surveillance and recording only if it is probable that the suspect shall be present there or that he is using those vehicles.</p> <p>Criminal Offences in Respect of Which Special Evidentiary Actions are Applied</p> <p>Article 162</p> <p>Under the conditions referred to in Article 161 of this Code, special evidentiary actions may be ordered for the following criminal offences:</p> <p>1) those which according to separate statute fall within the competence of a prosecutor's office of special jurisdiction;</p> <p>2) aggravated murder (Article 114 of the Criminal Code), abduction (Article 134 of the Criminal Code), showing, procurement and possession of pornographic materials and exploiting juveniles for pornography (Article 185 paragraphs 2 and 3 of the Criminal Code), robbery (Article 206, paras. 2 and 3 of the Criminal Code), extortion (Article 214 paragraph 4 of the Criminal Code), abuse of a position of a responsible person (Article 227 of the Criminal Code), abuse concerning public procurement (Article 228 of the Criminal code), accepting bribe in conducting of a business activity (Article 230 of the Criminal Code), giving bribe in conducting of a business activity (Article 231 of the Criminal Code), counterfeiting money (Article 241, paras. 1 through 3 of the Criminal Code), money laundering (Article 245, paras. 1 through 4 of the Criminal Code), unlawful production and circulation of narcotics (Article 246, paras.1 through 4 of the Criminal Code), threatening independence (Article 305 of the Criminal Code), threatening territorial integrity (Article 307 of the Criminal Code), sedition (Article 308 of the Criminal Code), inciting sedition (Article 309 of the Criminal Code), subversion (Article 313 of the Criminal Code), sabotage (Article 314 of the Criminal Code), espionage (Article 315 of the Criminal Code), divulging state secrets (Article 316 of the Criminal Code), inciting national, racial and religious hatred or intolerance (Article 317 of the Criminal Code), violation of territorial sovereignty (Article 318 of the Criminal Code), conspiring to conduct activities against the Constitution (Article 319 of the Criminal Code), plotting an offences against the constitutional order and security of Serbia (Article 320 of the Criminal Code), serious offences against the constitutional order and security of Serbia (Article 321 of the Criminal Code), illegal manufacture, possession and sale of weapons and explosive materials (Article 348 paragraph 3 of the Criminal Code), illegal crossing of the national boarder and human trafficking (Article 350 paragraphs 2 and 3 of the Criminal Code), abuse of office (Article 359 of the Criminal Code), trading in influences (Article 366 of the Criminal Code), taking bribes (Article 367 of the Criminal Code), offering bribes (Article 368 of the Criminal Code), human trafficking (Article 388 of the Criminal Code), endangering people enjoying international protection (Article 392 of the Criminal Code) and the criminal offence referred to in Article 98, paras. 2 through 5* of the Law on the Secrecy of Data;</p> <p>3) obstruction of justice (Article 336 paragraph 1 of the Criminal Code), if committed in connection with the criminal offence referred to in items 1) and 2) of this paragraph.</p> <p>A special evidentiary action referred to in Article 183 of this Code may be ordered only in connection with a criminal offence referred to in paragraph 1 item 1) of this Article.</p> <p>Under the conditions referred to in Article 161 of this Code the special evidentiary action referred to in Article 166 of this Code may also be ordered for the following criminal offences: unauthorised exploitation of copyrighted work or other works protected by similar rights (Article 199 of the Criminal Code), damaging computer data and programmes (Article 298 paragraph 3 of the Criminal Code), computer sabotage (Article 299 of the Criminal Code), computer fraud (Article 301 paragraph 3 of the Criminal Code) and unauthorised access to protected computers, computer networks and electronic data processing (Article 302 of the Criminal Code).</p>
--	---

	3. Covert surveillance and recording is ordered by the judge for preliminary proceedings by a reasoned order, acting on a reasoned motion of the public prosecutor. This order is executed by the police, Security Information Agency or Military Security Agency.
Bugging of a car	
Issuing state EU Member State	As this measure falls as well into special evidentiary action covert surveillance and recording, all of the answers provided under previous question apply (see answer to Question 1).
Surveillance through Trojan horse software	
Issuing state EU Member State	<p>1. Yes. Surveillance under software would fall under special evidentiary action of covert supervision/interception of communication provided under Article 166 of the CPC.</p> <p>2. The conditions provided under MLA Law and under Articles 161 and 162 of the CPC, enumerated under answers to question a) apply for this measure as well. Pursuant to Article 166 of the CPC, acting on a reasoned request by the public prosecutor, the court may order supervision and recording of communications conducted by telephone or other technical means or surveillance of the electronic or other address of a suspect and the seizure of letters and other parcels.</p> <p>3. n/a</p> <p>4. LoR is needed for provision of MLA. Republic of Serbia has ratified all the relevant international treaties of importance for MLA, both the treaties concluded within United Nations (UNTOC, UNCAC etc.), and the ones concluded under Council of Europe, in particular, Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS 182) and Convention on Cybercrime (ETS 185).</p> <p>5. Covert supervision of communication is ordered by the judge for preliminary proceedings, acting on a reasoned request by the public prosecutor. The order is executed by the police, Security Information Agency or Military Security Agency.</p>
Audio/video surveillance in a private place	
Issuing state EU Member State	<p>1. Due to constitutional guarantee of inviolability of home, CPC provided under article 171 that the special evidentiary action of covert surveillance and recording may not include a dwelling/home. Namely, if the conditions provided by the CPC are met, the court may order covert surveillance and recording of a suspect for the purpose of 1) detecting contacts or communication of the suspect in public places where access is limited or in premises, except in a dwelling/home; 2) determining the identity of a person or locating persons or things.</p> <p>2. n/a</p> <p>3. Special evidentiary action of covert supervision of communication might be considered as an alternative.</p>
Interception of telecommunication abroad	
Issuing state EU Member State	1. Covert supervision/interception of communication may be executed upon an MLA request if the conditions provided under Articles 7 and Art. 84 of MLA law (quoted under answer to 2b) are met, including the conditions provided under CPC (Articles 161,162 and 166 enumerated under questions a) and c).


	<p>2. Covert supervision/interception of communication is ordered by the judge for preliminary proceedings, acting on a reasoned request by the public prosecutor. The order is executed by the police, Security Information Agency or Military Security Agency.</p> <p>3. Direct communication of judicial authorities is possible in cases provided under bilateral/multilateral agreements. We note that, among other significant multilateral agreements, Serbia has ratified Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters (ETS 182) without reservations concerning possibility of direct communications between judicial authorities and Convention on Cybercrime (ETS 185). Certain bilateral agreements concluded by Serbia also enable direct communication between judicial authorities for certain types of MLA (Slovenia, Montenegro etc.)</p>
--	---

4.2.7. Switzerland (CH)


SWITZERLAND 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state EU Member State	<ol style="list-style-type: none"> 1. Letter of request (European Convention on Mutual Assistance in Criminal Matters, content of the LoR according to Art. 14; Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters) 2. There is no restriction with regard to the crimes, provided that an offence eligible for mutual legal assistance is the subject of the LoR. Due to the domestic standards, it is necessary that the LoR is submitted as soon as possible after it has been established that the border has been crossed. 3. In principle, the Federal Office of Justice is competent as the central authority, unless <ul style="list-style-type: none"> - contacts already exist with a competent PPO - the cantonal PPO was already involved when the border was crossed
Bugging of a car	
Issuing state EU Member State	<ol style="list-style-type: none"> 1. Letter of request (European Convention on Mutual Assistance in Criminal Matters, content of the LoR according to Art. 14; Second Additional Protocol to the European Convention on Mutual Assistance in Criminal Matters) 2. There is no restriction with regard to the crimes, provided that an offence eligible for mutual legal assistance is the subject of the LoR. Due to the domestic standards, it is necessary that the LoR is submitted as soon as possible after it has been established that the border has been crossed. 3. In principle, the Federal Office of Justice is competent as the central authority, unless <ul style="list-style-type: none"> - contacts already exist with a competent PPO - the cantonal PPO was already involved when the border was crossed
Surveillance through Trojan horse software	
Issuing state EU Member State	<ol style="list-style-type: none"> 1. Yes, in principle this is a legal form of interception, but under very restrictive conditions. 2. There is no established jurisdiction in this area, so decisions will have to be made on a case-by-case basis. <p>This surveillance measure can only be considered if the following conditions are met:</p> <ul style="list-style-type: none"> - there is a strong suspicion that a catalogue crime (Article 286 paragraph 2 CrimPC) has been committed <p>SR 312.0 - Swiss Criminal Procedure Code of 5 October 2007 (Criminal Procedure Code, CPC) (admin.ch)), and</p> <ul style="list-style-type: none"> - the seriousness of the offences justifies surveillance and - investigative activities carried out so far have been unsuccessful or the enquiries would otherwise have no prospect of success or be made unreasonably complicated and

	<p>- previous telecommunications surveillance measures under Article 269 CrimPC have been unsuccessful or surveillance with these measures would be futile or disproportionately difficult.</p> <p>3. -</p> <p>4. Letter of request</p> <p>5. The Federal Office of Justice</p>
Audio/video surveillance in a private place	
Issuing state Member State	<p>1. Yes.</p> <p>2. Reason to believe on the basis of specific information that felonies or misdemeanours have been committed and the enquiries would otherwise have no prospect of success or be made unreasonably complicated. Letter of request to the PPO at the location of the requested surveillance measure or at the location of the focus of the criminal activities (https://www.elorge.admin.ch/elorge). If this is not clear, the Federal Office of Justice is subsidiary the competent authority.</p>
Interception of telecommunication abroad	
Issuing state Member State	<p>1. Strong suspicion that an offence listed in Article 269 paragraph 2 CrimPC (SR 312.0 - Swiss Criminal Procedure Code of 5 October 2007 (Criminal Procedure Code, CPC) (admin.ch) has been committed; the seriousness of the offence justifies surveillance; and investigative activities carried out so far have been unsuccessful or the enquiries would otherwise have no prospect of success or be made unreasonably complicated.</p> <p>Retroactive data collection limited to a maximum of 6 months.</p> <p>The duration of monitoring is limited to 3 months and any extension must be duly justified.</p> <p>2. Letter of request to the PPO at the location of the surveillance, subsidiary to the Federal Office of Justice</p> <p>3. The real-time transfer of content data is only possible in cases of organised crime or terrorism.</p>

4.2.8. Ukraine (UA)


UKRAINE 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state EU Member State	
Bugging of a car	
Issuing state EU Member State	
Surveillance through Trojan horse software	
Issuing state EU Member State	
Audio/video surveillance in a private place	
Issuing state EU Member State	
Interception of telecommunication abroad	
Issuing state EU Member State	
Relevant documents	

4.2.9. United Kingdom (UK)

UNITED KINGDOM 	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state Member State EU	<ol style="list-style-type: none"> 1. Requests can be executed via police-to-police cooperation under Article 17 of the Second Additional Protocol to the 1959 Council of Europe Convention on Mutual Assistance in Criminal Matters 2. If the crime is under active investigation in the issuing state and the measure is proportionate the request will likely be granted. However, permission must be sought from the UK before any material is generated. 3. National Crime Agency
Bugging of a car	
Issuing state Member State EU	<ol style="list-style-type: none"> 1. Requests can be executed via police-to-police cooperation under Article 17 of the Second Additional Protocol to the 1959 Council of Europe Convention on Mutual Assistance in Criminal Matters 2. If the crime is under active investigation in the issuing state and the measure is proportionate the request will likely be granted. However, permission must be sought from the UK before any material is generated. 3. National Crime Agency
Surveillance through Trojan horse software	
Issuing state Member State EU	<ol style="list-style-type: none"> 1. Contact the National Crime Agency (National Cyber Crime Unit) to discuss any requirements. 2. N/A 3. Contact the National Crime Agency (National Cyber Crime Unit) to discuss requirements. 4. Contact the National Crime Agency (National Cyber Crime Unit) to discuss requirements. 5. Contact the National Crime Agency to discuss requirements.
Audio/video surveillance in a private place	
Issuing state Member State EU	<ol style="list-style-type: none"> 1. Yes 2. If the crime is under active investigation in the requesting state and the measure is proportionate the request will likely be granted. However, permission needs to be sought from the UK before any material is generated. It is likely that this request would fall to the National Crime Agency to fulfil 3. N/A
Interception of telecommunication abroad	

Issuing state EU Member State	<ol style="list-style-type: none">1. RIPA and the accompanying Codes of Practice provide the UK legal framework for interception of communications. Interception can only be authorised for the purpose of preventing/detecting serious crime.2. National Crime Agency3. Contact the National Crime Agency to discuss any requirements.
--	---

4.2.10. United States of America (US)

UNITED STATES OF AMERICA	
	
GPS tracking installed in the issuing country and crossing the border (no need for technical assistance)	
Issuing state EU Member State	
Bugging of a car	
Issuing state EU Member State	
Surveillance through Trojan horse software	
Issuing state EU Member State	
Audio/video surveillance in a private place	
Issuing state EU Member State	
Interception of telecommunication abroad	
Issuing state EU Member State	
Relevant documents	